D7.4 – SAFERtec Standardization Plan

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-Infrastructure (V2I) communications aiming at improving the cyber-physical security ecosystem of "connected vehicles" in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related Connected Vehicle and V2I systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics applications, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

DX.X & Title:	D7.4 – SAFERtec Standardization Plan
Work package:	Dissemination
Task:	T7.3 Standardization Plan and Activities
Due Date:	31/12/2017
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR Sammy HADDAD / OPP	**DATE** 27/04/2018
CONTRIBUTORS Sammy HADDAD / OPP Andras Varadi / CMS Andras Edelmayer / CMS Alessandro Marchetto / CRF Silvia Capato / SWA	**DATE** 27/04/2018 20/08/2018
REVIEWED BY Onn Haran / AUT Leo Menis / AUT Matthieu GAY / CCS Panagiotis Pantazopoulos / ICCS	**DATE** 1/10/2018 5/11/2018
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Document/Revision history

Version	Date	Partner	Description
V0.1	10/07/2017	OPP	First draft (definition of section and their content)
V0.2	26/10/2017	OPP	Sections and structure update
V0.3	29/12/2017	COMM	Added COMM contribution
V0.4	24/04/2018	OPP, CMS, CRF, SWA	Revised
V0.5	17/07/2018	OPP	Standards descriptions, internal review-ready
V0.6	19/08/2018	OPP	Updates after internal review
V0.7	23/09/2018	OPP and ICCS	Risks and mitigation actions related to the standardization plan
V0.8	09/11/2018	ICCS	Comments throughout the text
V1.0	12/11/2018	OPP	Final version
V1.1	30/1/2019	OPP	Revised according to the reviewers' comments. The changes include: • Clarifications of the deliverable's scope and content in the executive summary and introduction • Improvements in the presentation of standards state-of-the-art analysis (sources of information, WP involved, partners and standard knowledge, etc.) • Justification of the likelihood of each target (reflecting the priority of each target) • Updated and detailed standardization plan in section 4.3.3 with clear responsibilities.
V1.5	01/02/2019	ICCS	Comments and edits
V1.6	05/02/2019	OPP	Final version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Table of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Abbreviation	Description
BSS	Basic Service Set
CAM	Co-operative Awareness Message
CC	Common Criteria
C-ITS	Co-operative ITS
CPS	Cyber Physical Systems
DENM	Decentralized Environmental Notification Message
IoT	Internet of Things
IT	Information Technology
ITS	Intelligent transport system
IVI	In-Vehicle Information
KPSI	Key Performance Security Indicator
OBU	On-Board Unit
PKI	Public key infrastructure
SACA	Security Assurance Conformity Assessment
SAF	SAFERtec Assurance Framework
SFR	Security Functional Requirements
SRM	Signal Request Message
SSM	Signal Status Messages
ST	Security Target
SDO	Standard Development Organization
TOE	Target Of Evaluation
TSF	TOE Security Functions

Table 1: List of Abbreviations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

The current document proposes the SAFERtec standardisation plan. Its main objectives are

- the identification of existing standards using mainly publicly available data together with some specific partners knowledge:
    - for security assurance in the ITS and automotive industry
    - from other domains related to information assurance, privacy and safety in the scope of IoT and CPS
- the identification of interdependencies, gaps and emerging standardization activities related to the project scope or the identified existing standardisation activities
- the definition of a detailed standardisation action plan and recommendations for the project partners together with the available communication channels to those bodies

The proposed plan includes the definition of activities and the required time-scheduling to attain the SAFERtec standardization work objectives. Importantly, the plan is associated with a number of relevant risks and mitigation actions are defined for each one of them.

We've proposed a first generic action plan for a first set of targets at T0+12 in section 4.3.1 and 4.3.2 that we then updated in section 4.3.3 in order to provide a more detailed step by step action plan refined by targets and SAFERtec working groups, to better achieve an ambitious promotion and dissemination of the SAFERtec results in relevant ITS international standards.

1 Introduction

A standardization plan is presented in this deliverable. It identifies existing standards for functional specifications and security assurance in the ITS and automotive industry. Also, standards from other domains related to information assurance, privacy and safety in the scope of IoT and CPS are explored as well in order to identify interdependencies, gaps and emerging standardization activities and recommendations. A detailed list of standardization bodies, working groups, committees on EU level and international level are identified together with the available communication channels to those bodies. The current standardization plan then:

- makes a complete overview of standards related to ITS functional and security specifications
- defines from the overview a set of standards as candidate targets for receiving SAFERtec contributions
- defines responsible standardization groups (within the consortium) to facilitate any contribution to the above targets
- identifies a set of actions to be implemented towards the contribution (involving certain partners of the above groups)
- identifies the timing for each action to serve the SAFERtec standardization objectives.

1.1 Purpose of the Document

The current document proposes a standardisation plan for the project. Having identified the existing standards (for both ITS and other ICT domains) and the relevant gaps, the document introduces a clear standardization plan, discusses the channels to reach the standardization bodies and foresees related risks.

1.2 Intended readership

Besides the project reviewers, this deliverable is addressed to any interested reader (*i.e.*, Public dissemination level).

1.3 Inputs from other projects

No input from other projects was considered during the compilation of this deliverable.

1.4 Relationship with other SAFERtec deliverables

All the technical work items of the project on security issues, reflected in the corresponding deliverables (e.g., D2.2, D2.3, D2.4) are inputs for the present standardisation plan. In fact, the current document will evaluate for each of them the possibility to be used as standardization inputs.

2 Standardization bodies and contacts

Most of the following information is directly taken from the different standardization bodies web sites:

- http://www.sae.org
- https://www.etsi.org/
- https://www.iso.org/
- https://www.ieee.org/

We collected here that publicly available data in order to enhance and ease the definition and deployment of the SAFERtec standardization plan. In fact, since SAFERtec partners are not (at the beginning of the project) directly involved in ITS standardization activity, we first identify all the publicly known standardization bodies and their corresponding dedicated groups exploring the problem of ITS and assurance security standardization. Thus, once the standardization plan defined all the SAFERtec partners can easily find all the necessary data here with no need to redo time consuming internet researches.

2.1 SAE

http://www.sae.org

Society of Automotive Engineers International (SAE International), is a U.S.-based professional organization of scientists, engineers, and practitioners working in various industry fields, that is particularly active in aerospace, automotive and commercial-vehicle industry.

SAE aims at developing life-long learning and voluntary consensus industrial standards and it is a globally recognized as international automotive and aerospace standards setting body. SAE aims at developing standards that are then used by the global engineering community and regulatory agencies. SAE, in fact, develops standards for coordinating the work of government agencies and manufacturers working with advanced techniques to assure viable and safe technology, by means of shared standards.

In the last years, SAE focuses on standards advancing the vehicle connectivity. To this goal, the SAE International committees focused their work on developing standards related to dedicated short-range communications, automated vehicles, cybersecurity, and vehicle-to-vehicle safety communications. On this topic, special agreements have been developed by SAE International to collaboratively work on shared standards with the National Institute for Science and Technology (NIST), Wi-Fi Alliance, and the American Center for Mobility and ITS China.

One of the SAE International committee is the Vehicle Cybersecurity Systems engineering Committee of the SAE International works on several activities concerning several cybersecurity aspects, such as: dedicated events and publications (e.g., to propose and discuss new topics and approaches), new standards (e.g., see SAE J3061 the Cybersecurity Guidebook for Cyber-Physical Vehicle Systems), and training initiatives for industries and practitioners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.2 ETSI

ETSI was set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) in response to proposals from the European Commission.

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. The ETSI is officially recognized by the European Union as a European Standards Organization. It is an independent, not-for-profit organization.

ETSI is the recognized regional standards body – European Standards Organization (ESO) – dealing with telecommunications, broadcasting and other electronic communications networks and services.

The ETSI supports European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

From their official web sites ETSI announced that it publishes between 2,000 and 2,500 standards every year. Since their establishment in 1988, they have produced over than 30,000.

ETSI groups in the Transportation cluster are:

- ERM (EMC and Radio Spectrum Matters)
- ERM TG 26 (Task Group Maritime)
- ERM TG SRR (Task Group Automotive and Surveillance Radar)
- ERM TG AERO (Aeronautics)
- ITS (Intelligent Transport Systems)
- RT (Rail Telecommunications)
- SES (Satellite Earth stations and Services)

Standardization of Co-operative ITS is a global challenge and ETSI is collaborating with other standardization bodies in order to achieve worldwide interoperability and harmonized deployment.

In road transport many companies actively contribute to the standardization work - these include:

- vehicle manufacturers
- the automotive supply industry
- silicon vendors
- telecommunications network operators
- research bodies
- test houses

ETSI's aviation standards are developed by national regulators, air traffic management services, airport operators and aircraft manufacturers.

Much of the work performed in the cluster in support of European initiatives is done under Mandates issued by the European Commission and the European Free Trade Association (EFTA). The cluster also co-operates closely with various international organizations, including CEN, ISO, IEEE, SAE, IETF, ARIB, EUROCAE, EASA and ICAO to ensure harmonization and interoperability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

2.2.1 Types of ETSI standards

ETSI produces a variety of standards, specifications and reports to suit different purposes, in response to market demand.

- European Standard (EN)
- ETSI Standard (ES)
- ETSI Guide (EG)
- ETSI Technical Specification (TS)
- ETSI Technical Report (TR)
- ETSI Special Report (SR)
- ETSI Group Report (GR)
- ETSI Group Specification (GS)

These different types of standards are produced in different ways, in line with their respective purposes, and the time taken to draft and approve them varies.

All their standards are produced by consensus, and the standards work programme is determined by the ETSI members, according to their needs. ETSI's standards-making processes have been refined over the years and are well respected as being fair, transparent and efficient.

All specifications developed by the Third Generation Partnership Project (3GPP™) are also published by ETSI as Technical Specifications.

2.2.2 ETSI security dedicated working group : WG5

https://portal.etsi.org/TBSiteMap/ITS/ITSWG5ToR.aspx

Terms of Reference for Working Group 5: Security, approved at ITS#02

ETSI defined that working Group 5 shall be responsible for:

- Conducting studies leading to deliverables on Security;
- Assuring ITS solutions conform to regulatory requirements for privacy, data protection, lawful interception and data retention;
- Management and co-ordination of the development of security specifications for ITS communication and data;
- Investigation of security services and mechanisms required for providing ITS services over the Internet;
- Development of security analyses of candidate protocols and network elements to be used within the ITS framework to implement capabilities e.g., EMTEL aspects, IPv6 migration, keying strategies and methods;

Tracking the ongoing worldwide security activities of interest to ITS (notably in ISO TC204)

Working Group 5 shall undertake activities including, but not restricted to:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Determine and document the objectives and priorities for ITS security taking into account the needs and aspirations of users, operators, regulators and manufacturers (primarily building a secure Service Capability invocation and protection model).
- Accommodate, as far as is practicable, any regional regulatory requirements in security objectives. This includes regional regulatory requirements that are related to the processing of personal data and privacy.
- Ensure that a threat analysis for ITS is conducted and maintained as the feature set being standardised grows.
- Detail the security requirements for ITS to include, but not necessarily be limited to, security requirements for services, user access to services, billing and accounting, operations and maintenance, and fraud control.
- Detail the security requirements for the physical elements of ITS deployments to include, but not necessarily be limited to, security requirements for the access network, the core network and its interfaces to legacy networks and terminals.
- Define a security architecture for ITS which will satisfy the security requirements and align with the ITS system architecture.
- Produce specifications for:
    - All the elements in the security architecture.
    - Operations and management of the security elements.
    - Any cryptographic algorithms needed for the security elements.
- Ensure the availability of any cryptographic algorithms which need to be part of the common specifications (via SAGE for example).
- Define how the specifications for the security elements are to be integrated into the access network, core network, terminal, operation and maintenance and other relevant specifications produced for ITS, and to assist with that integration. Detail the requirements for lawful interception in ITS, and produce all specifications needed to meet those requirements. This work shall be performed in conjunction with TC Lawful Interception to ensure handover capabilities exist sufficient to support the intercepted material.
- Produce a time and milestones plan for the introduction of the various elements of the security architecture which is in line with the development of other relevant elements of ITS.
- Produce guidelines on the use of the ITS security elements, including any requirements for operator specific algorithms.
- Produce guidelines on the limitations of ITS security, and of the implications of not activating the security elements that are provided.

In addition, security services and mechanisms for providing services over the Internet will continue to be investigated. It is important to realize that security for open networks and for interoperability is challenging.

2.2.2.1 ITS Working Group Five work items in WG5

The mission of ITS-WG5 is to provide security standards within the ITS Standards platform:

- To protect the ITS platform (ITS-S)
- To protect the ITS infrastructure (RSU and beyond)
- To protect the ITS user

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ITS-WG5 also exists to provide guidance on the use of security standards to protect the ITS applications.

ITS-WG5 Current work is on:

- The development of standard for deploying signed CAM and DENM using IEEE 1609.2
- The PKI design to support IEEE 1690.2 and privacy

This work is being carried-out whilst maintaining regulatory compliance. It should provide minimum standards to support EU Mandates for ITS.

The ITS-WG5 future work should be:

- Extension for full communications technology suite
- Extension for full applications technology suite
- Extension for non-vehicle centric ITS

Standards under work (current work item as of 08/2017):

- Work Item RTS/ITS-00524 (TS 102 941)
  - Trust and Privacy Management
  - Stable draft (2017-06-26)
- Work Item DTR/ITS-00527 (TR 103 415)
  - Pre-standardisation study on pseudonym change management
  - Early draft (2017-05-10)
  - Literature survey of pseudonym change considerations and strategies with recommendations. Under development, expected mid-2018.
- Work Item DTR/ITS-00539 (TR 103 460)
  - Pre-standardisation study on misbehaviour detection
  - Early draft (2017-06-27)
  - Introduces concept of Misbehaviour Broker, collects Misbehaviour reports, distributes CRLs
  - Very early stage, completion date estimation not possible.
- Work Item RTS/ITS-00540 (TS 103 097)
  - Security header and certificate formats Release 2 revision
  - Final draft for approval (2017-06-29), Published 2017-11-06
  - This standard is directly used for the implementation of the SAFERtec use cases
- Work Item RTS/ITS-00541 (TS 102 940)
  - Security architecture and Management
  - Early draft (2017-03-29)
  - Combined with TS 102 941, TS 102 940 deals with Certificate management, CRL, CTL and Security at application layer (contrast to CAM/DENM where security is at network layer). CRL, CTL format is under development. Document under active development, multiple drafts this year. Expected completion date Q1 2018
- Work Item RTS/ITS-00542 (TS 103 096-1)
  - Security PICS
  - TB adoption of WI (2017-04-07)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Work Item RTS/ITS-00543 (TS 103 096-2)
  - Security TSS & TP
  - TB adoption of WI (2017-04-07)
- Work Item RTS/ITS-00544 (TS 103 096-3)
  - Security Testing ATS
  - TB adoption of WI (2017-04-07)
- Work Item DTS/ITS-00545 (TS 103 525-1)
  - ITS PKI PICS
  - TB adoption of WI (2017-04-28)
- Work Item DTS/ITS-00546 (TS 103 525-2)
  - ITS PKI PICS
  - TB adoption of WI (2017-04-28)
- Details of Work Item DTS/ITS-00547 (TS 103 525-3)
  - ITS PKI ATS
  - TB adoption of WI (2017-04-07)
- Work item DTR/ITS-00548 (TR 103 575)
  - Pre-standardisation study on adaptive certificate pre-distribution
  - No draft available yet, work item recently established 2017-09-02
  - Vehicles to send their future pseudonym cert to RSUs in their path.

http://www.etsi.org/standards-search#page=1&search=Intelligent%20Transport%20Systems%20(ITS)&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-07-12&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

(last accessed July 2017).

Use the ETSI search engine with query: “Intelligent Transport Systems (ITS)”.

2.2.3 ITS Standards

The complete list of ETSI ITS standards can be found at the following link:

https://portal.etsi.org/webapp/WorkProgram/Frame_WorkItemList.asp?SearchPage=TRUE&butExpertSearch=++Search++&qETSI_STANDARD_TYPE=&qETSI_NUMBER=&qTB_ID=824%3BCYBER&qTB_ID=607%3BESI&qTB_ID=755%3BISI&qTB_ID=608%3BLI&qTB_ID=160%3BSAGE&qTB_ID=534%3BSCP&qTB_ID=639%3BSCP+REQ&qTB_ID=640%3BSCP+TEC&qTB_ID=714%3BSCP+TEST&qINCLUDE_SUB_TB=True&includeNonActiveTB=FALSE&qWKI_REFERENCE=&qTITLE=&qSCOPE=&qCURRENT_STATE_CODE=&qSTOP_FLG=N&qSTART_CURRENT_STATUS_CODE=0%3BM40&qEND_CURRENT_STATUS_CODE=9+AB%3BN24&qFROM_MIL_DAY=&qFROM_MIL_MONTH=&qFROM_MIL_YEAR=&qTO_MIL_DAY=&qTO_MIL_MONTH=&qTO_MIL_YEAR=&qOPERATOR_TS=&qRAPTR_NAME=&qRAPTR_ORGANISATION=&qKEYWORD_BOOLEAN=OR&qKEYWORD=&qPROJECT_BOOLEAN=OR&qPROJECT_CODE=&includeSubProjectCode=FALSE&qSTF_List=&qDIRECTIVE=&qMandate_List=&qCLUSTER_BOOLEAN=OR&qCLUSTER=&qFREQUENCIES_BOOLEAN=OR&qFREQUENCIES=&qFreqLow=&qFreqLowUnit=1000&qFreqHigh=&qFreqHighUnit=1000&qSORT=HIGHVERSION&qREPORT_TYPE=SUMMARY&optDisplay=10&titleType=all

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

The complete list of standard references and title as of July 2017 is reported in the Appendix 8.1.

The most related standards to the SAFERtec work will be presented in more details in section 3.2.1.

2.3 ISO

2.3.1 Technical Committee: ISO/TC 204 Intelligent transport systems

- Secretariat: ANSI
- Secretary
  - Mr Adrian Guan
- Chairperson (until end 2019)
  - Mr Dick Schnacke
- ISO Technical Programme Manager
  - Mr Andrew Dryden
- ISO Editorial Programme Manager
  - Ms Claudia Lueje

Creation date: 1992

Scope: Standardization of information, communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services in the intelligent transport systems (ITS) field.

ISO / TC 204 is responsible for the overall system aspects and infrastructure aspects of intelligent transport systems (ITS), as well as the coordination of the overall ISO work programme in this field including the schedule for standards development, taking into account the work of existing international standardization bodies.

Excluded from the scope: in-vehicle transport information and control systems (treated by ISO / TC 22).

2.3.2 Technical Committee: ISO/IEC JTC 1/SC 27 IT Security techniques

- ISO/IEC JTC 1/SC 27
  - IT Security techniques
- Secretariat: DIN
  - Secretary: Mrs Krystyna Passia
  - Chairperson (until end 2018): Mr Walter Fumy
  - Vice chairperson (until end 2019): Dr Marijke De Soete
  - ISO Technical Programme Manager: Mme Blandine Garcia
  - ISO Editorial Programme Manager: Mr Bastien Gavoille
- Creation date: 1989
- Scope
  - The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Methodologies to accurately capture security requirements;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

  - SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas

ISO/IEC JTC 1 Information technology: https://www.iso.org/committee/45020.html

2.3.3 Technical Committee: ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

This includes:

- Wiring harness (e.g. cables, connectors, interconnections)
- Dedicated connectors (e.g. trailer connectors, OBD-connector)
- Dedicated E/E components and parts (e.g. alternators, fuses, ignition equipment)
- Electromagnetic compatibility
- Environmental conditions
- Functional safety

2.3.4 Technical Committee: ISO/TC 22/SC 32/WG 11 Cybersecurity

The WG 11 is one of the working group of the sub-committee number 32 (i.e. “Electrical and electronic components and general system aspect”) of the ISO technical committee 22 (i.e., “Road vehicles”). The group is active in the cybersecurity field and in particular it works on the coordination of the standardization activities together with the SAE Vehicle Electrical System Security Committee for Automotive security engineering.

2.4 Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a professional association with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers.

Today, the organization's scope of interest has expanded into so many related fields, that it is simply referred to by the letters I-E-E-E (pronounced Eye-triple-E), except on legal business documents. As of

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

2018, it is the world's largest association of technical professionals with more than 423,000 members in over 160 countries around the world. Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and allied disciplines.

2.4.1 IEEE Vehicular Technology Society

The IEEE Vehicular Technology Society (VTS) was founded in 1949 as the Institute of Radio Engineers' (IRE) Committee on Vehicular and Railroad Radio. The Society's name has changed five times since then and its scope has expanded to include not only the "Radio" of the original name, but all manners of electronics associated with vehicular systems. The Society (then known as the IRE Professional Group on Vehicular Communications) held its first "Meeting" (now Conference) in Detroit in 1950. The Society's first Transactions was published in 1952. Like the Society, the Transactions has carried many names. The Society has approximately 45 local chapters throughout the world.

The fields of interest of the Society are the theoretical, experimental and operational aspects of electrical and electronics engineering in mobile radio, motor vehicles and land transportation. (a) Mobile radio shall include all terrestrial mobile services. (b) Motor vehicles shall include the components and systems and motive power for propulsion and auxiliary functions. (c) Land transportation shall include the components and systems used in both automated and non-automated facets of ground transport technology.

It includes such standardisation activities as, IEEE 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. Which defines Multi-channel wireless radio operations, Wireless Access in Vehicular Environments (WAVE) mode, medium access control (MAC), and physical layers (PHYs), including parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations used in ITS technologies.

2.5 SAFERtec partners contacts and involvement in standardization groups

2.5.1.1 Institute of Communication an Computer Systems

ICCS is not participating in any standardization work related to the project so far.

2.5.1.2 Centro Ricerche Fiat

CRF, on-behalf of FCA (Fiat Chrysler Automobiles), is mainly involved in the cybersecurity working group of the European Automobile Manufacturers' Association (ACEA). The cybersecurity working group recently (i.e., September 2017) published the six ACEA key principles on cybersecurity [ACEA_principles]. Within ACEA, CRF supports such a set of six high-level principles on cybersecurity by:

1) Cultivating a cybersecurity culture in the automotive domain: the cybersecurity culture could be cultivated especially by promoting adequate training and awareness programs within automotive experts and promoting internal working teams on cybersecurity and adopting cybersecurity processes.
2) Adopting a cybersecurity life cycle for vehicle development: the integration of cybersecurity process into the vehicle design and development process is crucial for addressing cybersecurity issues. Hence, roadmaps for cybersecurity contents have to be defined and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

updated constantly and have to involve all aspects of a vehicle production lifecycle: vehicle design, vehicle development, vehicle operation and service/maintenance.

3) Assessing security functions through testing phases: within the implementation of cybersecurity procedures and features, an extensive cybersecurity testing phase is crucial and have to be adopted using penetration testing for critical systems. Automated security tests have to be adopted in particular for high-risk parts of a vehicular system such as parts exposed to known vulnerabilities. While, functional security testing has to be used to assess security functions. Both hardware and software must be tested separately and integrated, as well as the whole vehicle system.
4) Managing a security update policy: since cybersecurity threats evolve, thus cybersecurity procedures, testing tools and methods have to be evolved and updated when needed. In this case, three general requirements have to be consider in the automotive domain: the end-user should be informed if the support for a vehicle or a vehicle component and/or the support for security-fixes comes to an end; in case a fix is not available, a workaround may be applied; a plan for legacy, physical critical security updates should be considered, e.g., when over-the-air updates are not available.
5) Providing incident response and recovery: an incident response plan could be set-up and adopted to ensure that the appropriate response to an incident can take place to allow recovery in case an incident has taken place. The incident response plan, hence, define processes to be adopted for responding to cybersecurity incidents affecting the vehicle. This plan documents the incident response, from its identification and, where applicable, its containment through remediation and recovery. The plan has to be adaptive, built on experience to improve incident response over time.
6) Improving information sharing amongst industry actors: information sharing among multiple industry operators is essential for an effective defence strategy against cyberattacks. Therefore, automotive industries are strongly committed to engaging with public authorities as well as other stakeholders, from every sector of the industry.

The SAFERtec contact for CRF involvement in standardization activities will be Alexandro Marchetto who will be the interface with CRF standardization teams.

2.5.1.3 Cassidian Cybersecurity SAS (AIRBUS Defence and Space)

Cassidian is an ETSI member.

The SAFERtec contact for CCS involvement in standardization activities will be Matthieu Gay and Guillemette Massot who will be the interface with ETSI.

2.5.1.4 University of Piraeus Research Center

UPRC is not participating in any standardization work related to the project so far.

2.5.1.5 Autotalks

Autotalks is an **ETSI** member, mostly active in WG4.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Autotalks participates in **SAE** discussions, in particular related to DSRC profile J2945 and C-V2X profile J3161.

Autotalks is a member of **Car 2 Car Communication Consortium**, in particular active in communication (COM), architecture (ARCH), and security (SEC) working groups, where it provides significant insights about requirements, standards and achievable performance.

Autotalks is active in IEEE802.11NGV working group, which defines the next generation access layer of DSRC (ITS-G5). The most notable activity is co-authoring DSRC vs. C-V2X whitepaper, which gained wide spread market exposure and interest. They are also assisting the Israeli government with the DSRC standardization activity.

The SAFERtec contact for AUT involvement in standardization activities will be Leo Menis who will be the interface with AUT standardization teams.

2.5.1.6 SWARCO MIZAR S.r.l

Swarco is not participating in any standardization work related to the project so far.

2.5.1.7 TOM TOM Development GMBH

TomTom is not participating in any standardization work related to the project so far.

2.5.1.8 COMMSIGNIA KFT

Commsignia has been actively influencing standardization via the **Car 2 Car Communication Consortium**. The group acts as a collaboration ground for OEMs, TIERs, service providers and academia to progress on the deployment of V2X technology. The collective contribution of experts from different companies create whitepapers and other material which is then delivered to various standardization groups (mainly ETSI and ISO). Commsignia is active in the following topics: Communication, Deployment, Architecture, Roadmap, Security and Simulation.

Commsignia plans to become an **ETSI** member in 2018 to gain direct access to draft standards. Misbehaviour detection and Pseudonimity are key topics that could be directly beneficial for the project (as those topics are actively developed currently).

Commsignia provides the chair for Hungary within **ISO TC 204 and CEN 278** and thus monitors all WGs work. It is also possible to interact with the Hungarian expert group for information or voting.

Commsignia also acts as external member or supporter of relevant (V2X) groups within IEEE, SAE and Autosar (https://www.autosar.org/).

The SAFERtec contact for COM involvement in standardization activities will be András Váradi who will be the main and direct interface with most of those standardization bodies.

2.5.1.9 Oppida

Oppida is not currently a standardization body member.

However, Oppida is currently working with Renault in French research project (http://www.irt-systemx.fr/en/project/sca/). Renault is currently Co-chairman of the ETSI ITS WG5 and Oppida can

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

benefit from its contacts within Renault to discuss possible interaction with the ETSI on the ITS security standardization subject.

2.5.1.10 Summary of SAFERtec list of contacts for standardization activities

Partner	e-mail	Abbreviation
Alessandro Marchetto (CRF)	alessandro.marchetto@crf.it	AMA
András Váradi (COMM)	andras.varadi@commsignia.com	AVA
Guillemette Massot (CCS)	guillemette.massot@airbus.com	GMA
Leo Menis (AUT)	leo.menis@auto-talks.com	LME
Matthieu Gay (CCS)	matthieu.gay@airbus.com	MGA
Sammy Haddad (OPP)	sammy.haddad@oppida.fr	SHA

3 Existing standards related to SAFERtec

In this section we present all the standards that the consortium is aware-of to be related to ITS and to the SAFERtec scope. For each of the identified standards we describe how it is related to SAFERtec objectives and WP.

The standards descriptions are for most of them directly extracted from publicly available data (introduction of the standards published on the standardization bodies web pages). For those well known by the partners, additional or more specific information is provided. Partners information are presented as follow:

Specific partners' knowledge on the standard.

The goal here is to have an exhaustive list of standards that both influence the systems developments and the security assurance. Thus, we identify in a first subsection all the standards related to the specification of the ITS. In fact, security is directly related to system functionalities and also partially to interoperability, since poorly interconnected systems often imply lack of security between the different elements of the system.

Then as the project goal is to define an assurance framework, we identify all the ITS standards defining ITS security architectures and mechanisms. Assurance is all about trust. Trust, among other things, is gained by using common and widely recognized references and thus standards.

Finally, the project will study existing general Information Technology (IT) security definition, management and evaluation standards.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

In fact, all the identified standards are both important as project inputs to define the most trustworthy assurance framework and furthermore to serve the purposes of our standardization contribution. By relying as heavily as possible on recognized or emerging standards (ITS and security) our framework will greatly benefit from the current state of the art. Also, the use of standards can significantly accelerate the project work, allowing optimized reuse of already existing knowledge and trust mechanisms.

Within each section we identify all standards known by the SAFERtec consortium or publicly identifiable. For each of these standards, we provide a short description (i.e., mainly their introductions). This will help all the project partners to have a common list of standards, easy to use by everyone regardless of their initial knowledge of the listed standards.

We then tried to identify partners and WPs using the standards and explain why and how they are used. First, we simply identify the WPs to which the standards are related meaning covering partially or completely the standard scope. Subsequently, we describe for each of them more clearly how they related to these WP and if this standard is only an input for the identified WPs work or it can be a possible output, i.e. standardization target for the WPs' results.

Then we have asked every partner of the project to identify if they either know the content (read and worked on it), implement completely or partially that standard, in order to have an internal point of contact when further insights of the standard content is needed. We only mention company names. The intent here is to define an internal SAFERtec contact to get through if further information's are required (regular technical and managerial SAFERtec contacts). Since defining a precise level of a standard knowledge or declaring a full conformity for a specification standard is complicated (and not always achievable), we only required declaration for basic knowledge and existing minimum basic conformity efforts.

This global knowledge base of standards, will be used as a reference of all the standards useful for the project and also as an input for the standardisation plan to identify standardization gaps or standards covering SAFERtec contribution scope.

Thus, for each standard we will try to define the following information:

Content summary

Standard Status

How it is related to SAFERtec:

- **WP or task including the use of the standard**
  - *Simple Task and WP listing*
- **Is the standard an input or possible output of the project?**
  - *Description of the relationship between the identified WPs and tasks with the standard content*
- **Partners implementing or familiar with the standard content**
  - *Identification of companies knowing or using at least partially the standard in order to define contact lists.*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Information about standards in this deliverable are gathered from the partners' knowledge, the standardisation bodies websites and the http://www.itsstandards.eu/ website which aims at referencing all useful standards for ITS systems.

3.1 ITS specifications

The Vehicular V2X subsystems functions comply to the following set of existing standards.

3.1.1 Application layer

3.1.1.1 ISO 13111-1 - General information and use case definitions

Content summary

ISO 13111 Intelligent transport systems (ITS) -- The use of personal ITS station to support ITS service provision for travellers -- Part 1: General information and use case definitions defines the general information and use cases of the applications based on the personal ITS station to provide and maintain ITS services to travellers including drivers, passengers and pedestrians. The ITS applications supported by ISO 13111-1:2017 include multi-modal transportation information service and multimodal navigation service which are based on personal ITS stations in various application scenarios as follows.

- Slow transport information service and navigation service such as pedestrians, bicycles and disabled (wheelchair accessible) navigation, as well as internal traffic navigation inside the local transport area.
- Transfer information service. The considered application environment includes the transfer information service in a transfer node such as the integrated transportation hub, bus stations, car parking lot, an indoor transfer area, etc.
- Multi-modal traffic information service. Types of traffic information include real-time road traffic information, public transport operating information, service information for pedestrians' road network and service information for transfer node such as integrated transportation hub, bus stations, car parking lot, an indoor transfer area, etc.
- Multi-modal navigation service. Includes static and dynamic multi-modal routing and re-routing service, as well as real-time guidance service with voice/image/text/map drawings.
- Communities activities. For example, a team travel when a group of vehicles (or bicycles) track the lead vehicle on the way to the same destination.

Standard Status

- Publication date: 2017-06

WP or task including the use of the standard

- **WP4**
- **WP6**

Is the standard an input or possible output of the project?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This standard is an input for the use case developments and for the knowledge base required for the specification part of functional tests.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia (informative use)
- Autotalks
- Swarco
- CRF

3.1.1.2 ISO 14813-1 - ITS service domains, service groups and services

Content summary

ISO 14813-1:2015 Intelligent transport systems -- Reference model architecture(s) for the ITS sector -- Part 1: ITS service domains, service groups and services provides a description of the primary services that an ITS implementation can provide to ITS users.

Those services with a common purpose can be collected together in "'ITS service domains'" and within these there can be a number of "'ITS service groups'" for particular parts of the domain. This part of ISO 14813 identifies thirteen service domains, within which numerous groups are then defined. In this version of ISO 14813-1:2015 an indication has been provided to show the relationship of each service to Cooperative-ITS. Cooperative-ITS provides services that have previously been unavailable, notably those for ITS users who are on the move. For many other services, Cooperative-ITS can actually be seen as a "delivery mechanism" that can be used to enhance their use and availability.

Thus, for some services, Cooperative-ITS is essential, whilst for others it adds value. However, for a small number of services it is not relevant. ISO 14813-1:2015 is intended for use by at least two groups of people involved in the ITS sector. The first group is those looking for ideas about the services that ITS implementations can provide and the second is for those who are developing standards. For the first group, this part of ISO 14813 provides service descriptions that can act as the catalyst for more detailed descriptions. It is possible for the level of detail to differ from one ITS implementation to another, depending on whether or not a national ITS architecture is involved, and whether this architecture is based directly on services, or on groups of functions. For standards developers, this part of ISO 14813 is applicable to the working groups of ISO TC 204 and other Technical Committees who are developing standards for the ITS sector and associated sectors whose boundaries cross into the ITS sector (such as some aspects of public transport (transit), plus inter-modal freight and fleet management). This part of ISO 14813 is designed to provide information and explanation of services that can form the basis and reason for developing standards. ISO 14813-1:2015 is in itself, by its nature, advisory and informative. It is designed to assist the integration of services into a cohesive reference architecture, plus interoperability and the use of common data definitions. Specifically, services defined within the service groups shall be the basis for definition of 'use cases', 'user needs' or "user service requirements' depending on the methodology being used to develop the resultant ITS architecture functionality, along with definition of applicable data within data dictionaries, as well as applicable communications and data exchange standards.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Standard Status

- Published 2015-10 to be reviewed

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

No specific WP uses this standard. WP4 might use some part of it for the use cases' implementation but it's not mandatory.

No specific contribution to this standard is foreseen.

Partners implementing or familiar with the standard content

- None

3.1.2 Facility layer

3.1.2.1 ETSI TS 103 301 - Facilities layer protocols and communication requirements for infrastructure services

Content summary

Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services presents the specification of the infrastructure service. The infrastructure services are application support facilities provided by the Facilities layer that construct, manage and process messages distributed from infrastructure to end-users or vice-versa based on payload received from the application. The infrastructure services specified in the present document support infrastructure-based applications in order to achieve communication interoperability, and may be implemented in parallel to other services in an ITS-S.

The present document provides specifications of infrastructure related to ITS services aiming to support communication between ITS infrastructure equipment and traffic participants (e.g. vehicles, pedestrians). It defines services in the Facilities layer for communication between the infrastructure and traffic participants. The specifications cover the protocol handling for infrastructure-related messages as well as requirements to lower layer protocols and to the security entity.

It is related to ISO/TS 19321:2015 since it also defines the data types and format to be exchanged in the ITS infrastructure. It often use the ISO specification for some specific data format (e.g. *iviIdentifcationNumber, DE Provider, etc.)*.

Standard Status

- Published, publication date 2016-11

WP or task including the use of the standard

- WP2
- WP4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines some of the data exchanged which need to be protected in ITS communications.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco
- CRF

3.1.2.2 ETSI EN 302 637-2 - Specification of Cooperative Awareness Basic Service

Content summary

ETSI EN 302 637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications (BSA); Part 2: Specification of Cooperative Awareness Basic Service provides the specifications of the Cooperative Awareness basic service (CA basic service), which is in support of the BSA road safety application.

This includes definition of the syntax and semantics of the Cooperative Awareness Message (CAM) and detailed specifications on the message handling.

Cooperative awareness within road traffic means that road users and roadside infrastructure are informed about each other's position, dynamics and attributes. Road users are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians and roadside infrastructure equipment including road signs, traffic lights or barriers and gates. The awareness of each other is the basis for several road safety and traffic efficiency applications with many use cases as described in ETSI TR 102 638. It is achieved by regular exchange of information among vehicles (V2V, in general all kind of road users) and between vehicles and road side infrastructure (V2I and I2V) based on wireless networks, called V2X network and as such is part of Intelligent Transport Systems (ITS). The information to be exchanged for cooperative awareness is packed up in the periodically transmitted Cooperative Awareness Message (CAM).

CAM messages include e.g.: stationType, referencePosition, performanceClass, heading, speed, vehicleRole, lanePosition, driveDirection, longitudinalAcceleration, accelerationControl, lateralAcceleration, verticalAcceleration.

The construction, management and processing of CAMs is done by the Cooperative Awareness basic service (CA basic service), which is part of the facilities layer within the ITS communication architecture ETSI EN 302 665 supporting several ITS applications. The CA basic service is a mandatory facility for all kind of ITS-Stations (ITS-S) which take part in the road traffic (vehicle ITS-S, personal ITS-S, etc.). ETSI EN 302 637-2 focuses on the specifications for CAMs transmitted by all vehicle ITS-Ss participating in the V2X network. Nevertheless, this document defines the CAM format with flexibility in order to be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

easily extendable for the support of other types of ITS-Ss or future ITS applications. The requirements on the performance of the CA basic service, the content of the CAM and the quality of its data elements are derived from the Basic Set of Applications (BSA) as defined in ETSI TR 102 638 and in particular from the road safety applications as defined in ETSI TS 101 539-1 [i.8], ETSI TS 101 539-2, and ETSI TS 101 539-3.

Standard Status

- Published 2014-11

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines the CAM messages that are part of the messages that will be exchanged in our use cases.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco (currently using v1.3.1 (Published 2014-09) soon to be update soon to v1.3.2 (2014-11))
- CRF

3.1.2.3 ETSI EN 302 637-3 – Specifications of Decentralized Environmental Notification Basic Service

Content summary

Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service provides specification of the DEN basic service, which is in support of the RHW application. More specifically, the present document specifies the syntax and semantics of the "Decentralized Environmental Notification Message" (DENM) and the DENM protocol handling.

The DEN basic service may be implemented in a vehicle ITS-S, a road side ITS-S, a personal ITS-S or a central ITS-S.

ITS use cases are distributed over multiple instances of ITS stations (ITS-S). ITS-Ss interact in the ITS networks to provide a large diversity of co-operating customer services that satisfy different types of functional and operational requirements. ETSI TC ITS has defined a "Basic Set of Applications" (BSA) in ETSI TR 102 638 [i.1] that can be deployed within a three-year time frame after the completion of their standardization. In BSA, the Road Hazard Warning (RHW) application is composed of multiple use

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

cases with the objective to improve road safety and traffic efficiency using vehicle-to-vehicle and vehicle-to-infrastructure communication technologies. ETSI TC ITS defines the decentralized environmental notification (DEN) basic service that supports the RHW application. The DEN basic service is an application-support facility provided by the facilities layer. It constructs, manages and processes the Decentralized Environmental Notification Message (DENM). The construction of a DENM is triggered by an ITS-S application. A DENM contains information related to a road hazard or an abnormal traffic conditions, such as its type and its position. The DEN basic service delivers the DENM as payload to the ITS networking & transport layer for the message dissemination. Typically for an ITS application, a DENM is disseminated to ITS-Ss that are located in a geographic area through direct vehicle-to-vehicle or vehicle-to-infrastructure communications. At the receiving side, the DEN basic service of a receiving ITS-S processes the received DENM and provides the DENM content to an ITS-S application. This ITS-S application may present the information to the driver if information of the road hazard or traffic condition is assessed to be relevant to the driver. The driver is then able to take appropriate actions to react to the situation accordingly.

Example of DENM messages are: elevanceDistance, relevanceTrafficDirection, roadType, roadWorks, speedLimit, startingPointSpeedLimit, stationaryCause, stationarySince, stationaryVehicle, stationType, termination, traces, trafficFlowRule, transmissionInterval, turningRadius, etc.

Standard Status

- Published 2014-11

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines the DENM messages that are part of the messages that will be exchanged in our use cases.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco (currently using v1.2.1 (Published 2014-09) soon be updated to v1.2.2 (2014-11))
- CRF

3.1.2.4 ETSI TS 102 894-2 - Applications and facilities layer common data dictionary

Content summary

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary defines basic data sets to be exchanged by ITS stations.

ITS applications are enabled by the data exchanges among ITS stations (ITS-S) via wireless or wired communications. A basic set of application has been defined by ETSI TC ITS. Accordingly, a set of higher layer messages and communication protocols have been specified in support of this application set. Even though each message has specific requirements on the data being included and transmitted to other ITS-Ss, ETSI TC ITS has identified a set of data types which are commonly used in multiple ITS applications and facilities layer messages. A common data dictionary is therefore defined for this common set. For each data type, this common dictionary includes a textual description of the semantic of the data type in question. It also includes the ASN.1 definition of the data type. Therefore, this common data dictionary can be imported by any message when necessary during the encoding and decoding procedure.

The aforementioned document defines a repository of a set of data elements and data element sets, denoted as data frames, that are commonly used in the ITS applications and facilities layer messages. Each data element is defined with a set of attributes, enabling the identification of the data element in question in a number of perspectives, e.g. descriptive name, ASN.1 definition, data definition, minimum data granularity requirement, etc. The document focuses on the data elements being used by the Cooperative Awareness basic service as outlined in ETSI EN 302 637-2 (Cooperative Awareness Message (CAM)) and by the Decentralized Environmental Notification basic service as outlined in ETSI EN 302 637-3 (Decentralized Environmental Notification Message (DENM)). The present document does not specify the syntax and requirements of data elements in the specific context of any message. It defines the data dictionary structure.

Standard Status

- Published 2014-09

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines the data base to store messages like CAM and DENM messages that are the main part of the messages that will be exchanged in our use cases.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco
- CRF

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.1.2.5 ETSI EN 302 895 - Basic Set of Applications; Local Dynamic Map (LDM)

Content summary

ETSI EN 302 895 V1.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM) defines functional behaviour associated with a Local Dynamic Map (LDM) for usage in an ITS station unit (ITS-SU). It specifies functions and interfaces supported by a LDM. These functions and interfaces provide secure access to the LDM to manage LDM data objects stored in a LDM. It defines LDM data objects for safety-related and Vehicle to Vehicle (V2V)-related applications.

Standard Status

- Published 2014-09

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 as one of the main ITS function developed.

Partners implementing or familiar with the standard content

- Commsignia (partial support / use)
- Autotalks
- CRF

3.1.2.6 ETSI TR 103 061-1 - CAM validation report

Content summary

ETSI TR 103 061-1 V1.2.1 Intelligent Transport Systems (ITS); Testing; Part 1: Conformance test specifications for Co-operative Awareness Messages (CAM); CAM validation report presents the validation report of the CAM conformance tests derived from EN 302 637-2. It provides statistics of executed and validated CAM conformance tests. The information provided has been produced by validation against at least two prototype implementations from industry.

Standard Status

- Published 2015-09

WP or task including the use of the standard

- WP4

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 to define functional tests. Even if the standard is stable some feedback of the project could be pushed into the standard if need be.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.1.2.7 ETSI TR 103 061- DENM validation report

Content summary

Testing; Part 2: Conformance test specifications for Decentralized Environmental Notification basic service Messages (DENM); DENM validation report

Standard Status

- Published 2014-04

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 to define functional tests. Even if the standard is stable some feedback of the project could be pushed into the standard if need be.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.1.2.8 CEN ISO TS 19091 - Using V2I and I2V communications for applications related to signalized intersections

Content summary

CEN ISO/TS 19091:2017 Intelligent transport systems - Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections defines the message, data structures, and data elements to support exchanges between the roadside equipment and vehicles to address applications to improve safety, mobility and environmental efficiency. In order to verify that the defined messages will satisfy these applications, a system engineering process has been employed that traces use cases to requirements and requirements to messages and data concepts. This document contains the base specification and a series of annexes. The base specification lists the derived information requirements (labelled informative) and references to other standards for message definitions where available. Annex A contains descriptions of the use cases addressed by this document. Annex B and Annex C contain traceability matrices that relate use cases to requirements and requirements to the message definitions (i.e. data frames and data elements). The next annexes list the base message requirements and application-oriented specific requirements (requirements for a traceability matrix) that map to the message and data concepts to be implemented. As such, an implementation consists of the base plus an additional group of extensions within this document. Details on information requirements, for other than SPaT, MAP, SSM, and SRM messages are provided in other International Standards. The focus of this document is to specify the details of the SPaT, MAP, SSM, and SRM supporting the use cases defined in this document. Adoption of these messages varies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

by region and their adoption may occur over a significant time period. This document covers the interface between roadside equipment and vehicles. Applications, their internal algorithms, and the logical distribution of application functionality over any specific system architecture are outside the scope of this document.

Standard Status

- Published 2017-03

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines some of the data exchanged format. Those data need to be protected in ITS communications (integrity and proof of origin).

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.1.2.9 ISO TS 19321 - Dictionary of in-vehicle information (IVI) data structures

Content summary

ISO/TS 19321:2015 specifies the in-vehicle information (IVI) data structures that are required by different ITS services (for example, refer to ISO/TS 17425 and ISO/TS 17426) for exchanging information between ITS Stations. A general, extensible data structure is specified (see Clause 5). This is split into structures called containers to accommodate current-day information (see Clause 6). Transmitted information includes IVI such as contextual speed, road works warnings, vehicle restrictions, lane restrictions, road hazards warnings, location-based services, re-routing, etc. The information in the containers is organized in sub-structures called data frames and data elements which are described in terms of its content and its syntax.

The data structures are specified as communications agnostic. This Technical Specification does not provide the communication protocols. This Technical Specification then provides scenarios for usage of the data structure, e.g. in case of real time, short-range communications.

Standard Status

- Published, publication date 2015-04

WP or task including the use of the standard

- WP2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis. It defines some of the data exchanged format. Those data need to be protected in ITS communications (integrity and proof of origin).

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco
- CRF

3.1.2.10 SAE J2945/1- On-Board System Requirements for V2V Safety Communications

Content summary

SAE J2945/1 On-Board System Requirements for V2V Safety Communications specifies the system requirements for an on-board vehicle-to-vehicle (V2V) safety communications system for light vehicles, including standards profiles, functional requirements, and performance requirements. The system is capable of transmitting and receiving the Society of Automotive Engineers (SAE) J2735-defined Basic Safety Message (BSM) over a Dedicated Short Range Communications (DSRC) wireless communications link as defined in the Institute of Electrical and Electronics Engineers (IEEE) 1609 suite and IEEE 802.11 standards.

Standard Status

- Published 2016-03-30

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This standard is out of scope since it defines North American ITS messages standards. SAFERtec should only take into account European standard, and here the ETSI equivalent CAM and DENM.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.1.3 Network layer

3.1.3.1 ETSI EN 302 636-4-1 – Vehicular Communications; GeoNetworking - Media-Independent Functionality

Content summary

ETSI EN 302 636-4-1 – Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality specifies the media-independent functionality of the GeoNetworking protocol.

The GeoNetworking protocol is a network layer protocol that provides packet routing in an ad hoc network. It makes use of geographical positions for packet transport. GeoNetworking supports the communication among individual ITS stations as well as the distribution of packets in geographical areas. GeoNetworking can be executed over different ITS access technologies for short-range wireless technologies, such as ITS-G5 and infrared. The ITS access technologies for short-range wireless technologies have many technical commonalities, but also differences. In order to reuse the GeoNetworking protocol specification for multiple ITS access technologies, the specification is separated into media-independent and media-dependent functionalities. Media-independent functionalities are those which are common to all ITS access technologies for short-range wireless communication to be used for GeoNetworking. The media-dependent functionalities extend the media-independent functionality for a specific ITS access technology. Therefore, the GeoNetworking protocol specification consists of the standard for media-independent functionality and at least one standard for media-dependent functionality. However, it should be noted that the media-dependent extensions do not represent distinct protocol entities.

Standard Status

- Published, 2017-08

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco

3.1.3.2 ETSI EN 302 636-5-1 - GeoNetworking - Requirements

Content summary

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI EN 302 636-1 V1.2.1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements specifies, at an abstract level, the general, functional and performance requirements that apply to the GeoNetworking protocols (EN 302 636-4, EN 302 636-5 and EN 302 636-6) for use in ETSI ITS G5 access technology (EN 302 663). The present document is applicable to ITS stations implementing ETSI ITS G5 access technology (EN 302 663) and the GeoNetworking protocols (EN 302 636-4, EN 302 636-5 and EN 302 636-6) for both single hop and multi-hop communications.

Wireless communication is a cornerstone of future Intelligent Transport Systems (ITS). Many ITS applications require the dissemination of information with a rapid and direct communication, which can be achieved by ad hoc networking. GeoNetworking is a network-layer protocol for mobile ad hoc communication based on wireless technology, such as ITS-G5. It provides communication in mobile environments without the need for a coordinating infrastructure. GeoNetworking utilizes geographical positions for dissemination of information and transport of data packets. It offers communication over multiple wireless hops, where nodes in the network forward data packets on behalf of each other to extend the communication range. Originally proposed for general mobile ad hoc networks, variants of GeoNetworking have been proposed for other network types, such as vehicular ad hoc networks (VANETs), mesh networks and wireless sensor networks. Therefore, GeoNetworking can also be regarded as a family of network protocols based on the usage of geographical positions for addressing and transport of data packets in different types of networks. In VANETs, GeoNetworking provides wireless communication among vehicles and among vehicles and fixed stations along the roads. GeoNetworking works connectionless and fully distributed based on ad hoc network concepts, with intermittent or even without infrastructure access. The principles of GeoNetworking meet the specific requirements of vehicular environments: It is well suited for highly mobile network nodes and frequent changes in the network topology. Moreover, GeoNetworking flexibly supports heterogeneous application requirements, including applications for road safety, traffic efficiency and infotainment. More specifically, it enables periodic transmission of safety status messages at high rate, rapid multi-hop dissemination of packets in geographical regions for emergency warnings, and unicast packet transport for Internet applications. GeoNetworking basically provides two, strongly coupled functions: geographical addressing and geographical forwarding. Unlike addressing in conventional networks, in which a node has a communication name linked to its identity (e.g. a node's IP address), GeoNetworking can send data packets to a node by its position or to multiple nodes in a geographical region. For forwarding, GeoNetworking assumes that every node has a partial view of the network topology in its vicinity and that every packet carries a geographical address, such as the geographical position or geographical area as the destination. When a node receives a data packet, it compares the geo-address in the data packet and the node's view on the network topology and makes an autonomous forwarding decision. As a result, packets are forwarded "on the fly", without need for setup and maintenance of routing tables in the nodes. The most innovative method for distribution of information enabled by geographical routing is to target messages to certain geographical areas. In practise, a vehicle can select and specify a well-delimited geographic area to which messages should be delivered. Intermediate vehicles serve as message relays and only the vehicles located within the target area process the message and further send it to corresponding applications. In this way, only vehicles that are actually affected by a dangerous situation or a traffic notification are notified, whereas vehicles unaffected by the event are not targeted.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Standard Status

- Published, 2014-04

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco

3.1.3.3 ISO 21217 - Architecture

Content summary

ISO 21217:2014 Intelligent transport systems -- Communications access for land mobiles (CALM) – Architecture describes the communications reference architecture of nodes called "ITS station units" designed for deployment in intelligent transport systems (ITS) communication networks. The ITS station reference architecture is described in an abstract way. While ISO 21217:2014 describes a number of ITS station elements, whether or not a particular element is implemented in an ITS station unit depends on the specific communication requirements of the implementation.

ISO 21217:2014 also describes the various communication modes for peer-to-peer communications over various networks between ITS communication nodes. These nodes may be ITS station units as described in ISO 21217:2014 or any other reachable nodes.

ISO 21217:2014 specifies the minimum set of normative requirements for a physical instantiation of the ITS station based on the principles of a bounded secured managed domain.

Standard Status

- Published 2014-04

WP or task including the use of the standard

- **WP2**
- **WP4**

Is the standard an input or possible output of the project?

It is an input for the use case specification and risk analysis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Partners implementing or familiar with the standard content

- Commsignia (informative)

3.1.4 Access layer

3.1.4.1 ETSI EN 302 571 -Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band

Content summary

ETSI EN 302 571 V2.1.1 Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5855 MHz to 5925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU specifies technical characteristics and methods of measurement for radio transmitters and receivers operating in the frequency range 5855 MHz to 5925 MHz. The spectrum usage conditions are set out in ECC Decision (08)01 for the frequency range 5875 MHz to 5925 MHz (with 5905 MHz to 5925 MHz considered as a future ITS extension) and in ECC Recommendation (08)01 for the frequency range 5 855 MHz to 5 875 MHz. The Commission Decision 2008/671/EC mandates a harmonised use of the frequency band 5875 MHz to 5905 MHz dedicated to safety-related applications of ITS throughout the member states of the European Union.

Standard Status

- Published, (2017-02)

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Autotalks (major contributor)
- Swarco
- CRF

3.1.4.2 ETSI EN 302 663 - Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band

Content summary

ETSI EN 302 663 V1.2.1 Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band defines the two lowest layers, physical layer and the data link layer, grouped into the access layer of the ITS station reference architecture EN 302 665. The access layer technology that is specified in the document is collectively called ITS-G5. It is

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

part of the communication stack supporting data exchange between mobile stations without prior network set-up, i.e. ad hoc mode, for the following frequency bands in Europe:

- ITS-G5A: Operation of ITS-G5 in European ITS frequency bands dedicated to ITS for safety related applications in the frequency range 5,875 GHz to 5,905 GHz.
- ITS-G5B: Operation in European IT S frequency bands dedicated to ITS non-safety applications in the frequency range 5,855 GHz to 5,875 GHz.
- ITS-G5D: Operation of ITS applications in the frequency range 5,905 GHz to 5,925 GHz.

The ITS-G5 technology is based on IEEE 802.11-2012 and IEEE/ISO/IEC 8802-2-1998. By setting the MIB variable dot11OCBActivated to true in IEEE 802.11-2012 [3] communication outside the context of a BSS is possible. This type of communication allows for immediate exchange of data frames, avoiding the management overhead used with the establishment of a network. All requirements in IEEE 802.11-2012 associated with communication "outside the context of a BSS" are also requirements in the document. All optional functionality in IEEE 802.11-2012 associated with communication "outside the context of a BSS" is also optional in the present document.

This standard outlines the two lowest layers - physical layer and data link layer - in the protocol stack for supporting vehicle-to-vehicle communications in an ad hoc network to be used at the 5,9 GHz frequency band allocated in Europe. The two lowest layers are termed access layer in the present document and the technology specified for the access layer is collectively called ITS-G5. The ITS-G5 standard is using already existing standards for communications. The data link layer is divided into two sublayers; medium access control and logical link control. The physical layer and the medium access control layer are covered in IEEE 802.11-2012 (cf. 3.1.4.3). The logical link control is based on the IEEE/ISO/IEC 8802-2-1998. The ITS-G5 standard also adds features for decentralized congestion control (DCC) methods TS 102 687 to control the network load and avoid unstable behaviour. By setting the management information base (MIB) parameter dot11OCBActivated to true in IEEE 802.11-2012 a new capability is introduced namely the possibility to communicate outside the context of a basic service set (BSS), which is the smallest building block of a 802.11 network. Communication outside the BSS implies that neither authentication/association procedures nor security mechanisms are supported. Further, no access point functionality is present. The disable of these features also affects other built-in features of IEEE 802.11-2012. The requirement that nodes should share a common clock is no longer valid while dot11OCBActivated is true. Further, scanning of available frequency channels for joining a BSS is also disabled implying that communication outside the context of the BSS requires that a node is configured for a predetermined frequency channel where more information about other available frequency channels can be obtained.

IEEE has compiled a new version of the 802.11 standard where all approved amendments produced between 2007 and 2011 have been enrolled in the base standard including 802.11p. This new version called IEEE 802.11-2012 was approved in March 2012. Due to this new version of 802.11 the 802. 11p amendment is classified as superseded.

Standard Status

- Published, (2013-07)

WP or task including the use of the standard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco
- CRF

3.1.4.3 IEEE 802.11p - Wireless Access in Vehicular Environment

Content summary

IEEE 802.11p Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements - Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environment defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure, so called V2X communication, in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard based on the IEEE 802.11. It is also the base of a European standard for vehicular communication known as ETSI ITS-G5.

As the communication link between the vehicles and the roadside infrastructure might exist for only a short amount of time, the IEEE 802.11p amendment defines a way to exchange data through that link without the need to establish a basic service set (BSS), and thus, without the need to wait for the association and authentication procedures to complete before exchanging data. For that purpose, IEEE 802.11p enabled stations use the wildcard BSSID (a value of all 1s) in the header of the frames they exchange and may start sending and receiving data frames as soon as they arrive on the communication channel.

Because such stations are neither associated nor authenticated, the authentication and data confidentiality mechanisms provided by the IEEE 802.11 standard (and its amendments) cannot be used. These kinds of functionality must then be provided by higher network layers.

Standard Status

- Published, 2010

WP or task including the use of the standard

- WP2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks (major contributor to the next generation of this standard, code named 802.11px)
- Swarco
- CRF

3.1.4.4 IEEE 802.11- Wireless Local Area Networks

Content summary

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the marketplace, each revision tends to become its own standard.

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. 802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n, 802.11ac and upcoming 802.11ax. Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which may also include corrections to a previous specification.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the U.S. Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signalling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band offering only three non-overlapping channels, where other adjacent channels overlap—see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment. 802.11n can use either the 2.4 GHz or the 5 GHz band; 802.11ac uses only the 5 GHz band.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Standard Status

- Published 2016

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco

3.1.4.5 SAE J2735 - Dedicated Short Range Communications (DSRC)

Content summary

J2735-2016 Dedicated Short Range Communications (DSRC) Message Set Dictionary and J2945 On-Board System Requirements for V2V Safety Communications give the foundations for V2X communication within the US region (out of scope for the project).

This SAE Standard specifies a message set, and its data frames and data elements specifically for use by applications intended to utilize the 5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, referenced in this document simply as "DSRC"), communications systems. Although the scope of this Standard is focused on DSRC, this message set, and its data frames and data elements have been designed, to the extent possible, to be of potential use for applications that may be deployed in conjunction with other wireless communications technologies. This Standard therefore specifies the definitive message structure and provides sufficient background information to allow readers to properly interpret the message definitions from the point of view of an application developer implementing the messages according to the DSRC Standards.

Standard Status

- Published 2006-12-19 (latest revision 2016-03-30)

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This standard is out of scope since it defines North American communication standards. SAFERtec should only take into account European standard, and here the ETSI equivalent 302 571.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.1.4.6 SAE J2945 -Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts

Content summary

This SAE Standard serves as the guidance document for the J2945/x family of standards as illustrated. It contains cross-cutting material which applies to the other J2945/x standards, including recommended practice for the use of Systems Engineering (SE) and generic DSRC interface requirements content. The scope for the DSRC system environment is to provide for the information exchange between a host vehicle and another DSRC enabled device, a device worn by or otherwise attached to a traveller, a roadside device, or a management center, to address safety, mobility, and environmental system needs. The audience for this document includes the technical teams of developers of the J2945/x documents and the implementers of the applications which are based on the J2945/x documents.

Standard Status

- Published 2017-12-07

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This standard is out of scope since it defines North American communication standards. SAFERtec should only take into account European standard, and here the ETSI equivalent 302 571.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.1.4.7 IEEE 1609.2 - Security Services for Applications and Management Messages

Content summary

1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The IEEE 1609 standard family describes secure communication for the US region, which is out of scope for the implementation and the use cases. However, the 1609.2 should be mentioned as a standard that is being partially used and referenced by the European (ETSI) standards.

Standard Status

- Published 2016

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This standard is out of scope since it defines North American communication standards. SAFERtec should only take into account European standard, and here the ETSI equivalent 103 097.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks

3.1.5 Functional safety

3.1.5.1 IEC 61784 - Industrial communication networks – Profiles

Content summary

The standard consists of 36 documents that define a set of protocol specific communication profiles based primarily on the IEC 61158 series, to be used in the design of devices involved in communications in factory manufacturing and process control.

IEC 61784 with reference to IEC 61508 decomposes its safety functions and provides recommendations to achieve certain (overall) SIL levels with communication channels being part of the system.

This part of IEC 6 1784 provides a set of Communication Profiles (CP) in the sense of ISO/IEC TR 10000 -1. These answer the need of identifying the protocol families co- existing within the IEC 6 1158 series, as a result of the international harmonization of fieldbus technologies available on the market. More specifically, these profiles help to correctly state the compliance to the IEC 6 1158 series, and to avoid the spreading of divergent implementations, which would limit its use, clearness and understanding. Additional profiles to address specific market concerns, such as functional safety or information security, may be addressed by future parts of this standard. This standard contains several Communication Profile Families (CPF), which specify one or more communication profiles. Such profiles identify, in a strict sense, protocol subsets of the IEC 6 1158 series via protocol specific communication profiles. They do not define device- type -specific communication profiles for the purpose of guiding manufacturers in feature set selection – for example, in selecting the minimum set of communication services and protocol to implement a specific class of devices, such as generic slaves or transmitters ("implementation profiles"). Neither do they define device profiles that specify communication profiles together with application functions needed to answer the need of a specific

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

application ("application profiles"). It is agreed that these latter classes of profiles would help the use of the IEC 6 1158 series of standards; the profiles defined in this document are a necessary step to achieve that task. It is also important to clarify that interoperability – defined as the ability of two or more network systems to exchange information and to make mutual use of the information that has been exchanged (see 3.2.1 of ISO/IEC TR 10000- 1) – can be directly achieved on the same link only for those devices complying to the same communication profile. Profiles contained in this International Standard are constructed of references to IEC 6 1158 -2 and the IEC 6 115 8- 3, IEC 6 1158- 4, IEC 6 1158 -5 and IEC 6 1158 -6 series, and other IS, TS or worldwide -accepted standards, as appropriate. Each profile is required to reference at least one (sub)part of IEC 6 1158 -2 through IEC 6 1158 -6. Two or more Profiles, which are related to a common family, are specified within a "Communication Profile Family" (CPF).

Standard Status

- Published 2014-08

WP or task including the use of the standard

- WP2
- WP4

Is the standard an input or possible output of the project?

It's mainly an input for the use cases development. But it is also an input for the architecture definition in the risk analysis.

There is no objective for the project to update it.

Partners implementing or familiar with the standard content

- Autotalks
- CRF

3.1.5.2 ISO 26262 Road vehicles -- Functional safety

Content summary

ISO 26262-1:2011 Road vehicles -- Functional safety is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

Standard Status

- Published 2011-11

WP or task including the use of the standard

- WP3

Is the standard an input or possible output of the project?

This standard could be used as an input for the definition of the SAFERtec assurance framework. In fact, this standard is widely used in the automotive world to enforce high safety development standards. Many of the product lifecycle management process defined to enforce safety could be used or adapted to also fit in our security assurance framework. This process reuse could greatly enhance the ease to adopt our solution and lower its cost.

However, regarding the standardization plan, it is not plan to provide inputs for this standard.

Partners implementing or familiar with the standard content

- CRF
- Autotalks

3.2 ITS security

3.2.1 ETSI

3.2.1.1 ETSI TS 102 731 - Security Services and Architecture

Content summary

Intelligent Transport Systems (ITS); Security; Security Services and Architecture V1.1.1 has been developed between 2008 and 2010. It specifies mechanisms at the stage 2 level defined by ETSI 300 387 for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization. The mechanisms are specified as stage 2 security services according to the 3 stages method described in ETSI 300 387 and identify the functional entities and the information flow between them. The stage 2 security services will be refined into a number of security protocol s as part of the stage 3 specifications. There may be several security protocols able to fulfil the requirements of a security services. The present document describes the stage 2 security architecture of the ETSI Intelligent Transport System (ITS). The stage 2 security architecture and security services shall be used as the basis for further developing the ITS security architecture by mapping the security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

services and its functional components to the ITS architecture. This mapping is part of stage 3 specifications.

Standard Status

- Published, 2010-09

WP or task including the use of the standard

- WP3
- WP4
- WP5
- WP6

Is the standard an input or possible output of the project?

The use case will not imply the full use of the architecture defined in this standard. ITS-S will already be enrolled and no PKI will be deployed to handle all the Enrolment Credential, Authorization Ticket, Security Association, Remote management or Report Misbehaving ITS-S services. Nevertheless, it will use: single message, Integrity, Replay protection, Accountability, Plausibility.

This common standard (among many topics) deals with the process of reporting misbehaviour to the ITS infrastructure. Therefore, it might be a long-term target for the project for re-opening if found relevant for input.

SAFERtec use cases do not imply the use of misbehaviour detection. Thus, it is not an input but potential output of the project regarding the feedback gained on running attacks on the use cases. Also, it will be the base for test plan development since it defines many aspects of the security functions that will be deployed.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco
- CRF

3.2.1.2 ETSI TR 102 893 - TVRA

Content summary

ETSI TR 102 893 v1.2.1 Intelligent transport systems (ITS): Threat, Vulnerability and Risk Analysis (TVRA) of 5.9 GHz radio communication in an Intelligent Transport System (ITS) defines the process used to identify risks to a system by isolating and identifying the set of vulnerabilities of the system, assessing the likelihood of a malicious attack on each vulnerability and determining the impact that an attack will have on the system.

The proposed method process consists of the following main steps:

- Identification of the Target of Evaluation (TOE): it could be a single ITS station such as a vehicle or a roadside unit that are part of a more complex vehicle-centric system;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Identification of the objectives of the TVRA: a set of security aims and issues to be considered and solved;
- Identification of the functional security requirement, derived from the defined objective;
- Inventory and specification of the TOE main assets: relevant assets could be both functional elements (e.g., communication protocol control, ITS applications, on-board/roadside sensor monitor, vehicle control) and data elements (e.g., Local Dynamic Map, data resulting from received messaged such as CAMs/DEMNs messages, local vehicle information);
- Identification and classification (according to a set of aspects specified in the ETSI TR 102 893) of vulnerabilities of the ITS vehicular system, as well as threats that can exploit them, and the unwanted potential incidents;
- Quantifying the occurrence likelihood and impact of the threats;
- Establishment of the risks;
- Identification of conceptual countermeasures, a list of alternative security services and capabilities helpful to reduce the identified risk: the evaluation of potential ITS security countermeasure allows to identify the security mechanisms and services required to protect the system against the known security threats. Two main countermeasure strategies can be identified: asset redesign and asset hardening (e.g., enrich specification);
- Countermeasure cost-benefit analysis to identify the best fit security services and capabilities;
- Specification of detailed requirements for the security services and capabilities.

ETSI TR 102 893 defines the following set of high-level ITS security objectives: *Confidentiality*, *Integrity*, *Availability*, *Accountability* and *Authenticity*.
For each objective, moreover, a set of sub-objectives and functional security requirements are identified and described. For instance, the following **Erreur ! Source du renvoi introuvable.** lists objectives and requirements for the *Integrity*. The table shows that, e.g., the information used and exchanged by an ITS vehicle has to be protected from unauthorized access and modification (objective In1), this objective implies that only authorized access and use have to be allowed for security parameters, LDM information, and service profiles (Functional Security Requirements related to objective In1). Similar tables have been defined for all the other high-level objectives (i.e., *Confidentiality*, *Availability*, *Accountability,* and *Authenticity*).

Table 2: High-level objective and functional security requirements

Objective		Functional Security Requirements
ID	**Text**	
In1	Information held within an ITS-S should be protected from unauthorized modification and deletion	An ITS-S should permit only authorized ITS applications to modify or delete its security parameter and LDM Information
		An ITS-S should permit only authorized ITS applications and authorized ITS users to modify or delete Service profile information
In2	Information sent to or from an registered ITS user should be protected against unauthorized or	An ITS-S should implement one or more methods to enable it, if requested by an ITS user, to detect end route modification or manipulation of received data

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	malicious modification or manipulation during transmission	An ITS-S should implement one or more methods for preventing the modification or manipulation of data that it transmits or receives
In3	Management Information held within a ITS-S should be protected from unauthorized modification and destruction	The functional security requirements specified for objective In1 satisfy the needs of objective In3
In4	Management Information sent to or from an ITS-S should be protected against unauthorized or malicious modification or manipulation during transmission	The functional security requirements specified for objective In2 satisfy the needs of objective In4

ETSI TR 102 893 reports sets of examples of known vulnerabilities and threats concerning 5.9 GHz communication-based systems that can affect vehicles and roadside units. The following reports examples of such identified vulnerabilities for an ITS vehicle TOE with details on the concerned problem, the weakness of the system, and possible threat agents exploiting the vulnerabilities. **Erreur ! Source du renvoi introuvable.** For instance, the message saturation (Threat) concerns the broadcasting nature of V2X messages (ITS Problem Area) and tries to take advantage of the potential difficulties of V2X-based systems in processing large and continuous streams of messages (Weakness). According to, this threat could be exploited by malware agents installed in the vehicle environment (Threat Agent). Similarly, the replication of "expired" messages (Treat) concerns the uncertainness in the message timestamp management (ITS Problem Area) and tries to take advance of the difficulties of vehicles in verifying the validation of received messages (Weakness); this threat could be exploited by corrupted ITS vehicle or stations having the capability of sending messages with "expired"/old information (Threat Agent).

ID	Threat	ITS Problem Area	Weaknesses	Threat Agent
V-V1	Message saturation	Intrinsic high density of ITS message traffic due to broadcasting and beaconing in V2V systems	The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages or fabricated queue entries could: (1) cause it to miss important incoming ITS messages (2) cause it to delay or miss the sending of outgoing ITS messages or relaying of incoming ITS messages (3) leave it with no resources free for other essential tasks such as monitoring sensors and updating driver-displays (4) leave it with no resources free for other essential tasks	Malware installed on target ITS-S (Vehicle) filling the incoming message queue with spurious but valid messages Malicious ITS-S broadcasting a high level of ITS message traffic

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

			such as monitoring sensors and updating driver-displays	
V-V6	- Replay of "expired" messages - GNSS spoofing	Uncertainty regarding how timestamps are created and how to use them to check the validity of messages	An ITS-S (Vehicle) is unable to validate when or where a received message was originally generated	Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending "expired" information in ITS messages that are otherwise valid Equipment posing as a genuine ITS-S (Vehicle) or as an RSU sending information in ITS messages that are valid except for the source location

Table 3: Example of vulnerabilities for ITS vehicle TOE

According to the identified and characterized vulnerabilities and threats, examples of potential effects, i.e., when such vulnerabilities and threats are exploited by an attacker, are also described and characterized in the ETSI TR 102 893. The following **Erreur ! Source du renvoi introuvable.** reports examples of possible consequences of threats with details about the threat groups, the system weakness, possible consequences for each threat, and the impacted ITS security objectives. For instance, by exploiting the message saturation threat (Threat Type) an attacker could compromise the correct sharing of collision warnings (Undesirable Consequences), thus impacting the Availability security objective (Impacted ITS Security Objective). Again, by exploiting the message reply threat (Threat Type) an attacker could compromise traffic management applications (Undesirable Consequences), thus impacting the Integrity security objective (Impacted ITS Security Objective).

Threat Group	Threat Type	Weakness	Undesirable Consequences	Impacted ITS Security Objective
Denial of access to incoming messages	- Message saturation - Injection of false messages	An ITS-S (Vehicle) is unable to quickly determine whether a received message is valid and from a legitimate user and acts on information received in the message The time taken by an ITS-S (Vehicle) to process a high volume of real or spurious messages could cause it to miss important incoming ITS messages	Accidents if collision warnings are not received and processed by the attacked ITS-S (Vehicle) General compromise of traffic management applications which depend on the reliable and timely receipt of ITS messages	Availability
Modification and deletion of stored information	- Message replay - GNSS spoofing	An ITS-S (Vehicle) is unable to validate when a received message was originally generated	General compromise of traffic management applications which depend on the LDM for accurate and up-to-date information	Integrity

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

		The contents of the LDM can be incorrectly modified by received messages containing false time, position or status information or by maliciously planted software		

Table 4 Example of vulnerability consequence for an ITS vehicle TOE

By considering the identified vulnerabilities, threats and their potential consequences a risk analysis is also documented in the ETSI TR 102 893. The following table (Table 5 Example of risk analysis output) reports an example of an output of a risk analysis for two groups of threats with details characterizing different aspects regarding the attack, potential impact of the attack and the risk, according to factors and scales described in the ETSI TR 102 893 and other referenced ETSI standards. For instance, **Erreur ! Source du renvoi introuvable.** shows that threats concerning the modification and deletion of stored information (Threat Group) could be exploited with a limited likelihood (Attach Likelihood: level 2) and require a limited amount of time (Attach Range <= 1 week) but high expertise (Attack Factor – Expertise: level Expert) to be exploited; these threat however could have a high impact (Impact level 3) and lead to critical risks (Risk level 6).

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
Denial of access to incoming messages	Time	<= 1 week	1	11 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Easy	1				
	Equipment	Specialized	3				
Modification and deletion of stored information	Time	<= 1 week	1	14 (Moderate)	2 (Possible)	3 (High)	6 (Critical)
	Expertise	Expert	5				
	Knowledge	Restricted	1				
	Opportunity	Moderate	4				
	Equipment	Specialized	3				

Table 5 Example of risk analysis output

Standard Status

- Published 2017-03

WP or task including the use of the standard

- WP2
- WP6

Is the standard an input or possible output of the project?

This standard is mainly used in the WP2 for the risk analysis of use cases. It is used as a reference to be updated by the project. It will also be used by the WP6 to define the knowledge base as it already identifies many ITS threats and countermeasures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Partners implementing or familiar with the standard content

- CCS
- UPRC
- Oppida
- ICCS
- CRF
- Swarco
- Autotalks

3.2.1.3 ETSI TS 102 940 - ITS communications security architecture and security management

Content summary

ETSI TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731, it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665. The document also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.

Standard Status

- Last published 2016-11
- Drafting stage
  - Final draft for approval (2018-03-03)
  - Next Status: TB approval (2018-04-13)

WP or task including the use of the standard

- WP2
- WP4
- WP6

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 for the specification of the security architecture and functions. This standard is used together with ETSI TS 102 731, thus it will be the base for test plan development since it defines many aspects of the security functions that will be deployed.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- Swarco

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- CRF

3.2.1.4 ETSI TS 103 097 - Security header and certificate formats

Content summary

ETSI TS 103 097 V1.2.1 Intelligent Transport Systems (ITS); Security; Security header and certificate formats defines different aspects of the security applied to the V2X messages exchanged between the OBU and the RSU via V2X communication in the use cases.

It specifies security header and certificate formats for Intelligent Transport Systems. These formats are defined specifically for securing G5 communication.

Standard Status

- Stopped (2015-04-17)

WP or task including the use of the standard

- WP4
- WP6

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 for security implementation. It will also be the base for test plan development since it defines many aspects of the security functions that will be deployed. WP6 might also use it in its reference data base as security format recommendations.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.2.1.5 ETSI TS 102 941 - Trust and Privacy Management

Content summary

ETSI TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management defines rules for Pseudonymity. The vehicle subsystem uses its short-term certificates and protects its identity (replaces its IDs) in conformance to this standard.

It specifies the trust and privacy management for Intelligent Transport System (ITS) communications. Based upon the security services defined in TS 102 731 and the security architecture defined in TS 102 940, it identifies the trust establishment and privacy management required to support security in a ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in EN 302 665.

The present document identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in an Intelligent Transport System (ITS). Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Standard Status

- Drafting Stage
- Current Status: Final draft for approval (2018-03-16)
- Next Status: WG approval (2018-04-10)

Is the standard an input or possible output of the project?

This standard is mainly used in the WP4 for security implementation.

It will also be the base for test plan development since it defines many aspects of the security functions that will be deployed.

Partners implementing or familiar with the standard content

- Commsignia
- Autotalks
- CRF

3.2.1.6 ETSI TR 103 415 - Pseudonym change strategies

Pre-standardisation study on pseudonym change management. Literature survey of pseudonym change considerations and strategies with recommendations. Under development, expected in mid-2018. This standard indirectly influences the project as it gives guidance on the pseudonym change happening within a vehicle which is in relation to the privacy level realized. The vehicles will apply a pseudonym change strategy aligned with this draft standard.

Standard Status

- Early draft 2017-05-10
- Current Status: WG approval (2018-03-15)
- Next Status: TB approval (2018-06-02)

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This standard could be an output of the project if we manage to get feedback on pseudonym change strategy impact on safety and security in the use cases and in the test phase.

Partners implementing or familiar with the standard content

- Commsignia (informative, due to draft stage)
- CRF

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

3.2.2 ISO

3.2.2.1 ISO/CD TR 17427-5 - Cooperative ITS - Part 5: Common approaches to security

Content summary

Intelligent transport systems -- Cooperative ITS -- Part 5: Common approaches to security, the future content of this standard is not yet known.

Standard Status

- Under development

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

This standard could be a good candidate to participate to. But it is very difficult for the consortium to be able to influence ISO standards underdevelopment.

Partners implementing or familiar with the standard content

- None

3.2.2.2 ISO/NP TR 12859 - Privacy aspects in ITS standards and systems

Content summary

ISO/NP TR 12859 Intelligent transport systems -- System architecture -- Privacy aspects in ITS standards and systems gives general guidelines to developers of intelligent transport systems (ITS) standards and systems on data privacy aspects and associated legislative requirements for the development and revision of ITS standards and systems.

This deliverable is currently requesting to be accepted. If granted it will work on an update of the Technical Report to give general guidelines to developers of Intelligent Transport Systems (ITS) and relevant standards on data privacy aspects and associated legislative requirements. It is based on the EU-Regulation GPDR 2016/679 coming into force at 25 May 2018.

Standard Status

- Under review

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

The project could provide some feedback to this standard's authors. But it will be difficult for SAFERtec consortium to be able to contribute.

Partners implementing or familiar with the standard content

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- None

3.2.2.3 ISO 24100 - The basic principles for probe personal data protection

Content summary

ISO 24100:2010 - Privacy — The basic principles for probe personal data protection states the basic rules to be observed by service providers who handle personal data in probe vehicle information services. This International Standard is aimed at protecting the personal data as well as the intrinsic rights and interests of probe data senders, i.e., owners and drivers of vehicles fitted with in-vehicle probe systems.

A probe data collector is a party that is responsible for receiving probe messages sent by a probe data sender, where probe data are vehicle sensor information formatted as probe data elements and/or probe messages that are processed, formatted and transmitted to a land-based centre for processing to create a good understanding of the driving environment.

Standard Status

- Under review

WP or task including the use of the standard

- WP2
- WP4
- WP6

Is the standard an input or possible output of the project?

This standard is both an input and possible output of the project. It will be used as an input for use cases developments. This standard should be used to correctly implement privacy issues at service level.

Partners implementing or familiar with the standard content

- TOMTOM

3.2.2.4 ISO/IEC 17021 Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements

Content summary

ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems.

Certification bodies operating to ISO/IEC 17021-1:2015 do not need to offer all types of management system certification.

Certification of management systems is a third-party conformity assessment activity and bodies performing this activity are therefore third-party conformity assessment bodies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Certification of a management system provides independent demonstration that the management system of the organization:

- conforms to specified requirements;
- is capable of consistently achieving its stated policy and objectives;
- is effectively implemented.

Conformity assessment, such as the certification of a management system, thereby provides value to the organization, its customers and interested parties.

Certification activities involve the audit of an organization's management system. The form of attestation of conformity of an organization's management system to a specific management system standard or other normative requirements is usually a certification document or a certificate.

This standard is to be used together with to ISO/IEC 17021-7 with is further dedicated to road traffic safety management.

Standard Status

- Published 2015-06

WP or task including the use of the standard

- WP3

Is the standard an input or possible output of the project?

This is an input for WP3 and the definition of the SAF, especially the AOC. It provides information for any possible conformity assessment activities.

Partners implementing or familiar with the standard content

- None

3.2.2.5 ISO/IEC TS 17021-7 Competence requirements for auditing and certification of road traffic safety management systems

Content summary

ISO/IEC TS 17021-7:2014 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 7: Competence requirements for auditing and certification of road traffic safety management systems complements the existing requirements of ISO/IEC 17021:2011. It includes specific competence requirements for personnel involved in the certification process for road traffic safety (RTS) management systems.

ISO 39001 provides a tool to help organizations reduce, and ultimately eliminate, the incidence and risk of death and serious injury related to road traffic crashes and promotes the Safe System approach. Certification to ISO 39001 is one way of demonstrating that a systematic approach to road traffic safety (RTS) management has been taken.
RTS management system certification personnel need to have the generic competencies described in ISO/IEC 17021:2011, as well as the specific RTS management system competencies described in this Technical Specification.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This Technical Specification complements ISO/IEC 17021:2011. In particular, it clarifies the requirements for the competence of personnel involved in the certification process set out in ISO/IEC 17021:2011, Annex A.

The guiding principles in ISO/IEC 17021:2011, Clause 4, are the basis for the requirements in this Technical Specification.

Certification bodies have a responsibility to interested parties, including their clients and the customers of the organizations whose management systems are certified, to ensure that RTS certification is credible by only using certification personnel that have demonstrated relevant competence.

Standard Status

- Published 2014-10

WP or task including the use of the standard

- WP3

Is the standard an input or possible output of the project?

This could be an input for WP3 and the definition of the SAF, especially the AOC. It provides information for any possible conformity assessment activities even if this standard is probably not IT and cyber-security oriented but more regular physical safety oriented. But it could still be an interesting state of the art input to include safety management in SAF.

A survey is proposed to provide input to the current review process.

https://www.surveymonkey.com/s/B23RCVG

Partners implementing or familiar with the standard content

- None

3.2.2.6 ISO/IEC 2700X - Information technology — Security techniques — Information security management systems (ISMS)

Content summary

This is a complete set of standards that defines how to manage IT security at the system level. It is a generic but well detailed set of requirements and procedures to put in place to enhance security in any IT systems.

The ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary provides an overview of information security management systems and defines related terms. Thus, it describes the global approached covered by the IOS 200X standard, together with the specific scope and function of each of them. It covers the following topics:

- Definition of an Information Security Management System (ISMS);
- Purposes and principles of the ISMS;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- The importance of ISMS / Information Security to organizations;
- Strategic definitions of how to establish, monitor, deploy and improve their ISMS;
- Critical success factors for adoption of the ISMS / information security in organizations;
- Benefits in using a standardized approach / standardized to an ISMS;
- How the 27K family of standards are related

An Information Security Management System consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused upon normative standards describing ISMS requirements (ISO/IEC 27001), certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001, and additional requirement framework for sector-specific implementations of the ISMS (ISO/IEC 27009). Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance. Relationships between the ISMS family of standards are illustrated in the figure bellow.

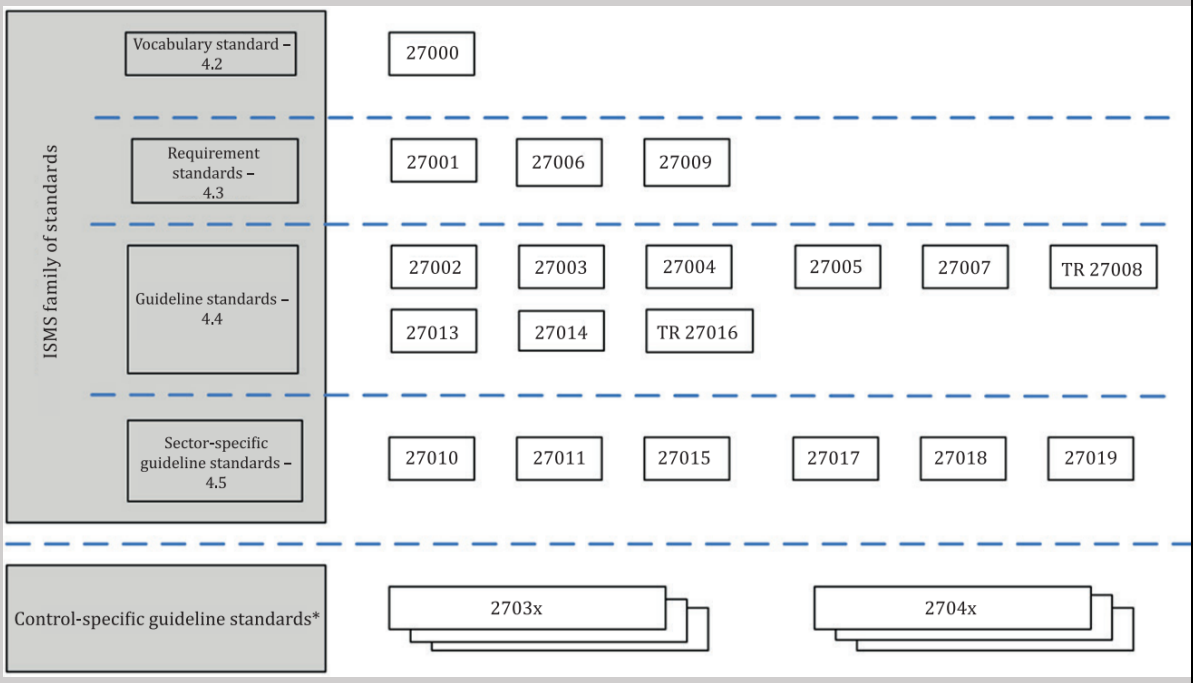

Figure 1: Relationships between the ISMS family of standards

All the sector specific standards (27009, 27010, 27011, 27015, 27017, 27018, 27019) are out of scope of SAFERtec tropic.

Here we focus on 27001 and 27006 requirements and their associated guidance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ISO/IEC 27001 Information technology— Security techniques— Information security management systems— Requirements specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of information security controls customized to the needs of individual organizations or parts thereof. This International Standard can be used by all organizations, regardless of type, size and nature.

ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from ISO/IEC 27001, Annex A shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in ISO/IEC 27001, Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002, Clauses 5 to 18.

ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. This standard specifies requirements and provides guidance for bodies providing audit and ISMS certification in accordance with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 17021. It is primarily intended to support the accreditation of certification bodies providing ISMS certification according to ISO/IEC 27001. Purpose: ISO/IEC 27006 supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001.

In SAFERtec we do not plan to have accredited ISMS bodies. Thus, we only focus on ISO/IEC 27001 and the corresponding standardized guidelines (ISO/IEC 27002-5).

ISO 27001 requirements are grouped in the following sections:

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Examples of the requirement are:

Leadership and commitment Top management shall demonstrate leadership and commitment with respect to the information security management system by:
a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b) ensuring the integration of the information security management system requirements into the organization's processes;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

[…]

Most of the categories defined in the 27001 are oriented towards security management at system and company level. Thus, they do not relate directly to technical measures as we aim at in SAFERtec. Nevertheless, some requirements are more security implementation oriented and can be good inputs for the definition of the assurance framework, such as:

Information security risk treatment
The organization shall define and apply an information security risk treatment process to:
a) select appropriate information security risk treatment options, taking account of the risk assessment results;
b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
[…]
Information security objectives and planning to achieve them
The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:
a) be consistent with the information security policy;
b) be measurable (if practicable);
c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
[…]
Monitoring, measurement, analysis and evaluation
The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:
a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
NOTE The methods selected should produce comparable and reproducible results to be considered valid.
c) when the monitoring and measuring shall be performed; d) who shall monitor and measure;
[…]

The ISO 2700X family then provides the corresponding security measure of reference to be implemented to fulfil those requirements.

The most interesting ones regarding SAFERtec objectives are the ISO27002 and the ISO 27005.

ISO 27002 provides measures for13 different topics, including the following that are part of the most relevant to us:

- Asset management
  - Responsibility for assets
  - Information classification
  - Media handling
- Access control
  - User access management

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

  - User responsibilities
  - System and application access control
- Cryptography
- Operational security
  - Operational procedures and responsibilities
  - Logging and monitoring
  - Control of operational software
  - Technical vulnerability management

The measures are still high level but are useful to us in order to define the SAF and more specifically to define security functional requirement for the different parts of the system, e.g.:

Classify information and assets in terms of value, criticality and sensitivity.
[…]
Implement procedures to manage the use of removable media.
[…]
Restrict and control allocation and use of privileged access rights.
[…]
Restrict access to information and applications based on access control policy
[…]

The ISO 27005 provides guidelines for information security risk management. It is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security. It details the different steps of the risk management process illustrated in the following figure.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

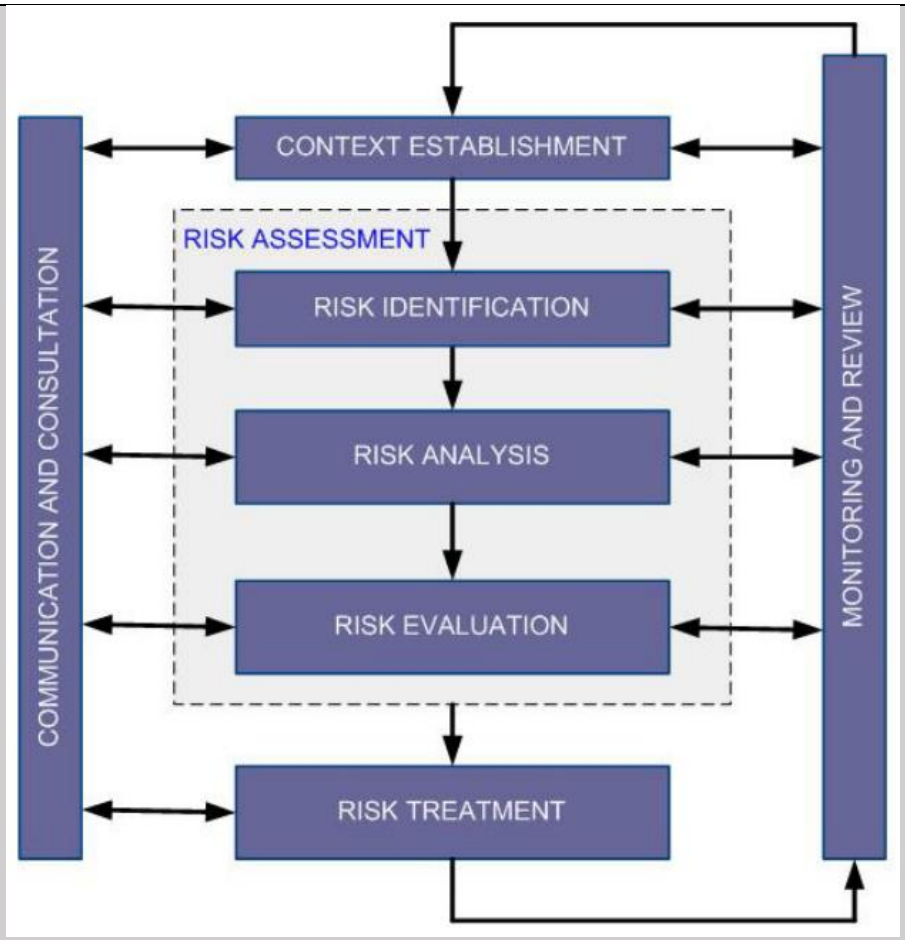

Figure 2: ISO 27005 Risk management process

The EBIOS risk analysis method used in WP2 is conformant to ISO27005.

Standard Status

- All standards are published

WP or task including the use of the standard

- WP2
- WP3

Is the standard an input or possible output of the project?

In SAFERtec, we are looking for more dedicated and product-oriented assurance approaches. But nevertheless, at system level, these are very interesting references. Those standards are direct inputs for WP2 & 3.

Partners implementing or familiar with the standard content

- Oppida
- CCS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- CRF

3.2.3 SAE

3.2.3.1 ISO/SAE AWI 21434 - Cybersecurity engineering

Content summary

ISO/SAE AWI 21434 Road Vehicles -- Cybersecurity engineering is currently under development.

This document specifies requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design and development), production, operation, maintenance, and decommissioning. A framework is defined that includes requirements for cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders. This document is applicable to road vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications. This document does not prescribe specific technology or solutions related to cybersecurity.

It should be decomposed in 4 parts:

- Risk Management
- Product Development
- Operation, Maintenance and other Processes
- Process Overview and Interdependencies

So far, the content is not known to us but the topic of the standard is clearly in the scope of SAFERtec.

Standard Status

- Under development, preparatory

WP or task including the use of the standard

- None

Is the standard an input or possible output of the project?

It could be a good output for the project regarding its scope. The SAF could be included in the scope of the standard to define an evaluation method for the components identified as critical, in either the product development or Operation, maintenance and other processes

Partners implementing or familiar with the standard content

- None

3.2.3.2 SAE J3061- Guidebook for Cyber-Physical Vehicle Systems

Content summary

SAE Cybersecurity Guidebook for Cyber-Physical Vehicle Systems – it represents a guidebook with high-level recommendations concerning the cybersecurity of cyber-physical automotive systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

SAE J3061 cybersecurity guidebook provides a set of high-level cybersecurity principles for cyber-physical automotive systems within the whole process development and maintenance lifecycle. This includes:

- defining a high-level framework for the whole process lifecycle of automotive systems that take into account relevant cybersecurity aspects;
- providing information on usable methods and tools used for designing and validating automotive systems;
- providing basic guidelines and principle to follow for automotive systems;
- providing the foundation for further standards development activities in vehicle cybersecurity.

This guidebook provides a complete lifecycle process framework that has to be tailored to a company-specific process. The presented framework is analogous, and inspired to, the process framework described in ISO 26262 Functional Safety Road Vehicles.

The guidebook suggests that for cybersecurity-critical vehicle systems an initial (short) assessment of threats and an initial estimation of risks have to be done. Then, in case this assessment indicates that high risk safety-related threats may exist, a cybersecurity process has to be (fully) applied. Generally speaking, the J3061 guidebook recommends that a cybersecurity process can be applied for all automotive systems that provide/use functions that are Automotive Safety Integrity Level (ASIL) rated to ISO 26262 or, in any case, if they are managing functions associated with the vehicle: propulsion, braking, steering, security and safety.

While the system safety is the state of a system that does not cause harm to life, property, or environment, the system cybersecurity is the state of a system that does not allow exploitation of vulnerabilities to lead to losses, e.g., related to finance, operational, privacy, or safety. All safety-critical systems are hence security-critical (i.e., a cyber-attack on a safety-critical system could potentially lead to safety losses), instead not all security-critical systems are safety-critical, i.e. entertainment system. System safety considers (by means of Fault Tree Analysis) potential hazards to identify safety mechanisms; instead, system cybersecurity considers (by means of Attack Tree Analysis) potential threats and vulnerabilities.

Guiding principles listed by J3061 are the following:

- Know your system's cybersecurity risks;
- Understand key cybersecurity principles;
- Consider vehicle owners' use of system;
- Implement cybersecurity in concept and design phases;
- Implement cybersecurity in development and validation;
- Implement cybersecurity in incident response;
- Cybersecurity considerations at end of the system's life-time.

J3061 also describes the cybersecurity process by covering all aspects of the process lifecycle of an automotive system. One key aspect is that, like for system safety, cybersecurity should be built in to the system rather than added on at the end of development: hence all phases of the automotive system lifecycle have to be considered. For instance, the J3061 covers:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- The concept phase: where the development of a cybersecurity program plan as to be defined. The Threat Analysis and Risk Assessment (TARA) activity could help to assess potential threats to the system and determine the risk associated with each threat;
- The product development phase: where different levels of activities have to be considered iteratively, by respectively considering the whole system, the adopted hardware and software;
- The production and operation/service phase: where cybersecurity aspects related to activities related to the product operation and service, i.e., maintenance and repair activities after the production, have to be considered;
- The supporting phase: where activities such as configuration management, documentation management, change management, management of cybersecurity requirements are considered.

In the whole process, the J3061 guidebook suggests to define review points (called gates) aiming at ensuring that appropriate activities have been performed and completed correctly and consistently before the next step of development begins.

Finally, the J3061 also reports about examples of security analysis techniques adopted in specific project, such as the following:

- E-Safety Vehicle Intrusion Protected Applications (EVITA) program;
- Threat, Vulnerabilities, and implementation Risks Analysis (TVRA) method;
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method;
- HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS) method and attack tree information.

In summary, the J3061 guidebook aims mainly at:

- creating, fostering and sustaining a cybersecurity culture for automotive systems;
- establishing methods to help ensure compliance to an adopted cybersecurity engineering process
- identifying and establishing the needed communication channels with respect to cybersecurity;
- incorporating a field monitoring process that includes, e.g., monitoring hacker-related media articles, reporting un/successful attacks;
- incorporating an incident response process that includes an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

Standard Status

- Publication date: January 2016

The J3061 SAE team is discussing potential joint work with ISO teams to define a global standard based on J3061

WP or task including the use of the standard

- WP2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Is the standard an input or possible output of the project?

This standard is an input for the definition of the SAF. This standard is recognized by the automotive industry and is a first proposition on how to integrate cyber-security in the product development life cycle and integrate it in the safety processes. This standard only defines self-assessment of cyber-security. The level of assurance gained by such processes is of course lesser than independent evaluation or review. Typically, the trust provided by external independent experts is at least equal and generally greater than pure self-assessment with no external validation of this assessment. But in the process developed by this standard, when identified as critical the element could be developed following their procedure, self-evaluated also and once ready be evaluated via the SAF to provide high level of confidence.

Partners implementing or familiar with the standard content

- CRF
- Autotalks

3.3 Security evaluation

3.3.1 ETSI

3.3.1.1 ETSI GS ISI 003 - Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection

Content summary

ETSI GS ISI 003 V1.1.2 Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection defines and describes a set of Key Performance Security Indicators (KPSI) to be used for the evaluation of the performance, the maturity levels of the detection tools and processes used within organizations for security assurance. The response is not included in the scope of the present document. In particular, the purpose of the present document is to enable organizations to:

- assess the overall maturity level of the security event detection;
- provide a reckoning formula to assess detection levels of major security events as summarized in GS ISI 001-1 [1];
- evaluate the results of measurements.

This work is mainly based on the US SANS CAG. The target groups of the present document are Head of detection, reaction teams, Cyber defence team and head of security governance.

Standard Status

- Published 2014-06

WP or task including the use of the standard

- WP3

Is the standard an input or possible output of the project?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

This standard is an input for the KPSI definition. It can also be an output of this same activity even if the scope of the standard is different of ITS and clearly regular enterprise IT oriented.

Partners implementing or familiar with the standard content

- Oppida

3.3.2 ISO

3.3.2.1 ISO/IEC AWI 15408 - Evaluation criteria for IT security

Content summary (D3.1 extract)

The Common Criteria for Information Technology Security Evaluation, commonly named more simply Common Criteria (CC) is an internationally used evaluation framework. It is defined and maintained by an international community. The latest version of the documents defining the CC together with other documents defining the level of international recognition, supporting documents for the methodology application on specific cases or the list of certified product or testing laboratories can be found on the common criteria portal (www.commoncriteriaportal.org).

The CC are decomposed in three parts each corresponding to one document:

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements

The first part is an introductory document that defines all the CC vocabulary and the different roles and interest for the different participant of an evaluation.

The most important concepts defined or redefined by the CC are:

- The Target of the Evaluation (TOE): the product or the system to be evaluated.
- The Security Target (ST): the document specifying TOE and the evaluation tasks.
- Protection Profiles (PP): Generic ST defining only evaluation tasks for a generic type of product.
- The Security Functional Requirements (SFR): the specification of the security functions that the TOE must implement.
- The TOE Security Functionality (TSF): the part of the TOE where the SFR are implemented.
- The TSF Interfaces (TSFI): the interfaces used by the users to interact with the TSF.

Also, the document defines the different actors and their roles in the evaluation.

The second part presents a standardized common set of Security Functional Requirements (SFR), i.e. a formalization of the most common security function, e.g.:

- Security audit data generation
- Non-repudiation of origin
- Cryptographic key management
- Access control policy
- Information flow control policy
- Rollback
- User authentication
- Anonymity

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Fail secure

As for the ITSEC, those security functions are presented and classified within 11 classes:

- CLASS FAU: SECURITY AUDIT
- CLASS FCO: COMMUNICATION
- CLASS FCS: CRYPTOGRAPHIC SUPPORT
- CLASS FDP: USER DATA PROTECTION
- CLASS FIA: IDENTIFICATION AND AUTHENTICATION
- CLASS FMT: SECURITY MANAGEMENT
- CLASS FPR: PRIVACY
- CLASS FPT: PROTECTION OF THE TSF
- CLASS FRU: RESOURCE UTILISATION
- CLASS FTP: TRUSTED PATH/CHANNELS

The part 2 also defines how to structure and write one of the most important documents of an evaluation, the Security Target (ST). Again, this central document will define, what is the product and in which precise version has to be or had been evaluated and for which function. The particularity of the CC is that all the evaluation process will consist in providing proofs to validate the SFR in the product. To do that, all the documents provided by the developer will have to trace the correct implementation of the SFR at the different level of the product life cycle and conception. Thus, all or most of the documents provided must clearly identify this traceability and thus make references to these SFR. This is one of the reasons why, evidences provided for the evaluation are dedicated to the evaluation and are usually not the regular documentation (i.e., product specifications, product architecture, user guides, etc.) produced by the developer.

Finally, the third and last part of the CC presents the evaluation tasks to be done to evaluate the product. The tasks are presented in this general way: description of the goal of the task, its dependencies with other evaluation tasks, evidence requirements for the developer, evaluation activities to be done by the evaluator. Different levels are presented for each task. At the end of the document they are combined to form seven Evaluation Assurance Level (EAL), EAL 1 to EAL7, each of them increasing the level of requirements and verification to be done on the TOE and evidences provided by the developer.

The CC defines 8 assurance classes, decomposed each in several assurance families.

Each assurance class is assigned a unique name. The name indicates the topics covered by the assurance class.

- PROTECTION PROFILE EVALUATION (APE)
- SECURITY TARGET EVALUATION (ASE)
- LIFE-CYCLE SUPPORT (ALC)
  - Life-cycle definition (ALC_LCD)
  - Development security (ALC_DVS)
  - Configuration Management capabilities (ALC_CMC)
  - Configuration Management scope (ALC_CMS)
  - Delivery (ALC_DEL)
  - Flaw remediation (ALC_FLR)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Tools and techniques (ALC_TAT)
- DEVELOPMENT (ADV)
  - Security Architecture (ADV_ARC)
  - Functional specification (ADV_FSP)
  - TOE design (ADV_TDS)
  - Security policy modelling (ADV_SPM)
  - Implementation representation (ADV_IMP)
  - TSF internals (ADV_INT)
- GUIDANCE DOCUMENTS (AGD)
  - Preparative procedures (AGD_PRE)
  - Operational user guidance (AGD_OPE)
- TESTS (ATE)
  - Functional tests (ATE_FUN)
  - Coverage (ATE_COV)
  - Independent testing (ATE_IND)
- VULNERABILITY ASSESSMENT (AVA)
- COMPOSITION (ACO)

Standard Status

- To be revised

WP or task including the use of the standard

- WP3
- WP5
- WP6

Is the standard an input or possible output of the project?

It is a direct input for the SAF.

Partners implementing or familiar with the standard content

- Oppida
- Autotalks

3.3.2.2 ISO/IEC AWI 18045 Methodology for IT security evaluation (CEM)

Content summary

Information technology -- Security techniques -- Methodology for IT security evaluation (CEM) is a companion document to ISO/IEC 15408, Information technology - Security techniques - Evaluation criteria for IT security. ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. ISO/IEC 18045:2008 does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Standard Status

- To be revised

WP or task including the use of the standard

- WP3
- WP5
- WP6

Is the standard an input or possible output of the project?

It is a direct input for the SAF.

Partners implementing or familiar with the standard content

- Oppida
- Autotalks

3.3.2.3 ISO/IEC TR 15443 - Security assurance framework

Content summary

ISO/IEC TR 15443-1:2012 Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts defines terms and establishes an extensive and organised set of concepts and their relationships for understanding IT security assurance, thereby establishing a basis for shared understanding of the concepts and principles central to ISO/IEC TR 15443 across its user communities. It provides information fundamental to users of ISO/IEC TR 15443-2.ISO/IEC TR 15443-2:2012

Thus, among other things it defines the word assurance, which is the cornerstone of SAFERtec objectives:

> **assurance**
>
> **grounds for justified confidence that a claim has been or will be achieved**
> **[SOURCE: SOURCE: ISO/IEC TR 15026-1:2010, definition 2.1]**
> **<ISO/IEC 15408>** grounds for justified confidence that a TOE meets the SFRs
> **[SOURCE: SOURCE: ISO/IEC 15408-1:2009, definition 3.1.4]**
> **[…]**
>
> **security assurance**
>
> **grounds for justified confidence that a claim about meeting security objectives has been or will be achieved**
> **[SOURCE: SOURCE: Adapted from ISO/IEC 15026-1:2010, definition 2.1]**
> **[…]**

ISO/IEC TR 15443-2:2012 Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis builds on the concepts presented in ISO/IEC TR 15443-1. It provides a discussion of the attributes of security assurance conformity assessment methods that contribute

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

towards making assurance claims and providing assurance evidence to fulfil meeting the assurance requirements for a deliverable.

ISO/IEC TR 15443-2:2012 proposes criteria for comparing and analysing different SACA methods. The reader is cautioned that the methods used as examples in ISO/IEC TR 15443-2:2012 are considered to represent popularly used methods at the time of its writing. New methods may appear, and modification or withdrawal of the methods cited may occur. It is intended that the criteria can be used to describe and compare any SACA method whatever its provenance.

Standard Status

- Published 2012-11

WP or task including the use of the standard

- WP3

Is the standard an input or possible output of the project?

It is a direct input for the SAF.

Partners implementing or familiar with the standard content

- None

3.3.2.4 ISO/IEC 27032 - Guidelines for cybersecurity

Content summary

ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security,
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

Standard Status

- Published 2012-07

WP or task including the use of the standard

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- None

Is the standard an input or possible output of the project?

This standard could be an input for the SAF definition, but it is not so far, ISO 15408 and SAE J3061 are the main inputs so far.

Partners implementing or familiar with the standard content

- None

4 Standardization plan

In this section we define the standardization plan of the project. For that, we first identify from the state of the art, the lack of standards, regarding our assurance framework and define for those gaps if the project has relevant results to push to standardization. Then we identify existing standards that could be enhanced or updated thanks to SAFERtec results.

Finally, we define a strategic plan based on these observations to define action points to push SAFERtec results towards standardization.

4.1 ITS assurance security standardization gaps

In Table 6Table 6: Standardization gaps to be addressed by SAFERtec, we recall the different assurance activities that we aim to do in our assurance framework and identify if there are existing standards on the matter and identify if they are sufficient. Then we identify if it is possible for the project to contribute to the standardization state of the art by proposing to a standardization body to standardize the project results on the matter.

So, we currently identify three possible targets regarding missing standards. For each of this opportunity we try to roughly estimate the extra efforts required to transform, adapt and complete the project results into standards on a scale Low (0 to 3 PMs), medium (3 to 6 PMs) and high (more than 6 PMs) and the likelihood to manage to create or participle to a working group to define this new standard on a scale unlikely, possible, likely.

- **Protection Profiles**
  - Content input
    - D2.4 and D3.2
  - Standardization body to be addressed
    - ETSI / ISO
  - Extra efforts to go from deliverables to standards:
    - Low
  - Likelihood
    - ETSI
      - likely
    - ISO
      - Unlikely
- **Conformity tests**
  - Content input
    - D3.2 and D6.2
  - Standardization body to be addressed
    - ETSI / ISO
  - Extra efforts to go from deliverables to standards:
    - Medium
  - Likelihood
    - ETSI
      - Possible
    - ISO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

        - Unlikely
- **Vulnerability tests**
    - Content input
        - D3.2 and D6.2
    - Standardization body to be addressed
        - ETSI / ISO
    - Extra efforts to go from deliverables to standards:
        - Low
    - Likelihood
        - ETSI
            - Unlikely
        - ISO
            - Unlikely

4.2 Existing ITS and ITS security related standards to update

In Table 7 we identify standards used by the project that could be update or enhanced thanks to SAFERtec work.

In this table we identify the following standards:

- ETSI TR 102 893 - TVRA
    - Standard Status
        - Published 2017-03
    - Partner involved in the standardization body and partners to support the standard
        - CCS, Autotalks, Oppida, UPRC
    - Efforts to provide inputs
        - Low
    - Likelihood
        - Possible
- ETSI TR 103 415 - Pseudonym change strategies
    - Standard Status
        - Early draft 2017-05-10
    - Partner involved in the standardization body and partners to support the standard
        - Commsignia, Autotalks, Oppida
    - Efforts to provide inputs
        - Low
    - Likelihood
        - Unlikely

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Assurance activity related standards	Assurance framework definition	ALC	APE/ASE	ADV	ATE	AVA	AOP
Developer activities (inputs)	N/A	DIN EN 50159 ISO 26262 ISO 2700X ISO/SAE AWI 21434 SAE J3061	CEN ISO TS 19091 ETSI EN 302 636-4 ETSI EN 302 637 ETSI EN 302 895 ETSI TR 102 893 ETSI TS 102 894-2 ETSI TS 103 301 ISO 13111 ISO 21217 ISO 27005 ISO TS 19321 SAE J2945/1	ETSI EN 302 571 ETSI EN 302 663 ETSI TR 103 415 ETSI TS 102 731 ETSI TS 102 940 ETSI TS 102 941 ETSI TS 103 097 IEC 61784 IEEE 1609.2 IEEE 802.11 IEEE 802.11p SAE J2735	ETSI TR 103 061 ETSI TR 103 061-1		ISO 24100 ISO/IEC 2700X
Evaluator activities (ouput)	ETSI GS ISI 003 ISO 15408 SAE J3061	ISO 2700X	ISO/IEC AWI 18045	ISO/IEC AWI 18045	ISO/IEC AWI 18045 ISO/IEC 17021	ISO/IEC AWI 18045 ISO/IEC 17021	ETSI GS ISI 003 ISO/IEC 17021 ISO/IEC 2700X
Lacks			PPs		Conformity tests lists	ITS vulnerability tests guides	Assurance activities at system level
Possible standardization target			• PPs ○ Content input: D2.4 ○ SDO: ETSI		• Conformity tests ○ Content input: D3.2 & D6.2 ○ SDO: ISO / ETSI	• Vulnerability tests ○ Content input: D3.2 & D6.2 ○ SDO: ISO / ETSI	

Table 6: Standardization gaps to be addressed by SAFERtec

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

SAFERtec WP	WP2				WP3			WP4				
Task	T2.1	T2.2	T2.3	T2.4	T3.1	T3.2	T3.3	T4.1	T4.2	T4.3	T4.4	T4.5
Related standard	ISO 13111-1 ETSI EN 302 637-2 ETSI EN 302 637-3	ETSI TR 102 893	N/A	ISO 15408	ISO 15408 SAE J3061 ISO/IEC 17021 ISO/IEC TS 17021-7 ISO/IEC 2700X	ETSI GS ISI 003	N/A	CEN ISO TS 19091 ETSI EN 302 637-2 ETSI EN 302 637-3 ETSI TR 103 415 ETSI TS 102 894-2 ETSI TS 102 731 ETSI TS 102 940 ETSI TS 102 941 ETSI TS 103 301 IEEE 1609.2 ISO 14813-1 ISO 21217	CEN ISO TS 19091 ETSI EN 302 636-4 ETSI EN 302 637-2 ETSI EN 302 637-3 ETSI EN 302 571 ETSI EN 302 663 ETSI EN 302 895 ETSI TS 102 894-2 ETSI TS 102 941 ETSI TS 103 097 IEEE 802.11p ISO TS 19321 SAE J2735 SAE J2945/1	CEN ISO TS 19091 ETSI EN 302 637-2 ETSI EN 302 637-3 ETSI EN 302 571 ETSI EN 302 663 ETSI TS 102 894-2 ETSI TS 102 941 ETSI TS 103 097 IEEE 802.11p SAE J2735	ETSI TS 103 301	
Possible input/update for the standard	None	ETSI TR 102 893	N/A	None	None	None	N/A	ETSI TR 103 415				

SAFERtec WP	WP5			WP6		
Task	T5.1	T5.2	T5.3	T6.1	T6.2	T6.3
Related standard	ISO 15408 ISO/IEC 2700X FIPS 140-2	N/A	ISO/IEC 2700X		CEN ISO TS 19091 ETSI EN 302 637-2 ETSI EN 302 637-3 ETSI TS 102 894-2 ETSI TS 103 301 IEEE 1609.2 ISO 14813-1 ISO 21217	N/A
Possible input/update for the standard	None	None	None			

Table 7: Existing standards to be updated by SAFERtec

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.3 SAFERtec standardization plan

4.3.1 Standardisation targets

We have identified 5 possible candidates for the SAFERtec standardization activities. One of them seems to be likely, two of them seem to be possible target and the last two seems to be unlikely.
The first one, Protections Profiles (D3.2) is in fact the most probable target since it will be a direct result of the project, that does not need to be reworked to be standardized, plus the ETSI seems to be a possible standardization body for these results and for the consortium. Protection Profiles for ITS are made mandatory by the Delegated Act on C-ITS, thus there is a strong need of internationally recognized PP. That's why se think that the PPs a very good target for standardization.
The second one, conformity tests, seems to be reachable even if more challenging. Conformity tests are not for seen to be fully mature results within the project. But still we think it's possible within the project formalize functional conformity tests based on ETSI ITS specifications, since tests and knowledge bases will be developed in WP4 and 5 and they will be an important part of the assurance framework. Additional work should be required by the standardization activity to obtain the right level of maturity of the raw project results to be standardized. Given that the project results are adequately good, the ESTI could be addressed by the partners to push for the standardization of conformity tests (including the PKSI).
The ETSI TR 102 893 TVRA could be a good standard to be updated by the project results, since the D2.2/D2.3 work directly updates this standard. The difficulty here lies more in the capability of the consortium to make the ETSI re-open a working group to update it.
Finally, the other targets seem less likely to be reached, since the project results do not seem to fully address the subject. In a nutshell, our targets are the PPs and Conformity Tests.

Title	Likelihood

Protection Profiles (NEW)	• ETSI
	  ○ likely
	• ISO
	  ○ Unlikely

Conformity tests (NEW)	• ETSI
	  ○ Possible
	• ISO
	  ○ Unlikely

ETSI TR 102 893	• Possible
ETSI TR 103 415	• Unlikely

Vulnerability tests (NEW)	• ETSI
	  ○ Unlikely
	• ISO
	  ○ Unlikely

Table 8: Initial standardization targets

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.3.2 Initial Action Plan

Table 9 presents the original SAFERtec standardization plan. Clearly, the plan developed in a fairly early stage of the project with no or minimum inputs from WP3 and WP4 activities, remained rather high level trying to identify initial opportunities.

Action	Participant	Deadline
Protection Profiles		
OBU PP redaction	UPRC, ICCS, Autotalks, CCS, Oppida	June-September 2018
Contact the ESTI	CCS, Commsignia, Autotalks, Oppida	Autumn 2018
Standardization activities	CCS, Commsignia, Autotalks, Oppida, UPRC, ICCS, Autotalks,	2019
Standardized PPs	-	End 2019
Conformity tests suites		
Conformity tests suites redaction from D3.2 and 6.2	ICCS, UPRC, CCS, Oppida	September 2019
Contact the ESTI	Oppida, CCS	June 2019
Standardization activities	CCS, Commsignia, Autotalks, Oppida, UPRC, ICCS, Autotalks,	2020
Standardized conformity checks	-	2020

Table 9: Initial standardization plan

A considerable update of this plan with numerous details and clearer set of involved partners and actions is presented next. The updated standardization plan exploits the work carried-out in WP2 as well as the lessons learned from the SAFERtec implementation activities as well as the interaction of the partners with related bodies, working-groups and stakeholders.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.3.3 Updated action plan (01/19)

Regarding standardization opportunities and project results at T0+24, the following targets and actions are refined or redefined from the initial action plan.

4.3.3.1 Targets update

At T0+24 the most likely target is the ETSI standardization body and its open draft.

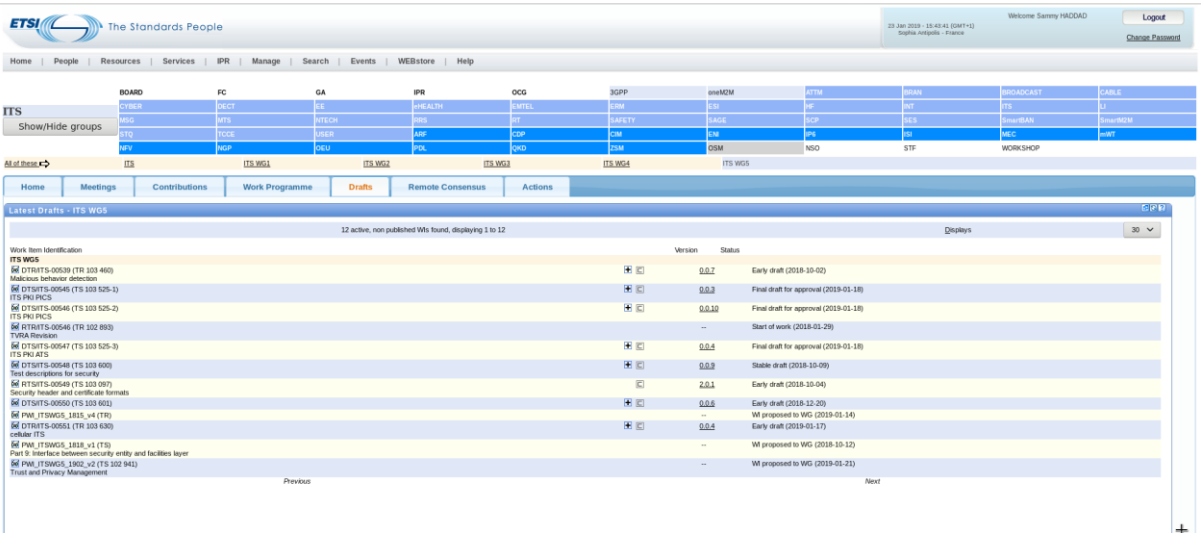

Figure 3 - ETSI current drafts and open items

Those standards present very likely opportunities for SAFERtec to push the project results to standardization. The main target is the ETSI ITS TVRA. Thus, we update the target priority order as follow:

Title	Likelihood
ETSI TR 102 893 - ITS TVRA	• Very likely
ETSI TR 103 460 – Malicious behaviour detection	• Likely
Protection Profiles (ETSI)	○ Likely
SAF	• De facto / regulation ○ Likely
ETSI TR 103 415 - Pre-standardization study on pseudonym change management	• Unlikely
Vulnerability tests (NEW) (ETSI)	• ETSI ○ Unlikely • De facto / regulation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	○ Unlikely

Table 10: First standardization targets update

The main changes compared to the initial plan are the addition of a new target and the reordering of the targets priority.

In fact, one entry has been added, compared to the original plan. The Malicious behaviour detection standardization input has been identified during the PP (D3.2) elaboration. In fact, we've started to define in that documents plausibility checks on data exchanged that can be directly used for malicious behaviour detections, since implausible data are either due to errors or attacks. We have also, observed during implementation phase (WP4) some wrong behaviours that we managed to detect thanks to metrics that could also be used in malicious detection. We have identified thanks to discussion some SAFERtec partners had with people involved in this working group that there is a real opportunity for SAFERtec's ETSI members to contribute to that ongoing work.

The new main target is the ETSI ITS TVRA. In fact, both the work done in WP2 (risk analysis) and the first contacts initiated with this ETSI task force working on that subject, confirmed that we have adequate updates and inputs to provide to this standard. In the project we have considered new threats and updated the ITS reference architecture to be closer to the more recent ITS implementation and thus the real need of new ITS systems. We could help make a good enhancement of the current standard version.

4.3.3.2 SAFERtec standardization groups

For each standardisation target we define a dedicated working group of SAFERtec partners to reach the specific standardization target. The dedicated group is separated in two sub-groups, one for input preparation and one for contact and dissemination toward the identified standardization body or group of interest. In these groups the different individual responsible for each partner are presented with their abbreviation as listed in Table 12.

Regarding the dissemination groups, since we have three different targets, we have three recurring groups. One group to address the ETSI: Oppida (SHA) as the task leader, Autotalks (LME) and CCS (GMA) as representatives of ETSI members. A second group to address the dissemination toward the C2C: Oppida (SHA) as the task leader, Autotalks (LME) and Commsigna (AVA) as representatives of C2C members. Finally, a group to address the SOG-IS though the ANSSI: : Oppida (SHA) as the task leader and ITSEF notified by the ANSSI and CCS (GMA & MGA) as major French industrial working regularly with the ANSSI.

The groups we have defined are as follow.

Standardization	SAFERtec working group
ETSI TR 102 893 - ITS TVRA	• Leader

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA) ▪ Commsigna (AVA)
ETSI TR 103 460 – Malicious behaviour detection	• Leader ○ Oppida (SHA) • Participants ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA)
Protection Profiles	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA) ▪ Commsigna (AVA)
SAF	• Leader ○ Oppida (SHA) • Participants

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	○ Standardization Input formalization ▪ Oppida (SHA) ▪ UPRC (KOM) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA & MGA) ▪ Commsigna (AVA)
ETSI TR 103 415 - Pre-standardization study on pseudonym change management	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ UPRC (KOM) ▪ CCS (MGA) ▪ Autotalks (LME) ▪ Commsigna (AVA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ Autotalks (LME) ▪ CCS (GMA)
Vulnerability tests (NEW)	• Leader ○ Oppida (SHA) • Participants ○ Standardization Input formalization ▪ CCS (MGA) ▪ Oppida (SHA) ○ Communication with standardization bodies ▪ Oppida (SHA) ▪ CCS (GMA & MGA))

Table 11: SAFERtec standardization working groups

Partner	Abbreviation
Matthieu Gay (CCS)	MGA
Guillemette Massot (CCS)	GMA
Kostas Maliatsos (UPRC)	KOM

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

András Váradi (COMM)	AVA
Sammy Haddad (OPP)	SHA
Leo Menis (AUT)	LME

Table 12: Abbreviations of names of responsible partners'in standardization activities

4.3.3.3 Action points

4.3.3.3.1 ETSI TR 102 893 - ITS TVRA

ID	Action point description	Partners involved	Date
AP1.1	• Identify and contact ETSI working item responsible • Ask for possible inputs and their formats	Oppida Commsigna ICCS	31/01/2019
AP1.2	Formalize SAFERtec standardization inputs for the TVRA based on the D2.3	UPRC CCS	27/02/2019
AP1.3	Send standard modification request to the ETSI	CCS Autotalks	08/03/2019

Table 13: ETSI TR 102 893 - ITS TVRA related action plan

4.3.3.3.2 ETSI TR 103 460 – Malicious behaviour detection

ID	Action point description	Partners involved	Date
AP2.1	• Identify and contact ETSI working item responsible • Ask for possible inputs and their formats	Oppida Commsigna ICCS	31/01/2019
AP2.2	Identify from D 2.3 (Vulnerability analysis), D3.2 (PPs) and D5.2 potential plausibility checks to be potential inputs for the standard	UPRC CCS	31/06/2019
AP2.3	Send inputs to the ETSI via the ETSI member portal	CCS Autotalks	08/03/2019

Table 14: ETSI TR 103 460 – Malicious behaviour detection related action plan

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4.3.3.3.3 Protection Profiles

ID	Action point description	Partners involved	Date
AP3.1	Request a time slot to the C2C WG SEC for SAFERtec PPs presentation during the C2C week to held place 11th to 14th of March 2019 in Guyancourt, France	Oppida Commsigna Autotalks	15/02/2019
AP3.2	Contact the ANSSI to present the SAFERtec project, the PPs and the SAF	Oppida CCS	15/02/2019
AP3.3	Present the SAFERtec PPs and propose to the C2C consortium to study the possibility to standardize the PP	Oppida Commsigna Autotalks	11/03/2019

Table 15: PPs related action plan

4.3.3.3.4 SAF

ID	Action point description	Partners involved	Date
AP4.1	Request a time slot to the C2C WG SEC for SAF presentation during the C2C week to held place 2nd to 4th of July 2019 in Guyancourt, France	Oppida Commsigna Autotalks	17/05/2019
AP4.2	Contact the ANSSI to present the SAFERtec project, the PPs and the SAF	Oppida CCS	15/02/2019
AP4.3	Present the SAF to the SOG-IS with the ANSSI support define a European alternative to the regular CC certifications.	Oppida Commsigna Autotalks	-

Table 16: SAF related action plan

4.3.3.3.5 ETSI TR 103 415 - Pre-standardization study on pseudonym change management

ID	Action point description	Partners involved	Date
AP5.1	Contact working group coordinator to present SAFERtec project and identify possible collaborations or inputs to provide.	Oppida	15/02/2019

Table 17: ETSI TR 103 415 - Pre-standardization study on pseudonym change management related action plan

4.3.3.3.6 Vulnerability tests

ID	Action point description	Partners involved	Date

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

AP6.1	Formalize a vulnerability test plan based on the security requirement provided in the PPs (D3.2) and the actual vulnerability tests run in WP3 and 5. Contact the ANSSI in order to present the vulnerability test plan to their experts.	Oppida CCS	27/09/2019
AP6.2	Present the SAFERtec vulnerability test plan to the ANSSI and discuss possible collaboration with other SOG-IS members to define standardized tests plan to be used under the C-ITS Delegated act.	Oppida CCS	10/2019
AP6.3	Present the SAFERtec test plan to the SOG-IS members?	Oppida CCS	12/2019

Table 18: Vulnerability tests action plan

5 Risk Matrix

The following table constitutes a new addition to the (generic) SAFERtec Risk Matrix (presented originally in D1.2). As mentioned there, the table will be updated regularly as the work progresses and the consortium moves to important (technical) choices.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

In the following entries, we identify a number of risks associated to the SAFERtec standardization plan; we highlight mitigation actions for each of them (first and second column of the table respectively). In the two rightmost columns we approximately assess their probability of occurrence (using three levels: low, moderate, high) and the estimated impact (using a 1-10 scale). In the last column, finally, the other WPs impacted by the risk are listed.

Risk	**Mitigation plan**	**Estimated probability** (3 levels)	**Estimated Impact** (1-10 scale)	**Other WPs Potentially Impacted by the RISK**
The consortium is not able to conclude a standardization contribution because the required process is demanding and time-consuming extending beyond the life-time of the project.	The involved industrial / SME partners will continue working on potential standardization contributions following (directly or indirectly) the SAFERtec contribution. The actual impact of SAFERtec is therefore, expected after the completion the project.	High	6	None
The SAFERtec Modular Protection Profile (of the connected vehicle) faces difficulties (or is not accepted) to be standardized in ETSI (or ISO)	The modular protection Profile will be communicated / promoted to the Car2Car Communication Consortium and other major players in the European automotive arena (e.g. PFA - French Automobile Manufacturers' Association, ERTRAC- European Road Transport Research Advisory Council, SOG-IS members, etc). Despite the fact that those organizations lack the characteristics of a standardization body, they can act as proxies to the standardization process and maximize the impact of the SAFERtec protection profile within the European automotive sector.	High	6	(indirect impact on WP3)
Conformity tests suites (and associated knowledge bases) realized in SAFERtec are not mature enough to become a candidate for standardization.	As a first mitigation measure we aim to direct the efforts to the modular protection profile. The SAFERtec Protection profile can/will serve as a basis for writing test suites and will be a key component towards that end. A second measure would be an attempt (from the consortium) to continue the relevant work in future initiatives and a potential SAFERtec follow-up project.	High	6	None
Difficulties in pushing a standardization body (i.e., ETSI) re-open a working group to update a related standard (i.e., ETSI TR 102 893).	Direct the efforts to the modular protection profile and make sure to deliver the proposed change in form of a comment to a standards developing organization (SDO), or a white-paper (to be available if the item would be re-opened after the project's end.	High	5	None
Difficulty to have SAFERtec partners directly involved in standardization working groups.	The SAFERtec results estimated as deemed to be pushed toward standardization will be communicated / promoted to the Car2Car Communication Consortium and other major players in the European automotive arena (e.g. PFA - French Automobile Manufacturers' Association, ERTRAC- European Road Transport Research Advisory Council, SOG—IS members, etc). So they can support SAFERtec standardization process or directly push themselves SAFERtec results towards standardization bodies.	High	7	None

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Lack of maturity or completeness of SAFERtec results.	SAFERtec results might not be mature or complete enough to be worth standardization process or to be able to support a full standard, however they can still be important inputs for future standardization works. In that case, relevant results still deemed important enough to be part of standards will be identified and formalized by the SAFERtec consortium and will be communicated / promoted to the Car2Car Communication Consortium and other major players in the European automotive arena (e.g. PFA - French Automobile Manufacturers' Association, ERTRAC- European Road Transport Research Advisory Council, SOG—IS members, etc) for future standardization work.	High	7	None

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

6 Conclusions

The deliverable presents a comprehensive overview of the current standardization landscape in the ITS and security assurance areas. It constitutes a fundamental output of the SAFERtec WP7 but at the same time offers a reference document to any relevant research effort.

In terms of structure, the document firstly identifies the different standardization bodies that could be candidates for SAFERtec standardization objectives. Then, it details the relevant standards that those bodies have proposed/adopted and fall into the SAFERtec's scope. It identifies the SAFERtec works that stand as the most appropriate candidates for standardization contributions and sketches a corresponding time-line of actions. The relevant risks identified together with the mitigation actions complete the content of the deliverable.

Standardization has been set as a highly important contribution for the project. Standards do require time and in view of the limited project lifetime, the consortium invests some efforts on innovative ideas (e.g., modular PP) to ease road towards a standardization contribution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

7 References

[ACEA] http://www.acea.be
[ACEA_principles]
http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

8 Appendices

8.1 A 1: ETSI ITS standards

ETSI deliverable	Title
ETSI TR 103 403 V1.1.1 (2017-06)	Intelligent Transport Systems (ITS); Mitigation techniques to avoid harmful interference between equipment compliant with ES 200 674-1 and ITS operating in the 5 GHz frequency range; Evaluation of mitigation methods and techniques
ETSI TS 102 871-1 V1.4.1 (2017-05)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma
ETSI TS 102 871-2 V1.4.1 (2017-05)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 871-3 V1.4.1 (2017-05)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI EN 302 636-4-1 V1.3.0 (2017-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality
ETSI EN 302 636-5-1 V2.1.0 (2017-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
ETSI TS 102 890-1 V1.1.1 (2017-05)	Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification
ETSI TR 102 893 V1.2.1 (2017-03)	Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
ETSI TS 103 096-1 V1.3.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)
ETSI TS 103 096-2 V1.3.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 103 096-3 V1.3.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TR 103 099 V1.4.1 (2017-03)	Intelligent Transport Systems (ITS); Architecture of conformance validation framework
ETSI TS 102 869-1 V1.5.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	Service (DEN); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma
ETSI TS 102 869-2 V1.5.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 869-3 V1.5.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Decentralized Environmental Notification Basic Service (DEN); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TS 103 191-1 V1.2.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma
ETSI TS 103 191-2 V1.2.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 103 191-3 V1.2.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Facilities layer protocols and communication requirements for infrastructure services; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TS 102 868-1 V1.4.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma
ETSI TS 102 868-2 V1.4.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 868-3 V1.4.1 (2017-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Cooperative Awareness Basic Service (CA); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI EN 302 571 V2.1.1 (2017-02)	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU
ETSI EN 300 674-2-2 V2.1.1 (2016-11)	Transport and Traffic Telematics (TTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5 795 MHz to 5 815 MHz frequency band; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU; Sub-part 2: On-Board Units (OBU)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 103 248 V1.1.1 (2016-11)	Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)
ETSI TS 103 301 V1.1.1 (2016-11)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
ETSI TS 102 965 V1.3.1 (2016-11)	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration
ETSI TS 102 940 V1.2.1 (2016-11)	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management
ETSI EN 300 674-2-1 V2.1.1 (2016-09)	Transport and Traffic Telematics (TTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5 795 MHz to 5 815 MHz frequency band; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU; Sub-part 1: Road Side Units (RSU)
ETSI TS 102 723-8 V1.1.1 (2016-04)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer
ETSI TS 101 556-2 V1.1.1 (2016-02)	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Part 2: Communication system specification to support application requirements for Tyre Information System (TIS) and Tyre Pressure Gauge (TPG) interoperability
ETSI TR 101 613 V1.1.1 (2015-09)	Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium; Validation set-up and results
ETSI TR 103 061-6 V1.1.1 (2015-09)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 6: Validation report
ETSI TS 102 792 V1.2.1 (2015-06)	Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range
ETSI TS 103 175 V1.1.1 (2015-06)	Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium
ETSI TS 103 097 V1.2.1 (2015-06)	Intelligent Transport Systems (ITS); Security; Security header and certificate formats
ETSI EN 302 636-3 V1.2.1 (2014-12)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture
ETSI EN 302 637-2 V1.3.2 (2014-11)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service
ETSI EN 302 637-3 V1.2.2 (2014-11)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 101 556-3 V1.1.1 (2014-10)	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communications; Part 3: Communications system for the planning and reservation of EV energy supply using wireless networks
ETSI EN 302 895 V1.1.1 (2014-09)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)
ETSI TR 101 612 V1.1.1 (2014-09)	Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium; Report on Cross layer DCC algorithms and performance evaluation
ETSI TS 102 894-2 V1.2.1 (2014-09)	Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
ETSI EN 302 636-5-1 V1.2.1 (2014-08)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
ETSI TS 102 760-1 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 1: Implementation Conformance Statement (ICS) proforma
ETSI TS 102 760-2 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 760-3 V1.1.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for Access Technology Support (ISO 21218); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma
ETSI TR 101 611 V1.1.1 (2014-06)	Intelligent Transport Systems (ITS); Testing; Conformance test specification for CALM Fast Services; FNTP/FSAP/IICP validation report
ETSI TR 103 101 V1.1.1 (2014-06)	Intelligent Transport Systems (ITS); Test suite validation; Access technology support ISO 21218
ETSI TS 102 797-1 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 1: Protocol Implementation Conformance Statement (PICS) specification
ETSI TS 102 797-2 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 797-3 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 102 985-1 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 1: Protocol Implementation Conformance Statement (PICS) proforma
ETSI TS 102 985-2 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 985-3 V1.2.1 (2014-06)	Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281); Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma
ETSI EN 302 636-6-1 V1.2.1 (2014-05)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
ETSI EN 302 636-1 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements
ETSI TR 103 061-3 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Part 3: Conformance test specifications for Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; GeoNetworking validation report
ETSI TS 102 859-2 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 859-3 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TS 102 859-1 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Transmission of IP packets over GeoNetworking; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
ETSI TR 103 061-1 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Part 1: Conformance test specifications for Co-operative Awareness Messages (CAM); CAM validation report
ETSI TR 103 061-2 V1.2.1 (2014-04)	Intelligent Transport Systems (ITS); Testing; Part 2: Conformance test specifications for Decentralized Environmental Notification basic service Messages (DENM); DENM validation report
ETSI TR 103 083 V1.1.1 (2014-03)	Electromagnetic compatibility and Radio spectrum Matters (ERM); System Reference document (SRdoc); Technical characteristics for pan European harmonized communications equipment operating in the 5,855 GHz to 5,925 GHz range intended for road safety and traffic management, and for non-safety related ITS applications

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 102 723-11 V1.1.1 (2013-12)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 11: Interface between networking and transport layer and facilities layer
ETSI EN 302 636-2 V1.2.1 (2013-11)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios
ETSI TS 101 539-3 V1.1.1 (2013-11)	Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) application requirements specification
ETSI TS 102 636-4-2 V1.1.1 (2013-10)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5
ETSI EN 302 571 V1.2.1 (2013-09)	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
ETSI TS 102 894-1 V1.1.1 (2013-08)	Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications
ETSI TS 101 539-1 V1.1.1 (2013-08)	Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification
ETSI EN 302 663 V1.2.1 (2013-07)	Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI ES 200 674-1 V2.4.1 (2013-05)	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band
ETSI TR 101 607 V1.1.1 (2013-05)	Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1
ETSI TS 102 708-2-1 V1.3.1 (2013-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification
ETSI TS 102 708-2-2 V1.4.1 (2013-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI TS 102 708-2-3 V1.4.1 (2013-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TR 102 965 V1.1.1 (2013-03)	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list
ETSI TS 102 917-1 V1.1.1 (2013-01)	Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 1: Protocol Implementation Conformance Statement (PICS)
ETSI TS 102 917-2 V1.1.1 (2013-01)	Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 2: Test Suite Structure and Test Purposes (TSS & TP)
ETSI TS 102 917-3 V1.1.1 (2013-01)	Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TR 102 960 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (RTTT DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range; Evaluation of mitigation methods and techniques
ETSI TS 102 723-10 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 10: Interface between access layer and networking & transport layer
ETSI TS 102 723-1 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 1: Architecture and addressing schemes
ETSI TS 102 723-2 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 2: Management information base
ETSI TS 102 723-3 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 3: Interface between management entity and access layer
ETSI TS 102 723-4 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 4: Interface between management entity and networking & transport layer
ETSI TS 102 723-5 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 5: Interface between management entity and facilities layer
ETSI TR 103 061-5 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); Testing; Part 5: IPv6 over GeoNetworking validation report
ETSI TR 103 061-4 V1.1.1 (2012-11)	Intelligent Transport Systems (ITS); Testing; Part 4: Conformance test specification for GeoNetworking Basic Transport Protocol (BTP); GeoNetworking BTP validation report
ETSI TS 102 724 V1.1.1 (2012-10)	Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI TS 101 556-1 V1.1.1 (2012-07)	Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Electric Vehicle Charging Spot Notification Specification
ETSI TS 102 941 V1.1.1 (2012-06)	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 102 942 V1.1.1 (2012-06)	Intelligent Transport Systems (ITS); Security; Access Control
ETSI TS 102 943 V1.1.1 (2012-06)	Intelligent Transport Systems (ITS); Security; Confidentiality services
ETSI TS 102 867 V1.1.1 (2012-06)	Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2
ETSI TS 102 916-1 V1.1.1 (2012-05)	Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 1: Protocol Implementation Conformance Statement (PICS)
ETSI TS 102 916-2 V1.1.1 (2012-05)	Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI TS 102 916-3 V1.1.1 (2012-05)	Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC; Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TR 102 962 V1.1.1 (2012-02)	Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)
ETSI TR 102 861 V1.1.1 (2012-01)	Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part
ETSI TR 102 862 V1.1.1 (2011-12)	Intelligent Transport Systems (ITS); Performance Evaluation of Self-Organizing TDMA as Medium Access Control Method Applied to ITS; Access Layer Part
ETSI EN 302 931 V1.1.1 (2011-07)	Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition
ETSI TS 102 687 V1.1.1 (2011-07)	Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part
ETSI TS 102 636-4-1 V1.1.1 (2011-06)	Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality
ETSI TR 102 863 V1.1.1 (2011-06)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization
ETSI TS 102 860 V1.1.1 (2011-05)	Intelligent Transport Systems (ITS); Classification and management of ITS application objects
ETSI TS 102 636-6-1 V1.1.1 (2011-03)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols
ETSI TS 102 637-2 V1.2.1 (2011-03)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 102 870-3 V1.1.1 (2011-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for Geonetworking Basic Transport Protocol (BTP); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
ETSI TS 102 870-1 V1.1.1 (2011-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
ETSI TS 102 870-2 V1.1.1 (2011-03)	Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking Basic Transport Protocol (BTP); Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI EN 302 686 V1.1.1 (2011-02)	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 63 GHz to 64 GHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
ETSI TS 102 636-5-1 V1.1.1 (2011-02)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol
ETSI EG 202 798 V1.1.1 (2011-01)	Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing
ETSI EN 302 665 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Communications Architecture
ETSI TS 102 731 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Security; Security Services and Architecture
ETSI TS 102 637-1 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements
ETSI TS 102 637-3 V1.1.1 (2010-09)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
ETSI TR 102 698 V1.1.2 (2010-07)	Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications
ETSI TS 102 636-1 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements
ETSI TS 102 708-1-1 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification
ETSI TS 102 708-1-2 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI TS 102 708-1-3 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	the 5,8 GHz ISM band; Part 1: Data Link Layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma
ETSI TS 102 636-2 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 2: Scenarios
ETSI TS 102 636-3 V1.1.1 (2010-03)	Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture
ETSI ES 202 663 V1.1.0 (2010-01)	Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band
ETSI TR 102 638 V1.1.1 (2009-06)	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions
ETSI TS 102 486-1-3 V1.2.2 (2009-05)	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma
ETSI TR 102 707 V1.1.1 (2009-05)	Intelligent Transport Systems (ITS); ETSI object identifier tree; ITS domain
ETSI TR 102 654 V1.1.1 (2009-01)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Co-location and Co-existence Considerations regarding Dedicated Short Range Communication (DSRC) transmission equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range and other potential sources of interference
ETSI TS 102 486-1-2 V1.2.1 (2008-10)	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI TS 102 486-2-1 V1.2.1 (2008-10)	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification
ETSI TS 102 486-2-2 V1.2.1 (2008-10)	Intelligent Transport Systems (ITS) Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)
ETSI TS 102 486-2-3 V1.2.1 (2008-10)	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 2: DSRC application layer; Sub-Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

ETSI TS 102 486-1-1 V1.1.1 (2006-03)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Test specifications for Dedicated Short Range Communication (DSRC) transmission equipment; Part 1: DSRC data link layer: medium access and logical link control; Sub-Part 1: Protocol Implementation Conformance Statement (PICS) proforma specification

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319