EU-US Standards Harmonization Task Group Report: Overview of Harmonization Task Groups 1&3

Document HTG1&3-1

EU-US ITS Task Force
Standards Harmonization Working Group
Harmonization Task Groups 1&3

November 12, 2012

Publication # FHWA-JPO-13-073

U.S. Department of Transportation

Produced by the Implementing Arrangement between the European Commission and the U.S. Department of Transportation in the field of research on Information and Communications Technologies for transportation

U.S. Department of Transportation

Research and Innovative Technology Administration (RITA)

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-13-073		

4. Title and Subtitle	5. Report Date
EU-US Standards Harmonization Task Group Report: Overview of Harmonization Task Groups 1&3 (Document HTG1&3-1)	November 12, 2012
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Scott Cadzow, Paul Eichbrecht, Knut Evensen, Hans-Joachim Fischer, Emilio Davila-Gonzalez, Wolfgang Hoefs, Frank Kargl, Eric Koenders, Ola Martin Lykkja, John Moring, Richard Roy, Steve Shladover, Steve Sill, Takaaki Sugiura, Siebe Turksma, William Whyte	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
ITS Joint Program Office, Research and Innovative Technology Administration, U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Washington, DC 20590	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
ITS Joint Program Office, Research and Innovative Technology Administration, U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Washington, DC 20590	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Harmonization Task Groups 1 and 3 (HTG1 and 3) were established by the EU-US International Standards Harmonization Working Group to attempt to harmonize standards (including ISO, CEN, ETSI, IEEE) on security (HTG1) and communications protocols (HTG3) to promote cooperative ITS interoperability. This document provides the background and overview of both HTG1 and HTG3, which worked in close cooperation, and also provides an introduction to the reports they generated regarding harmonization of cooperative communication standards for ITS. The scope was limited to standards harmonization and "gap" analysis, but does not specify system design or implementation. The outputs of HTGs 1 and 3 are recommendations to relevant Standards Development Organizations (SDO) and are intended to assist the development of the respective standards by focusing attention on areas where action is needed to obtain or maintain harmonization and on areas where there are gaps in the existing standards that should be addressed in the near future.

17. Key Words	18. Distribution Statement
intelligent transport systems, vehicle, mobile, standards, harmonization, cooperative, 5.9 GHz, safety, interoperability, security, communications, protocol	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		71	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

1 Introduction

This document is intended as an introduction to the work performed and the outputs produced by a group of experts in the area of standards for Intelligent Transport Systems (ITS) communications. Two groups of experts, denoted Harmonization Task Groups 1 and 3 (HTG1 and HTG3 respectively), were assembled and tasked to produce a set of recommendations to Standards Development Organizations (SDOs) over a six-month period.

> The outputs of Harmonization Task Groups 1 and 3 are recommendations to SDOs and the ITS stakeholder community. These outputs are not specifications regarding system design or implementation.

1.1 Summary of purposes and goals

This report describes the goals, assumptions, constraints, efforts and results of HTG1 and HTG3. The work was jointly sponsored by the U.S. Department of Transportation's (USDOT) Research and Innovative Technology Administration (RITA), Intelligent Transportation Systems Joint Program Office (ITS-JPO) and the European Commission's (EC) Directorate General on Communications Networks, Content & Technology (DG CONNECT). The HTG1 effort, which focused on security issues, and the HTG3 effort, which focused on communication protocol issues, were the first jointly sponsored and jointly led work programs of the European Union (EU)-USDOT International Standards Harmonization Working Group, formed as part of the 2010 agreement on joint ITS research between the USDOT and the EC. The intent of the working group is to facilitate harmonization of Intelligent Transportation System (ITS) cooperative communication standards to support rapid, cost effective deployment of connected vehicle (U.S. terminology) or cooperative ITS (EU terminology) technologies. HTG1 and HTG3 were initiated to make the first cooperative attempt under the joint EU-US intergovernmental agreement to achieve harmonization of security and communication protocols between the U.S. and Europe in support of connected vehicle technologies. Their primary objectives are to identify gaps and overlaps in existing, in-development and planned standards; develop technical descriptions of limited interoperability tests between US and European cooperative ITS; and provide feedback to the relevant Standards Development Organizations (SDOs).

The work of these HTGs was not intended to prescribe specific equipment architectures or designs, nor was it intended to provide guidance or directions for implementation and deployment. It was focused solely on achieving harmonization amongst SDOs to ensure that ITS can be deployed globally based on a set of standards harmonized to the greatest extent feasible, where conformance to the standards will give very high assurance (but not necessarily a

guarantee) of both interoperability and interworking of deployed equipment irrespective of where in the world the equipment is deployed. A secondary concern was to ensure that the standards support the widest possible range of deployment models and implementations.

Since the HTG1 security issues and HTG3 communication protocol issues were sufficiently closely interrelated, the work of these two HTGs was closely coordinated. With significant overlap in membership, the work was conducted jointly by the members (cf. Annex A).

The longer-term goal of the EU-US International Standards Harmonization Working Group is to harmonize ITS-related standards between the U.S. and Europe, according to Clause 10 of the EU-US Joint Declaration on Cooperative Systems for ITS. The short-term goal is to accelerate progress on a set of harmonized standards sufficient to support a joint interoperability test of the technical capabilities of cooperative ITS equipment and systems. In performing these tasks, valuable lessons have been learned which will be useful for general feedback to SDOs, as well as for developers of test/commercial systems.

Clause 10 – EU-U.S. Joint Declaration of Intent on Research Cooperation in Cooperative Systems

"Globally harmonized standards are essential to support and accelerate the adoption of Cooperative Systems. The parties strongly support the development of global open standards which ensure interoperability through appropriate actions which include, but are not limited to, coordinating the activities of the standardisation organisations. In particular the parties intend to make efforts to preclude the development and adoption of redundant standards. The adoption of multiple standards within a given area of interest should be limited to those cases where there are demonstrated technical needs, such as differing frequency spectrum allocations, and legal requirements, such as privacy protection laws. The parties welcome participation of other countries and regions, particularly those of the Asia Pacific region, in the development of global open, harmonized standards for Cooperative Systems."

Existing standards were relied upon to maximize the chances of acceptance of the HTG1 and HTG3 recommendations, and to build on the substantial amount of work that has already been done by the International Standardization Organization (ISO), the European Committee for Standardisation (CEN), the European Telecommunications Standardization Institute (ETSI), SAE International, and the Institute of Electrical and Electronics Engineers (IEEE). Furthermore, reliance on existing standards is likely to lead to a set of harmonized standards much more rapidly than if the existing standards work were not considered, which is of importance in accelerating deployment.

Given the time and resource constraints, realistic objectives were identified, focusing on minimum technical recommendations for harmonization of selected standards. Accordingly, the HTG1 and HTG3 deliverables, while intended to be of the highest technical quality, should not necessarily be held to be complete in light of the compromises that had to be made to work within the operative time and resource constraints, nor should they necessarily represent the ideal long-term solutions that will ultimately evolve from continuing research and standards development work. However, the recommendations were formulated with the focus on real-world functionality and eventual expansion towards the full scope of cooperative ITS. The HTG1 and HTG3 efforts were also intended to provide a learning experience that will help the European and U.S. entities evolve processes for effective future cooperation on standardization matters.

1.2 Purpose and intent

This report provides an overview of the issues addressed in the HTG1 and HTG3 tasks, as well as the background, scope and progress of the efforts. This information is intended to be useful in assessing the importance of these tasks separately, and their joint value in achieving the common goal of harmonized international standards for cooperative ITS.

This report consists of the sections listed below:

1. Introduction
2. Executive Summary
3. Background
4. ITS Communications Overview
5. Use Cases/Applications
6. Future Vision
7. Annex A. HTG 1&3 Members
8. Annex B. Harmonization Task Groups (HTG): General Description (Original Document)
9. Annex C. Harmonization Task Group 1 (HTG1) (Original Document)
10. Annex D. Harmonization Task Group 3 (HTG3) (Original Document)
11. Annex E. ITS Communication and Security Issues Related to Border Crossing
12. Annex F. References
13. Annex G. Glossary

HTG1 and HTG3 have each developed three reports as outlined in the table below. These reports are the primary deliverables of the HTG1 and HTG3 teams and should be read along with this overview document. In addition, one topic whose scope extends across the HTGs, GeoNetworking, was found to warrant a report of its own. An additional document was prepared

to summarize the stakeholder comments that were received on the first drafts of the HTG1 and3 documents and the responses from the HTG1 and3 teams.

Table 1: HTG1 and HTG3 Products

Topic	HTG1 (Security)	HTG3 (Communication Protocols)
Status – gap and overlap analysis	HTG1-1 "*Status of ITS Security Standards*"	HTG3-1 "*Status of ITS Communication Standards*"
Interoperability tests	HTG1-2 "*Testing for ITS Security*"	HTG3-2 "*Testing for ITS Communications*"
Feedback to Standards Development Organizations (SDOs)	HTG1-3 "*Feedback to ITS Standards Development Organizations - Security*"	HTG3-3 "*Feedback to ITS Standards Development Organizations - Communications*"
Geo-dissemination of information	HTG1&3-3 *"Observations on GeoNetworking"*	
Responses to initial review comments from stakeholders	HTG1&3-2 *"Stakeholder Engagement and Comment Resolution"*	

2 Executive Summary

This report provides the background and overview of the work of Harmonization Task Groups 1 and 3 (HTG1 and 3) serving as the introduction to the full set of reports produced by HTG1 and 3 regarding harmonization of cooperative communication standards for ITS.

Harmonization Task Groups 1 and 3 were established under the auspices of the EU-US International Standards Harmonization Working Group to make the first joint attempt to harmonize standards on security (HTG1) and communications protocols (HTG3) to promote cooperative ITS interoperability. This effort was motivated by the longer term standards harmonization goal of Clause 10 of the EU-US Joint Declaration on Cooperative Systems for ITS, and is intended to set a positive example for future EU-US joint efforts to facilitate development and deployment of cooperative ITS. Standards harmonization is understood to encourage economically efficient development and deployment of cooperative ITS, to promote a world market for cooperative ITS products and services and to enable interoperability of cooperative personal, vehicular and roadside ITS elements, particularly for persons and vehicles crossing jurisdictional and international borders.

> The outputs of HTGs 1 and 3 are recommendations to standards development organizations and the ITS stakeholder community. They are not specifications regarding system design or implementation.

The scope of the HTG1 and 3 efforts was limited to standards harmonization and "gap" analysis. The outputs are neither product specifications nor designs, nor are they intended to guide product development or system deployment. Herein, standards are defined to be the consensus-based technical standards developed by the standards development organizations (SDOs) active in cooperative ITS, including ISO, CEN, ETSI, IEEE and SAE (although SAE's current work on message sets is outside the scope of HTG1 and 3). Harmonization has been defined to exist at several different levels, and the goal of HTG1 and 3 has been to aim for the highest achievable level of harmonization, while recognizing that the level that can actually be achieved will be constrained by political and commercial, as well as technical considerations. The relationship between the levels of harmonization and interoperability is sufficiently complicated that it is not possible to specify what level of interoperability will be achieved for any given standards harmonization action. The gap analysis was performed to note areas in which there is a need for a globally harmonized standard to be revised or created in order to fill an observed need for further interoperability specifications.

HTG1 and 3 comprise a small group of international experts who worked together intensively between March and August 2012 with co-leadership provided by the EC DG-CONNECT and

USDOT. These experts were chosen from among the editors of many of the current cooperative ITS standards in the different SDOs providing direct linkages into those SDO activities, and representatives of the EU and USDOT and the Vehicle Infrastructure Integration Consortium (VIIC) plus an observer from Japan. The scope of the HTG effort was tightly constrained by schedule, resources and the availability of the experts, who already have many other responsibilities. The level of detail in the documentation of the HTG recommendations is commensurate with available resources, and opportunities for review by and iterations with the stakeholder community were limited by schedule constraints.

The products of the HTG1 and 3 work include three reports from each of the two HTGs: (x-1) a review of the current standards, their overlaps and inconsistencies, and gaps between the standards, as well as some consideration of the feasibility of harmonization to minimize the overlaps, inconsistencies and gaps; (x-2) recommended near-term tests that should be done to test interoperability; and (x-3) recommendations to the SDOs (and, where relevant, other bodies) outlining actions considered by the HTGs to be necessary to achieve harmonization. In addition, Annex E of this background report analyzes the border crossing situation as an illustration of some of the more challenging interoperability issues. A brief separate report on GeoNetworking explains why that topic was determined to be outside the scope of the HTG1-3 and HTG3-3 recommendation documents. The document was created to provide information and rationale supporting associated GeoNetworking references in the technical reports from HTG1 and 3. Additionally, a comment resolution document provides responses to the comments that were submitted on draft versions of the HTG documents by some of the key European and U.S. stakeholder organizations.

Report HTG1-3 provides guidance to the SDOs for actions to be taken that raise the assurance of security interoperability of deployed equipment. The bulk of the analysis for the findings presented in HTG1-3 is given in the supporting document HTG1-1. Report HTG3-3, *Feedback to ITS Standards Development Organizations-Communications***,** further considers the technical topics of communications interoperability documented in HTG3-1. For each topic, one or more actions are described promoting harmonization and the high-level objectives (e.g., interoperability, testability) of the action. These are recommendations to the specified SDO(s) to perform the action, with assignment of a priority (high, medium, low) to each action. As the findings of both HTGs are to be seen as recommendations for action by the SDOs involved in ITS, the SDOs are invited to review them as input to their internal decisions about their program of work.

The development of these reports represents an initial step toward harmonization of standards for cooperative ITS rather than the completion of that process. These reports are being provided to the international cooperative ITS stakeholder community, with special emphasis on the SDOs, as expert recommendations for standardization actions that should be initiated in support of more efficient development and implementation of cooperative ITS. The HTG members and their

sponsors remain eager to encourage further discussion of the issues that are raised in these reports in SDO working groups and other forums.

While the SDOs are the chief determiners of their own program of work, these documents are intended to help the SDOs in developing their programs of work by bringing attention to those areas where action is needed to obtain or maintain harmonization and to those areas where there are gaps in the existing standards that should be filled in a timely manner.

3 Background

3.1 Objectives and tasks overview

This section provides an overview of the issues being addressed in each harmonization task group and the scope of the efforts for the HTGs. The assignments originally given to the HTGs are reproduced in Annex B, Annex C and Annex D, but these evolved in the course of the work. This chapter provides an updated description based on the work performed.

3.2 Goals

The two high-level goals for the HTGs were:

- Long-term goal: Harmonization of ITS-related standards between the U.S. and Europe in accordance with Clause 10 of the EU-US Joint Declaration on Cooperative Systems for ITS
- Short-term goal: Accelerate progress on a minimum set of standards

The original short-term goal included plans for the HTG1 and HTG3 security and communication profile harmonization efforts to be available to support a potential joint showcase at the 2012 ITS World Congress in Vienna, Austria. The demonstration was intended to highlight the feasibility, efficacy and significant value of achieving harmonization and to promote the long-term goal of achieving a set of harmonized standards that allows for global deployment of interoperable ITS-related products and services. That short-term goal was modified during the early efforts of HTG1 and HTG3. The modified goal maintained the objective to accelerate harmonization progress on a minimum set of security and communication protocol standards, but HTG1 and HTG3 have also included in their efforts development of a building-block series of interoperability tests. (See documents HTG1-2 and HTG3-2.) The interoperability tests provide a practical basis for a near-term future demonstration and can also be used as a basis for formal conformance tests.

The HTGs focused on achieving specific targets within a given timeframe. In performing these tasks, valuable lessons were learned which will be useful both for general and specific feedback and recommendations to SDO working groups, as well as for developers of test/commercial systems. These lessons are documented in a separate “Lessons Learned” document.

3.3 Assumptions and Constraints

The task of achieving complete international harmonization of standards for communications in ITS is very large, indeed so large that it could be perceived by some as unachievable within reasonable time and resource constraints. Nevertheless, HTG1 and 3 were established to make the first cooperative EU-US attempt to achieve harmonization of the communication protocol and security standards under the US-EU intergovernmental cooperation agreement on ITS

research. The benefits in terms of cost-effective development, mass production and widespread deployment of connected vehicle systems are expected to justify these efforts.

In order to maximize the likelihood of a timely and useful result, the joint effort was executed within prescribed schedule and resource constraints. It is important to make note of the constraints and assumptions underlying this activity to understand where it fits within the overall EU-U.S. Task Force work and the long-term goal of achieving international interoperability of ITS systems.

3.3.1 Assumptions

The work of HTG1 and 3 proceeded under the following basic assumptions:

- Procedures
  - The direct participants in the harmonization work are drawn from the Subject Matter Expert (SME) communities in both the EU and U.S. In addition, a representative of Japan agreed to observe and offer inputs for consideration.
  - The HTG1 security issues and HTG3 protocol issues are so closely coupled that the work of these two HTGs had to be closely coordinated. Indeed, with significant overlap in membership, the work has been conducted jointly.
- Approach
  - Existing published and draft standards should be relied upon to the greatest extent possible to maximize the chances of acceptance and to build on the good work that has already been done, rather than inventing new approaches that would have to be "sold" to stakeholders on both sides of the Atlantic.
  - The priorities for feedback to the SDOs are not necessarily the same as the priorities for near-term interoperability testing, since the SDO inputs have longer term implications.
  - The interoperability testing has been planned in a "building block" fashion, beginning with testing of individual functions before those functions are integrated into complete applications or use cases.
- Technology
  - The primary wireless technology for the harmonized standards is assumed to be 5.9 GHz, because it is vital for the crash-imminent safety applications needed in both the U.S. and EU, and it is the subject of current standards development activities that have not yet been harmonized between the U.S. and EU. Other technologies have also been considered as applicable for less latency sensitive requirements (e.g., cellular data communications for certificate management).

  - The emphasis in the harmonization work is on achieving interoperability of vehicle- and infrastructure-based ITS stations, rather than on the internal architecture of the ITS stations, which is not needed for interoperability.
  - Nomadic devices (e.g., smart phones or tablets or purpose-specific devices) are for the purposes of this effort considered to be secondary targets for harmonization compared to devices installed in vehicles by the vehicle OEMs, although it is recognized that these devices are already playing a substantial role in deployment of cooperative ITS applications (those that do not address crash-imminent safety).
  - The target applications or use cases must at least include those of greatest interest to the U.S. and EU government policy makers and sponsors of research efforts (crash-imminent safety and sustainability).
  - The target applications to serve as the baseline cases for interoperability testing are chosen based on their ability to span the range of required communications system characteristics, to provide the broadest possible basis for proving interoperability.
  - The focus is on single-hop rather than multi-hop communications in this effort, since the U.S. architecture does not currently envision multi-hop communications.

- Output
  - The outputs of HTG1 and 3 must be of the highest quality technically so as to be of maximum value to the research and development communities. At the same time, they may not be complete, nor may they represent the ultimate long-term solution because of the need to operate strictly within schedule and resource constraints.
  - The HTG1 harmonization work does not aim at the ultimate long-term security needs, but rather at the minimum level of security needed to deploy practical systems within the next few years so that deployment is not unduly delayed.

3.3.2 Constraints

The HTG1 and 3 work has proceeded under several important constraints:

- The technical results of the work (i.e., the recommendations to the SDOs and interoperability testing plans) need to be ready for public dissemination in fall 2012 in order to be in time to influence the shape of standards approaching ballots.
- The interoperability testing has to be defined such that it can be performed using largely existing systems before the end of 2012, rather than covering more conditions/applications than would be feasible to test by then.
- Since the budgets to cover the harmonization work are limited, the scope of the effort has been constrained to fit within those budgets, while assigning highest priority to the most important interoperability issues and assuring the availability of sufficient resources to produce products of the highest quality.

- HTG1 and 3 are not SDOs so they cannot issue standards, nor can they compel the SDOs to follow their recommendations. Rather, their products are intended to convince the SDO memberships of their merits in order to be adopted.

3.4 ITS global interoperability challenge

> The EU and US agreed to cooperate in ITS research in order to achieve interoperability on a national/regional level with a focus on creating a global market for ITS products and services with minimal trade barriers.

Achieving interoperability for mobile ITS stations (defined explicitly in Section 4.1), personal or vehicular, traveling between different operational regions (e.g., crossing the border between two neighboring countries with different management, registration and/or security operations) requires communications interoperability among ITS stations. This is combined with interoperability between back-office systems so that proper operation of safety critical systems and provisioning of expected services can be ensured. This challenge of achieving interoperability across multiple operational regions is even more pronounced if operational regions decide to create their own selection of technical parameters (profiles), which can and often do lead to essential differences in the implementations (e.g., in device hardware and/or software), in spite of having started from the same set of core standards and technologies. The HTGs' work is intended to identify these interoperability challenges and begin the process of mitigating them. Further details on these issues can be found in Annex E.

3.5 Levels of interoperability and their consequences

For the purposes of the HTG1 and HTG3 efforts, the following interoperability levels related to transiting across regulatory boundaries were identified along with their associated challenges:

0. No interoperability. A mobile ITS station[1] must be physically exchanged when crossing a border. This is not a viable option.

---

[1] ITS station: A collection of (functional) components that participates in the provision of ITS services at a particular location. Thus, an ITS station may exist in a vehicle, at the roadside, in a central location or in a personal device. Note that it can have one of two meanings: (1) functional or (2) physical (i.e., an actual physical device), and the meaning is generally clear from the given context.

1. Interfaces and functional requirements are compatible, but applications, security and operations are different. Various software components of the ITS station need to be replaced, and if the station is mounted in a vehicle, the vehicle could be registered as a local vehicle and the ITS station not allowed to operate other than in its local domain. This could be an option when exporting a vehicle, but not an option for a daily commuter or truck operator.
2. Mobile ITS stations are functionally identical. All interfaces, functions, apps, security, etc., are based on the same standards and all stations have passed similar certification procedures, however, the operations of applications and security are "affiliated" with regional back-office systems that do not talk to each other. Potentially, a new "affiliation" could be loaded at the border, or ITS stations could be configured with dual "affiliations", however, the complexity of setting up and managing this is likely to be more challenging than level 3 below.
3. Mobile ITS stations are *functionally* identical. All interfaces, functions, apps, security, etc., are based on the same standards and all stations have passed similar certification procedures, and the operations of applications and security "affiliated" with regional back-office systems have been "harmonized." The back offices may be connected in a hierarchical or flat structure. The institutional challenges are likely to be severe in this case because differences in national cultures lead to different legal protections with regard to privacy, for example.

The difference between Level 2 and Level 3 is the formation of agreements between operational centers and the creation of additional global functions on security, application and identity management. These additional global functions are likely neither complex nor time consuming to create, but may pose political, location and operation cost challenges (e.g., which country gets which operational center, and how are operations financed?).

Note that both Level 2 and Level 3 require common communication profiles.

3.6 Standards harmonization and the interoperability challenge

Harmonized standards are needed to achieve Level 1 or higher ITS interoperability. While the long-term goal is to achieve Level 3 interoperability for the full range of ITS applications, significant economic and societal benefits may be realized by phased implementation of interoperable ITS applications on a regional basis. EC DG CONNECT and USDOT should encourage SDOs to conduct standards development and harmonization activities in such a manner that it supports early implementation of interoperable Cooperative ITS systems. The work of these HTGs is intended to contribute to this outcome. Longer term, an EU-US ITS technical management team could be set up to advise on standards harmonization and other technical policy issues such as common certification procedures, global ITS registration authorities, common security certificate authority (CA) hierarchies, etc.

3.7 Initial standards harmonization tasks

To expedite the accomplishment of the initial harmonization effort, a segmented approach with parallel HTGs was used:

- HTG1 focusing on management and security-related issues.
- HTG3 focusing on the 5.9 GHz air interface and the communications protocol stack.

To achieve the goals in a short timeframe, the scope of each of the tasks was initially reduced to the essential elements with the additional restriction that the outcome is an achievable and demonstrable "real scenario." The results need to be scalable and ultimately deployable, and feedback is to be provided to regional SDOs for possible adoption and inclusion in new or revised standards. As such, this work contributes to establishing the kernel for real interoperability, not only regionally in the Americas and Europe, but also globally.

This work contributes to establishing the kernel for global interoperability, not only regionally in the Americas and Europe.

HTG1 and 3 comprised a small number subject matter experts selected via EU and U.S. processes. A Japanese expert observed and provided input when appropriate. The tasks were clearly delimited, and an aggressive time schedule was developed in order to provide timely guidance to the ongoing work of the SDOs developing ITS standards. HTG1 and 3 officially started work in March 2012. The project duration was six months, during which time HTG1 and 3 met formally five times.

The results of the HTG initiatives are documented in reports (including this one) submitted to the Standards Harmonization Working Group of the EU-U.S. Task Force and made publicly available by the EC and USDOT. The reports contain recommended general ITS standards harmonization principles and guidance, technical information and recommendations addressing specific standardization issues and other information the HTGs deemed relevant. The specific technical details take the form of a joint profile that refers to standards from the relevant SDOs. By doing this, there is a clear connection to the existing standards, so that the same parameter may exist and be referenced to two or more standards. In addition, this will automatically become an overlap and gap analysis for the standards set from ETSI, IEEE, ISO and SAE. Throughout these reports, both U.S. and European terminologies have been used, reflecting the diverse lexicons seen in this field.

With the EU-US Standards Harmonization Working Group's concurrence, the HTG1 and HTG3 reports and recommendations will be provided to the SDO working groups for consideration in the development of the relevant ISO/CEN/ETSI/IEEE/SAE standards.

4 ITS communications overview

The communication component of ITS is, and will continue to be, composed of a variety of currently existing and next-generation communication systems that will need to be interconnected in order to provide seamless peer-to-peer communications among various types of communication nodes in a variety of locations. This interconnected set of communication systems will need to accommodate components and applications from a variety of suppliers, invariably based on a large number of standards. Furthermore, to achieve the maximum benefit from the deployment of these applications, ITS communications must allow for and support the ability to share information among applications and services both on the same platform and across different platforms. This sharing of information gives rise to the term "cooperative ITS/Cooperative ITS" (C-ITS).

For the purpose of this document, the communications architecture focus is vehicle-centric (vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V)) and covers communications, security and management issues that will influence interoperability of systems based on the various ITS standards from CEN/ETSI/IEEE/ISO/SAE. However, this document also takes into account the global scope of C-ITS.

To enable sharing of information in the most efficacious manner on communication platforms with multiple communication stacks, a set of non-overlapping "harmonized" standards is necessary.

4.1 ITS station definition

ITS communications will be comprised of a wide variety of communication nodes/devices connected via a wide variety of networks. These communication nodes/devices will consist of:

- Embedded or after-market devices in vehicles ("vehicular ITS stations").
- Handheld or nomadic devices ("personal ITS stations").
- Devices installed at the roadside ("roadside ITS stations").
- Devices installed in back offices ("central ITS stations").

Until recently, each SDO had its own terminology and communications architecture with relatively large commonalities. As a result, experts from a number of SDOs representing various countries developed the concept of an ITS station (ITS-S), which is described in standard ISO 21217 [7] from the International Standards Organization (ISO). Development of the ITS-S architecture provided structure to the terminology and references, so that now SDOs can exchange documents and re-use or reference information freely.

Having a common architecture, however, does NOT imply that the functions behind it are harmonized, nor does it imply that implementations are standardized. In particular, implementers

are free to build ITS stations that conform closely to the architecture or not at all. In order to interoperate with their peers, however, all ITS stations must conform to a set of standards describing behavior at all exposed/open interfaces, such as wired and/or wireless communication interfaces.

The formal definition of the term ITS station (ITS-S) is an abstract one. At the highest level of abstraction, an ITS-S is a set of functionalities in a bounded secured managed domain that provides communication services to applications residing therein ("ITS-S applications"). From an architectural perspective, an ITS-S is a set of functionalities in an Open Systems Interconnection (OSI)-like layered model (from ISO/IEC 7498-1) based on the abstraction of ITS-S applications from communication protocols serving these ITS-S applications. Included in the set are functionalities to securely manage the applications and communication resources.

The concept of the ITS station and its architecture have been adopted by CEN TC278, by ETSI TC ITS and by ISO TC204.

4.2 ITS station architecture

> While the reference architecture for an ITS station is described here, this architecture does not describe the only suitable architecture. Implementations of ITS stations, such as in a vehicle, may use any internal architecture so long as relevant interoperability requirements are met.

The ITS station architecture was developed by ISO TC204 WG16 and published in ISO 21217 [6]. Further refinements are ongoing, and a revised version of this standard (cf. [7]) is being developed through a harmonization effort between ISO TC204 WG16 and ETSI TC ITS WG2 (cf. EN302 665). The harmonization effort involves recently developed protocol standards and data/message definitions.

The high-level ITS station architecture shown in Figure 1 contains a number of functionalities that are further described in document HTG3-1:2012 (HTG3, *Status of ITS Communication Standards*). The architecture is based on the general OSI reference model, with some adaptations such as compressing the Session, Presentation and Application layers into the Facilities layer. Note that the block "Applications" in Figure 1 is not part of the OSI communication protocol stack, but is using this protocol stack for communications.

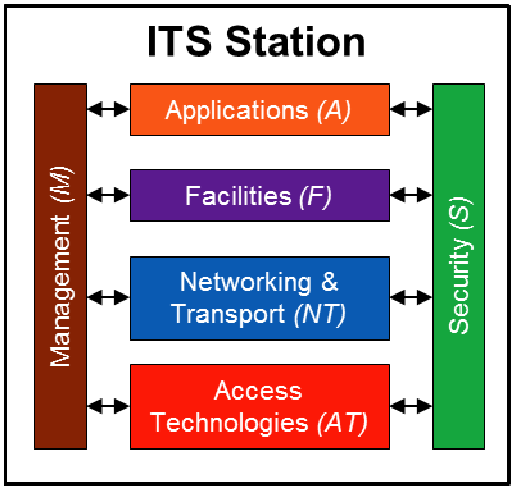

Figure 1: ISO/ETSI ITS station architecture

Source: EU-U.S. ITS Task Force, November 2012.

This architecture comprises applications, lower layer (communications) services and the related management and security services. This abstract architecture, when implemented, may expose internal interfaces for the purpose of allocating functionalities among different boxes and permits, but does not require exposing Application Programming Interfaces (APIs) to enable an open application environment. An implementer may choose to hide these interfaces and APIs completely.

> Implementers of ITS stations, including vehicle manufacturers, may choose to conceal or maintain control over APIs and other internal interfaces to meet their needs. For example, crash-imminent safety or other safety-of-life applications could remain inaccessible to unauthorized parties, should the implementer so choose.

4.3 WAVE station architecture

While the IEEE WAVE reference architecture standard P1609.0 (cf. [39]) has yet to be published, Figure 2 has been adopted by the IEEE 1609 WG and contains a subset of the functionalities shown in the CEN/ETSI/ISO ITS station architecture above. Note that the current IEEE WAVE reference architecture does not explicitly include Facilities or Application layer functions. The colors indicate the correspondences with the ITS station architecture from CEN/ETSI/ISO in a relaxed way. The CEN/ETSI/ISO approach is intended to support (but not require) multiple network stacks from the outset, while IEEE work is focused on a 5.9 GHz radio interface.

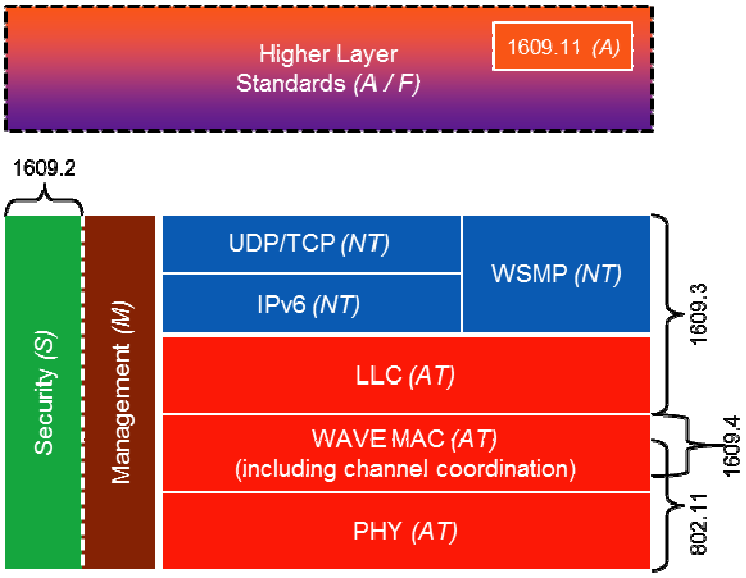

Figure 2: IEEE 1609 WAVE reference architecture

Source: EU-U.S. ITS Task Force, November 2012.

These architecture drawings do not reflect the way to implement the ITS devices. They only form a way to reference and describe the functional behavior and the logical connections between the functional blocks. These logical connections may or may not be implemented as observable interfaces.

One obvious difference between these architecture drawings is how much of the higher level they describe. The Application block and the Facilities layer are mainly outside the scope of IEEE 1609, though P1609.11 specifies Electronic Payment as a service residing on top of the 1609 stack.

> While a reference architecture for a WAVE station is described here, this architecture does not describe the only suitable architecture. A specific WAVE station, such as in a vehicle, may use any internal architecture so long as relevant interoperability requirements are met.

4.4 ITS station implementations

The globally harmonized set of standards for interoperability that are the target of the HTG efforts need to allow for the widest possible variety of implementations of those standards. Figures 3 and 4 below illustrate two of the many possible approaches for implementing an ITS station based on these standards. The figures use the same set of four generic ITS services for illustrative purposes.

4.4.1 Segmented implementations

Figure 3 illustrates four services implemented in separate ITS units:

- Crash imminent safety service ("Hard safety"/collision warning and avoidance).
- Emergency call service (eCall/OnStar, etc.).
- Tolling service (Electronic Fee Collection/ Electronic Payment).
- Infotainment/Sustainability services.

In this model, the services remain separated in stand-alone systems, each remaining in full control of its communication subsystem, HMI, security, etc. While this is clearly a modular approach to deploying services, the model presents challenges in coordinating access to spectrum and to other shared resources.

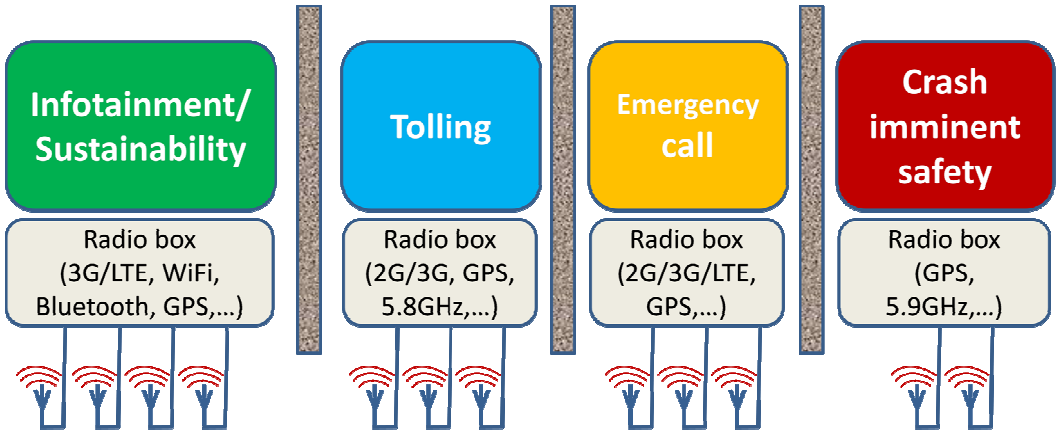

Figure 3: Example of segmented implementation of multiple ITS station applications

Source: EU-U.S. ITS Task Force, November 2012.

4.4.2 Integrated implementation

Figure 4 illustrates an example implementation of the same four services presented in Figure 3, integrated in a single ITS station. This figure also illustrates a crash imminent safety system protected behind a firewall, while all other applications are implemented in a common host. All applications have access to the same radio system, which may contain several different access technologies and networking protocols.

The basic idea behind the integration is to minimize the amount of hardware while supporting the need to protect "crash-imminent safety" operations implemented in a proprietary system behind a firewall from interference by other services implemented on the '"Open" ITS System. The openness of the Open ITS System enables it to support the "App" paradigm familiar in iPhone, Android and Windows Mobile operating systems.

Note that the current security model adopted by SDOs supports this integrated model, and ongoing security related standards development is already actively being harmonized.

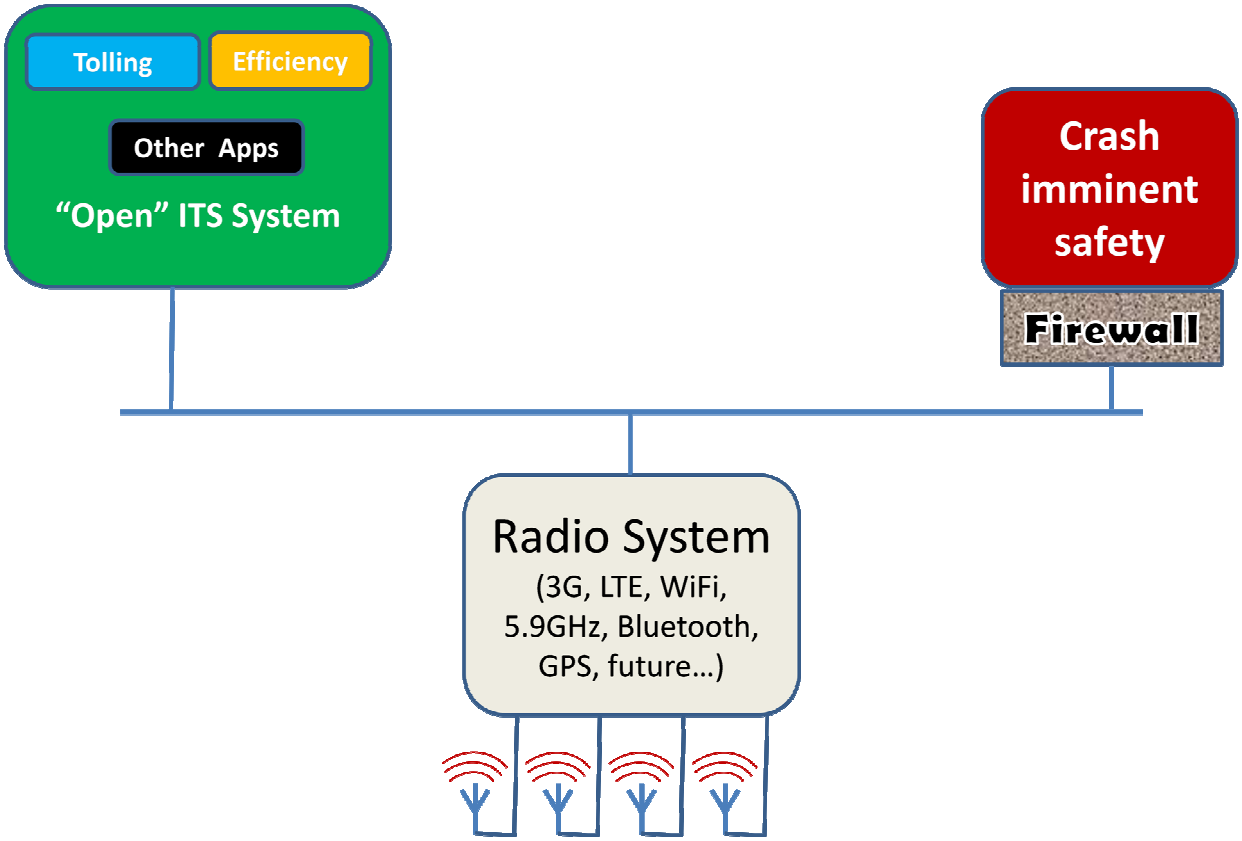

Figure 4: Example of integrated implementation of multiple ITS station applications

Source: EU-U.S. ITS Task Force, November 2012.

4.4.2.1 Crash-imminent safety system

The crash-imminent safety system may be implemented in various ways in a vehicle, depending on the particular design requirements for each vehicle platform. The design may involve single or multiple "Electronic Control Units" (ECUs) in a vehicle or roadside unit, including ECUs, with the responsibility to manage communication and/or security.

The assumption is that the ECUs contain mission-critical functions that require isolation/protection from the effects of other activities in the vehicle. Examples of such critical functions and services include active collision avoidance and commercially sensitive services that need to be implemented in a protected environment. The required isolation is provided using a firewall, as illustrated.

4.4.2.2 "Open" ITS system

The "Open" ITS system is a more open environment where applications can be downloaded, as is done on smartphones and tablet computers, and advantage can be taken of the full set of communication protocols and media available in the integrated implementation. This requires a rich set of functions in the facilities layer to support the ITS station applications, including a strong security component that likely would build on that which the current major “apps” environments offer (iOS, Android and WM).

4.4.2.3 Radio system

The radio system is a device that contains one or more radios. Currently, in Europe and the U.S., it is envisioned that vehicle radio systems will contain at a minimum two 5.9 GHz radios and at least one GPS/GNSS receiver. Other radios such as 4G/LTE and traffic broadcast receivers may also be included in vehicles, as well as personal devices. While minimizing the number of radio systems is advantageous from a cost perspective, it is of critical importance from the perspective of minimizing/avoiding radio interference.

Note that the logical separation between safety and non-safety systems also allows for isolation and prioritization of safety system operation. To have two unsynchronized 5.9 GHz radio systems in one vehicle or collocated in one roadside unit could be damaging for the overall radio performance. Going beyond the 5.9 GHz radios, there are a number of applications and services that require other communications channels and accurate positioning, and it makes good economic sense to integrate these functions.

4.4.2.4 Rationale

The integrated implementation can accommodate everything from legacy functions already deployed in ITS networks to next-generation functions and hardware. Using the integrated approach, advantage can be taken of the full set of communication protocols and media available. For example, applications need not prescribe which radio interfaces to use[2], and in particular may use any available media that meets their requirements.

> The integrated approach significantly reduces the complexity of migration to future communications technologies. For the more integrated approach to be realized, there is a need for a single set of sufficient and non-overlapping standards.

---

[2] Unless required to do so by regional regulations such as mandated 5.9 GHz interfaces for safety services.

5 Use Cases/Applications

In this section, a set of representative Use Cases or Applications that should be considered as the targets for interoperability testing are introduced. These Use Cases are defined at a broad level rather than with great precision, since they are merely the means for showing that the widest possible range of interoperability has been achieved.

5.1 Purpose/Goal of this Section

ITS communication systems provide support for delivering a wide variety of ITS applications/services. In order to demonstrate that the communication system standards harmonization has been a success, it is necessary that the harmonized standards can support the full range of cooperative ITS applications. These applications are highly diverse, and therefore require diverse combinations of communication support.

Some representative cooperative ITS applications are identified in Table 2. This is not meant to be an exhaustive listing of all cooperative ITS applications but it is meant to exercise the range of wireless communication features that are needed by diverse ITS applications. Each application is associated with the type of communication that it is expected to need.

The communication systems were characterized, as shown below, based on similar characterizations used both in a standard text [3] and in ongoing work within ETSI[4].

- Traffic pattern:
  - Unicast.
  - Broadcast.
  - Geocast.
- Network mode:
  - Multi-hop.
  - Single-hop.

---

[3] *Handbook of Intelligent Vehicles*, (Azim Eskandarian, Ed.) Springer, 2012, 1599 pp.

[4] ETSI TS 102 940 V0.0.14 (2012-03), Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management.

- Time criticality:
  - Critical.
  - High.
  - Low.
- Transaction size:
  - Small (single message).
  - Medium (multiple messages but transaction can be completed in the time it takes two vehicles to pass at high speed).
  - Large (larger than medium).
- Transaction frequency:
  - Frequent (multiple times a second, generally a broadcast such as CAM/BSM).
  - Infrequent (once a second or less).
- Endpoints:
  - V2V.
  - V2I/I2V.
  - V2Remote (vehicle to remote infrastructure, reached over a backhaul network).
- Session:
  - Individual messages.
  - Unicast local session.
  - Unicast session with a server remote over the network.
  - Unicast session with a server remote over the network, which must be maintained across several V2I communications sessions.
- Protocol type:
  - Messaging.
  - IP.

These characteristics describe the range of communication alternatives that need to be considered for harmonization. A transaction is defined here as a data exchange that accomplishes one complete application communications operation (e.g., a file transfer or a complete tolling message exchange), also including the broadcast of messages where there is no such data exchange (e.g., broadcast of CAM/BSM).

The different cooperative ITS use cases and applications will require differing combinations of these characteristics in their supporting communication systems, herein called communication scenarios. Various communication scenarios are tabulated in Table 3 and summarized in the paragraphs below.

5.2 Vehicle-Originated Broadcast

Vehicles broadcast information about their movements and safety-related attributes frequently to make sure that this information is available to other vehicles so that they can identify potentially hazardous situations or in support of other applications. This most commonly involves broadcast of Cooperative Awareness Messages (CAM) or Basic Safety Messages (BSM), which are individual single-hop broadcast V2V or V2I messages, with highest time criticality and small but frequent transactions. Application examples include emergency vehicle approach, slow vehicle, emergency electronic brake lights and forward collision warnings. These represent the most time-critical and safety-critical category of connected vehicle applications, since they are used to warn drivers of imminent-crash hazards. Other examples of vehicle-originated broadcasts that are not as time critical and are intended for reception by the infrastructure rather than other vehicles include Mayday messages or stolen vehicle alerts.

5.3 Infrastructure-Originated Broadcast

Infrastructure-originated broadcasts are used to disseminate data that are relevant to all vehicles in the vicinity of a specific road infrastructure location where an RSU is installed, in support of safety, mobility or sustainability applications. These broadcasts are individual, single-hop I2V messages, involving small transactions, with frequent transmission. When used to support the imminent-crash safety applications (e.g., Signal Phase and Timing – SPaT), they are highly time critical, but when used in support of the sustainability applications, they are only moderately time critical, and for in-vehicle traffic sign display applications or broadcast of intersection maps, their time criticality is low.

5.4 Infrastructure-Vehicle-Unicast

Infrastructure-vehicle-unicast messages are individual transactions between a vehicle requesting service from the infrastructure and the infrastructure responding to that vehicle about whether it can provide that service (e.g., traffic signal priority or pre-emption, or access to a location such as a private parking facility). These messages are generally unicast local sessions with low time criticality, low transaction frequency and small transactions.

5.5 Local Time-Critical Sessions

These are combinations of multiple V2I and I2V unicast messages to support time-critical transactions, with small and time-critical transactions. These could be advertised services or financial transactions such as multi-lane open road electronic toll collection. Advertised services refer to services where a Provider unit sends out a message of particular type advertising that the

service is being provided, and a User unit with the corresponding user application connects to the service. This description of advertised services is based on WAVE Service Announcements (WSAs) as specified in IEEE 1609.3.

5.6 Local Non-Time-Critical Sessions

These are combinations of multiple V2I and I2V unicast messages to support non-time-critical transactions, with small- to moderate-size transactions at low frequency, probably using IP. These could be advertised services, such as uploading probe vehicle data, downloading moderate amounts of data such as local or regional traffic conditions, or fleet management or customer relationship management services. For these transactions, multiple frames would be transmitted while a moving vehicle is within range of one RSU.

5.7 Multi-RSU Sessions

Multi-RSU sessions with hand-offs are needed to transfer large quantities of data or to execute transactions that take considerable time, which cannot be accommodated within a single encounter between a moving vehicle and one roadside ITS station, but must be maintained across several V2I/I2V unicast communication sessions with a remote server. These transactions include single-hop, low time-criticality with large and low frequency transactions. This service involves connecting with a service provider across a network, but the logical communication session needs to persist across multiple “touches” between the OBU and a series of RSUs offering access to the backhaul. The persistence may be provided at the application level, the transport layer or the network layer. Example applications would be downloads of large infotainment/media or map update files, some concierge services or continuous web surfing.

Table 2: Representative Cooperative ITS Applications and Their Communication Profiles

Applications	Communication Scenario	Examples
Safety Applications		
V2V Cooperative collision warning	Vehicle-Originating Broadcast	Forward collision warning, blind spot warning, EEBL, emergency vehicle approach warning, overtaking (do not pass) warning.
I2V Cooperative collision warning	Infrastructure-Originating Broadcast	Intersection collision/violation warning, vulnerable road user presence warning.
Roadwork (Work zone) warning	Infrastructure-Originating Broadcast	Low time criticality, but safety critical
Mayday/SOS	Vehicle-Originating Broadcast	Also stolen vehicle alerts
Mobility Applications		
Cooperative Adaptive Cruise Control	Vehicle-Originating Broadcast	Extensions could include platooning
Multi-lane toll collection	Local time-critical session	
Probe data upload	Local non-time-critical session	
Local traffic data download	Local non-time-critical session	Also route guidance, point of interest info
In-vehicle signing	Infrastructure-Originating Broadcast	Static or slow-changing contents
Signal priority or pre-emption	Infrastructure-Vehicle Unicast	
Local access control	Infrastructure-Vehicle Unicast	Parking, loading zone mgt., tolling with barriers
Efficiency/Sustainability Applications		
Basic efficiency improvement	Infrastructure-Originating Broadcast	Broadcast SPaT, then vehicles determine speed profiles
Interactive efficiency improvement	Local non-time-critical session	
Comfort/Convenience/Commercial Applications		
Personal data synchronization	Local non-time-critical session	Synch car computer to home PC
Customer relationship management	Local non-time-critical session	Include remote diagnosis, software updates
Fleet management	Local non-time-critical session	
Large media download	Multi-RSU session	
Web surfing	Multi-RSU session	(For passengers rather than drivers)
Concierge services	Multi-RSU session	

Table 3: Cooperative ITS Communication Profiles

Communication Scenarios (5.9 GHz media only)	Traffic Pattern (unicast,, broadcast, multicast)	Network Mode (Single hop or multi-hop)	Time criticality (critical, high, low)	Transaction size (small, medium, large)	Transaction frequency (frequent or infrequent)	End points (V2V, V2I,/I2V, V2Remote)	Session (individual, local session, remote session, multi-RSU session)	Protocol type (messaging or IP)
1. Vehicle-Originating Broadcast	Broadcast	Single	Critical to Low*	Small	Freq.	V2V, V2I	Individual	Messaging
2. Infrastructure-Originating Broadcast	Broadcast	Single	Critical to Low*	Small	Freq.	I2V	Individual	Messaging
3. Infrastructure – Vehicle Unicast	Unicast	Single	Low	Small	Infreq.	I2V	Individual	Messaging
4. Local time-critical session	Unicast	Single	High	Small	Infreq.	V2I/I2V	Local	Messaging
5. Local non-time-critical session	Unicast	Single	Low	Medium	Infreq.	I2V/V2I	Local	IP
6. Multi-RSU session	Unicast	Single	Low	Large	Infreq.	I2V/V2I	Multi-RSU	IP

* Communication performance has to be governed by critical requirement for most demanding application.

6 Future vision

As described in detail in the "Feedback to ITS Standards Development Organizations" documents, the current set of international ITS standards related to cooperative ITS communications has gaps that should be filled and inconsistencies that should be resolved. This is becoming increasingly important since trials in several regions are currently underway using implementations based on different subsets of these standards. These implementations are not interoperable and cannot be made so without significant investment and re-engineering.

- While direct interoperability between, for example, a vehicle sold for the EU market and one sold for the U.S. market is likely to be a rare requirement, the ability to interoperate offers many potential advantages beyond the opportunity to execute joint demonstrations and tests: To the extent that harmonized standards can permit common hardware and/or software to be used in products destined for multiple regions, both product development and manufacturing costs can be reduced while potentially speeding implementation due to more efficient use of scarce resources.
- Multi-regional interoperability opens markets to suppliers and service providers from other regions, allowing suppliers and service providers to compete in larger markets, driving down costs and increasing innovation.
- While many vehicles may not often travel between regions, carry-in and nomadic devices and their users are expected to have such mobility. These services and applications need to be globally uniquely identifiable and would be expected to serve pedestrians and as carry-in devices for vehicles (e.g., rental cars).

Thus, it is beneficial that ITS communication systems intended for different regions can interoperate to the greatest extent feasible.

The output of this effort has documented in detail the gaps and inconsistencies in existing standardization and technical guidance and has provided that information as feedback to the SDOs in deliverables HTG1-3 and HTG3-3. Our general recommendations with respect to those standards that are necessary and critical for global interoperability going forward are as follows:

- Work on developing overlapping standards should be coordinated, and to the extent possible, consolidated to avoid duplicative efforts and to enable system developers to focus their resources on developing single rather than multiple solutions for the world market. Developing overlapping standards is an inefficient use of scarce resources. If, rather than proceeding independently, parties proceed cooperatively, development time and cost can be reduced while quality and scope may be increased.
- Where multiple standards already exist, the harmonization process should aim to merge them, with the intent to take the "best of each" and produce only a single harmonized

standard for use by all parties. While the technical barriers to such an approach are often manageable, institutional resistance of one or more entities to giving up sole control of standards processes and/or products in favor of harmonization may in some cases prove to be insurmountable. However, in those cases where the benefits appear to justify it, harmonization should be at least attempted.

- Gaps should be filled as soon as possible so that all important interoperability issues are addressed, leading toward implementations that can be as widespread and cost effective as possible. A harmonized, cooperative approach almost certainly offers the best opportunity to address these gaps efficiently and effectively.
- Procedures need to be put in place to determine when these new harmonized standards are sufficiently mature to be suitable for large-scale implementation. These processes, which may include harmonized test procedures, should be conducted to assure that standards are indeed suitable for deployment prior to actions to require/incentivize their use. Even in the case of harmonized or identical standards, individual jurisdictions may choose diverse combinations or include regulatory or voluntary/incentivized approaches to achieve implementation.
- Standards should be designed to support the widest possible range of implementation choices and use cases.

To fully meet these objectives, support from the relevant SDOs, as well as from both the EU and the US authorities, is necessary. With full support, the long-term vision of a single set of critical communication standards for ITS can be realized.

Annex A HTG1 and 3 members

Name	Affiliation / Organization	Region/Country
EU lead: Wolfgang Höfs Emilio Dávila González	European Commission Directorate General on Communications Networks, Content & Technology	EU
US Lead: Steven Sill	US Department of Transportation - Research and Innovative Technology Administration, Intelligent Transportation Systems Joint Program Office	US
Scott Cadzow	Cadzow Communications Consulting Ltd. (sponsor: EC)	UK
Knut Evensen	Q-Free ASA (sponsor: EC)	Norway
Paul Eichbrecht	Vehicle Infrastructure Integration Consortium (sponsor: USDOT)	US
Hans-Joachim Fischer	Elektrische Signalverarbeitung Dr. Fischer GmbH (ESF) (sponsor: EC)	Germany
Frank Kargl	University of Ulm, (sponsor: EC)	Germany
Eric Koenders	Peek Traffic, B .V. (sponsor: EC)	Netherlands
Ola Martin Lykkja	Q-Free ASA (sponsor: EC)	Norway
John Moring	Moring Consulting (sponsor: USDOT)	US
Richard Roy	SRA, Inc.(sponsor: USDOT)	US
Steven Shladover	University of California Berkeley – PATH (sponsor: USDOT)	US
Takaaki Sugiura	Mitsubishi Research Institute on behalf of the Japanese Ministry of Land, Infrastructure, Transport and Tourism (MLIT)	Japan
Siebe Turksma	Peek Traffic, B.V. (sponsor: EU)	Netherlands
William Whyte	Security Innovation (sponsor: USDOT)	US

Annex B Harmonization Task Groups (HTG): General Description (Copy of Original Document)

B.1 Standards Harmonization Objectives and Tasks Overview

The purpose of this document is to provide an overview of how the Standards Harmonization Working Group will facilitate the harmonization of specific standards through the establishment and oversight of Harmonization Task Groups (HTG). An attempt is made to describe the current status of developments related to the issues being addressed in each task and the scope of the proposed efforts for the HTGs. This background information should be useful in assessing the importance of these tasks separately and their value jointly in achieving the common goal of harmonized international standards for ITS.

B.2 Goals

There are currently two goals being pursued by the Standards Harmonization Working Group:

- The long-term goal is harmonization of ITS-related standards between the U.S. and Europe, according to Clause 10 of the EU-US Joint Declaration on Cooperative Systems for ITS.
- The short-term goal is to accelerate progress on a minimum set of standards that could be used in a joint showcase at the Vienna ITS World Congress. The showcase is intended to highlight the progress being made toward achieving harmonization, and to promote the long-term goal of achieving a set of harmonized standards that allows for global deployment of interoperable ITS-related products and services.

It is important to note that the tasks proposed herein will have great value whatever form the showcase will take. The HTGs established by the work group will focus on achieving specific targets within a given time frame. In the performance of these tasks, valuable lessons will be learned which will be useful both for general feedback to SDOs, as well as for developers of test/commercial systems.

B.3 ITS architectures

CEN / ETSI T ISO ITS station architecture

Figure 5 shows the ITS station Reference Architecture created by ISO TC204 and adopted by CEN TC278 and ETSI TC ITS. It has been colored to highlight each of the main functions. This architecture is described in great detail in ISO 21217 [6] and ETSI EN 302 665 [23].

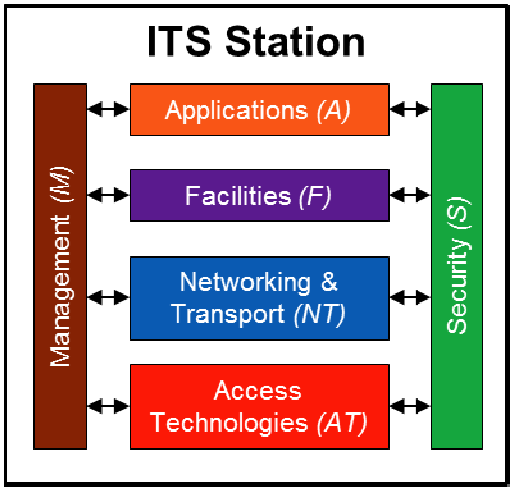

Figure 5: CEN / ETSI / ISO ITS station architecture

Source: EU-U.S. ITS Task Force, November 2012.

B.4 IEEE WAVE device architecture

While the IEEE WAVE device reference architecture (P1609.0) has yet to be published, figure 6 has been adopted by the IEEE 1609 WG and contains a subset of the functionalities shown in the ISO/ETSI/CEN ITS station architecture above. The colors used indicate the correspondence. Also indicated in the figure are the scopes of the various 1609 tasks (1609.2, .3 and .4).

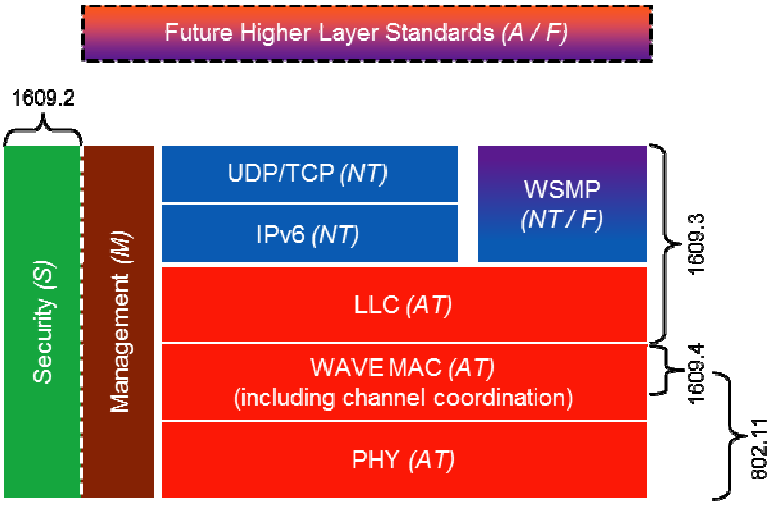

Figure 6: IEEE WAVE device architecture

Source: EU-U.S. ITS Task Force, November 2012.

B.5 ITS global interoperability challenge

The EU and U.S. agreed to cooperate in ITS research in order to achieve interoperability on a national/regional level with a focus on creating a global market for ITS products and services with minimal trade barriers.

Achieving interoperability for mobile ITS stations (personal or vehicular) traveling between different operational regions (e.g., crossing the border between two neighbor countries with different management, registration and security operations) requires both communication interoperability between ITS stations combined with interoperability between back-office systems so that proper operation of safety critical systems and provisioning of expected services can be ensured. This challenge of achieving interoperability across multiple operational regions is even more pronounced if operational regions decide to create their own selection of technical parameters (profiles) which can and often do lead to essential differences in the implementations, in spite of having started from the same set of core standards and technologies.

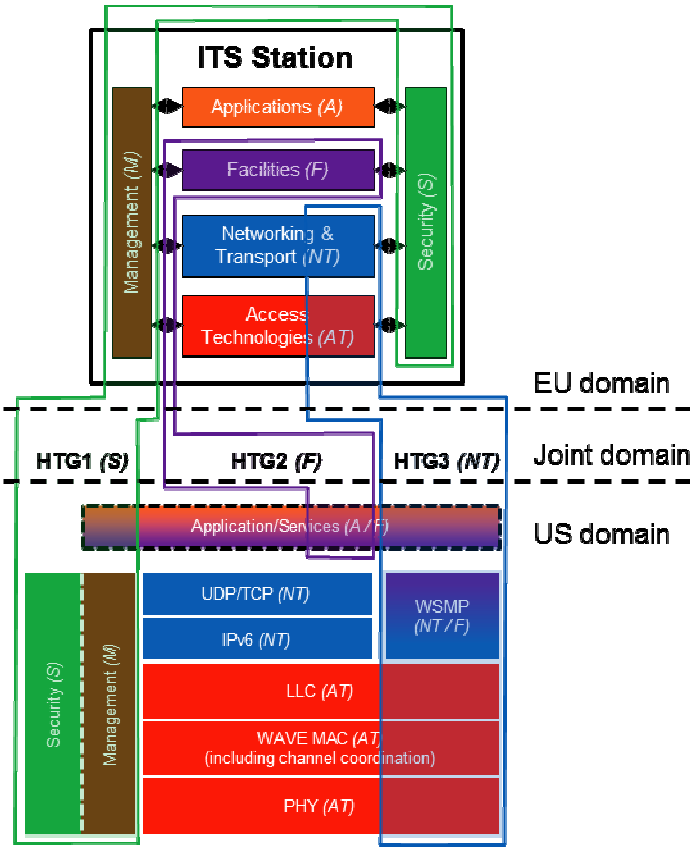

Figure 7: HTG Work Efforts Span EU and US Domains

Source: EU-U.S. ITS Task Force, November 2012.

B.6 Levels of interoperability and their consequences:

0. No interoperability. The Mobile ITS station must be physically exchanged when crossing a border. Not a viable option.

1. Interfaces and functional requirements are compatible, but applications, security and operations are different. Various software components of the ITS station need to be replaced, and if the station is mounted in a vehicle, the vehicle could be registered as a

local vehicle. Could be an option when exporting a vehicle, but not an option for the daily commuter.

2. Mobile ITS stations are functionally identical. All interfaces, functions, apps and security, etc., are based on the same standards, and all stations have passed similar certification procedures, however, the operations of applications and security "affiliated" with regional back-office systems do not talk to each other. Potentially, a new "affiliation" could be loaded at the border, or ITS stations could be configured with dual "affiliations," however, the complexity of setting up and managing this is likely to be more challenging than level 3 below.
3. Mobile ITS stations are functionally identical. All interfaces, functions, apps and security, etc., are based on the same standards, all stations have passed similar certification procedures and the operations of applications and security "affiliated" with regional back-office systems have been "harmonized." The back-offices may be connected in a hierarchical or flat structure.

The differences between 2 and 3 are the formation of agreements between operational centers, and the creation of additional global functions on security, application and identity management. These additional global functions are likely neither complex nor time consuming to create, but may pose political location and operation cost challenges (what country will get which operational center, and how will operations be financed).

Note that both 2 and 3 require common profiles with little variability.

B.7 Standards Harmonization and the Interoperability Challenge

Harmonized standards are needed to achieve Level 1 or higher ITS interoperability. While the long-term goal is to achieve level 3 interoperability for the full range of ITS applications, significant economic and societal benefits may be realized by phased implementation of interoperable ITS applications on a regional basis. EC DG INFSO and US DOT should encourage SDOs to conduct standards development and harmonization activities in such a manner that it supports early implementation of interoperable ITS cooperative systems. The work of the HTGs will contribute to that outcome. Longer term a permanent EU-US ITS technical management team could be set up to advise on standardization harmonization and other issues such as common certification procedures, global ITS registration authorities and common security CA hierarchies, etc.

B.8 Initial Standards Harmonization Task

To expedite the accomplishment of the initial standards harmonization effort described herein, a segmented approach with three parallel Harmonization Task Groups (HTGs) is being used:

- HTG1 will focus on management and security-related issues.
- HTG2 will focus on messages and application interfaces.

- HTG3 will focus on the 5.9 GHz air interface and the communications protocol stack above.

These HTGs will have strong links to the Safety Application WG and the Sustainability Application WG. The HTGs share a common near-term goal to accelerate progress on a minimum set of standards that could be used by the showcase and related demonstrations. To achieve this in the proposed timeframe, the scope of each of the tasks initially needs to be reduced to the essential elements, with the additional restriction that the outcome is a "real scenario." Whatever is developed needs to be scalable and ultimately deployable, and feedback will be provided to regional SDOs for adoption and inclusion in new or revised standards. As such, this work will contribute to establishing the kernel for real interoperability, not only regionally in the Americas and Europe, but also globally.

Each HTG will consist of an appropriate (small) number of experts appointed by DG INFSO and US DOT respectively. Japanese experts are invited to participate as observers on the HTGs. The tasks are clearly delimited, and an aggressive time schedule is proposed in order to provide timely guidance to the ongoing work of the SDOs developing ITS standards, as well as developments aimed for the joint showcase at Vienna World Congress 2012.

The results of the HTG initiatives will be documented in a report and presentation submitted to the Standards Harmonization Working Group. The report could contain recommended general ITS standards harmonization principles and guidance, technical information and recommendations addressing specific standardization issues, and other information the HTG deems relevant. The specific technical details should take the form of a joint profile that refers to standards from the relevant SDOs. By doing this, there is a clear connection to the existing standards so that the same parameter may exist and be referenced to two or more standards. In addition, this will automatically become an overlap and gap analysis for the standards set from ETSI, IEEE, ISO and SAE.

With the Standards Harmonization Working Group concurrence, the HTG report and recommendations will be provided to the SDO working groups for inclusion in the relevant ISO/CEN/ETSI/IEEE/SAE standards.

Annex C Harmonization Task Group 1 (HTG1) (Copy of Original Document)

C.1 Management procedures to support EU-US joint safety and sustainability applications

Current minimum standards focus on the operational interfaces for 5.9GHz protocols and messages between ITS stations (vehicular, roadside, personal) and the related security provisions to protect this communication. This has left out management procedures and operational aspects at the system level, such as how to initiate and maintain services and data in stations (lifecycle: production, initialization, commissioning, operation, destruction). The task of HTG1 is to start filling this gap.

Figure 8 shows the scope of HTG1.

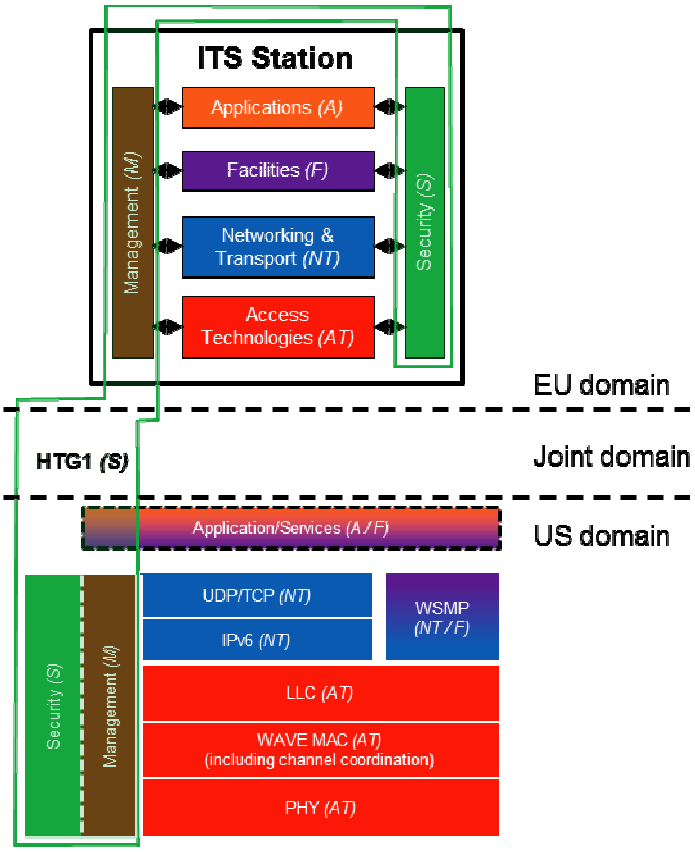

Figure 8: HTG 1 work efforts span EU and US domains

Source: EU-U.S. ITS Task Force, November 2012.

The scope includes:

- Security features for the air interface and networking layers.

- Security features for the implementation (misbehavior detection and certificate revocation).
- Security features for the back office (initialization/CA operation).
- Management of ID and numbering (e.g., applications, protocols, message sets, devices).
- Management of technical platform initialization (correct data and profile selection).
- Management of operations with focus on initial small scale configurations needed for tests and demonstrations requiring interoperability. However the operations view should be scalable to full operations as outlined in the earlier background chapters.

C.2 Task description

The generic standards items to be addressed by HTG1 will be selected by the HTG experts, and the interoperability specification to support a potential joint demonstration should follow these principles:

- Agreement on a common set of trust relation and management features to implement the scope as listed above and:
  - **Limit the initial work to that required to enable interoperability demonstrations, but with a vision for full deployment!**
  - Make a selection from features such as security modules.
  - Define protocols and messages between ITS stations and central system/authorities, including initializing and maintaining security objects.

Note that procedures can be direct (local control) or indirect (linking home register to visiting register).

- Scope limitation:
  - Analytical and protocol groundwork for security and management is assumed to be available for the purposes of HTG1, either as part of current ITS standards work, or from related ICT sectors. Experts need to be familiar with these.
  - Detailed management policy analysis and TVRA (Threat, Vulnerability, Risk Analysis) will not be done as part of the HTG1 work.

Note that these issues still need to be handled. That can happen either afterwards, or in parallel with the HTG work, involving the SDOs, and involving national/regional authorities.

C.3 Group composition

HTG1 will need two to three experts from each region to cover security, policy/management and operations experience. The candidates must be acknowledged hands-on experts with motivation to complete specific assignments. It is essential that the experts are deeply involved in the standardisation effort, preferably in leading technical roles such as editors of standards.

C.4 Proposed structure and candidates

- U.S. lead: Steve Sill <Steve.Sill@dot.gov>
  - Co-manager: Steven Shladover <steve@path.berkeley.edu>
  - Security expert: William Whyte <wwhyte@SECURITYINNOVATION.COM>
  - OEM/Supplier expert: Paul Eichbrecht <peichbrecht@yahoo.com>
  - System/Operator expert: Dick Roy (Richard Roy <dickroy@alum.mit.edu>)
- EU lead: Wolfgang Höfs <Wolfgang.HOEFS@ec.europa.eu>
  - PM: Knut Evensen <knut.evensen@q-free.com>
  - Security expert: Frank Kargl <f.kargl@utwente.nl>
  - OEM/Supplier expert: (TBD)
  - System/Operator expert: Hans-Joachim Fischer <HJFischer@fischer-tech.eu>
- Japan is represented by Takaaki Sugiura <takaaki@mri.co.jp>

C.5 Time plan and milestones

- HTG1 will have three face-to-face meetings during the first half of 2012.
- Work will continue between meetings, based on email exchange, web meetings and a project management tool (WebMeeting).
- The first meeting will have a kick-off session jointly with HTG3, and then focus on drafting straw man for a technical report with two sections:
  - Recommendations for completing management standards and security standards.
  - Technical details for minimum demonstration interoperability between the U.S. and European Cooperative ITS.
  - The meeting will also agree on responsibilities and homework for the experts.
- Second meeting will continue the work and will include a joint session day between HTG1 and HTG3. Very beneficial if HTG2 can join. The goal of the second meeting is to have a stable draft with final tasks that can be done as homework.
- Shortly after the second meeting, a final draft of the technical report should be produced. This draft should be circulated to selected experts for comment and feedback. Feedback due one week before third meeting.
- Third meeting will finalize all agreements on the technical report, so that editorial homework is the only remaining part.
- Completion of technical report within two weeks after third meeting.
- Review and concurrence by Standards Harmonization Working Group principals.
- Distribution to relevant SDOs and R&D projects.
- Follow-up and preparation involvement in showcase events.

C.6 Resource requirements

- Each expert is expected to supply 5 to 10 person weeks of effort. The actual amount of time to be negotiated depending on expert time availability and actual tasks assigned to this expert.
- The experts should be available for the three meetings in Europe and U.S.

Annex D Harmonization Task Group 3 (HTG3) (Copy of Original Document)

D.1 Joint protocols for Safety and Sustainability services

HTG3 will describe a minimalistic joint specification for the 5.9GHz protocols, with a focus on implementable solutions.

This specification should take the form of a *profile* with references to existing standards, wherever possible.

Figure 9 shows the scope of HTG3.

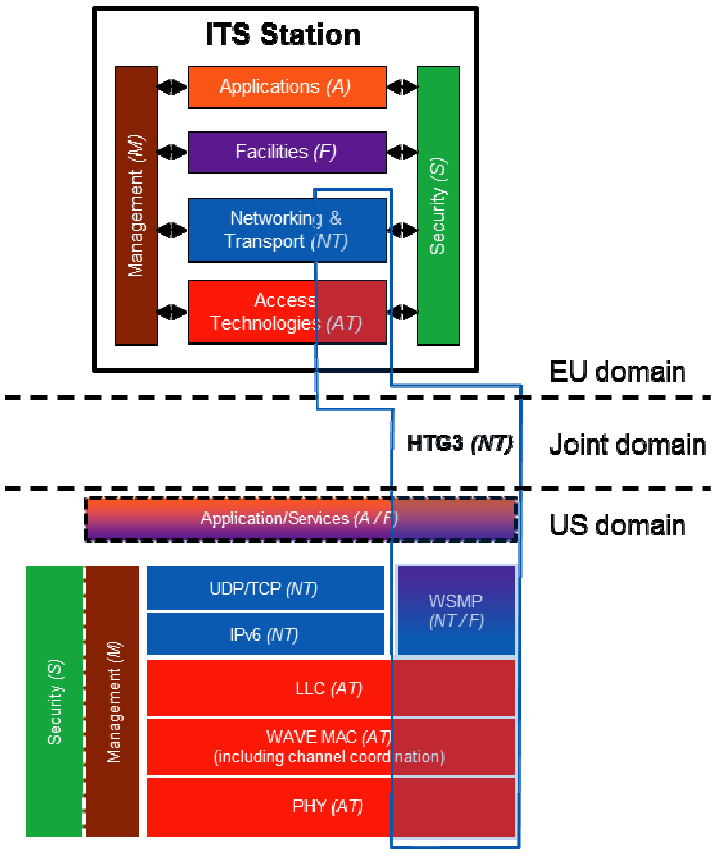

Figure 9: HTG3 work efforts span EU and US domains

Source: EU-U.S. ITS Task Force, November 2012.

The scope includes:

- Parameter selection for PHY/MAC operation in showcase.
- Protocol selection for Link, Network and Transport layer.
- Operational specifications regarding channel usage and congestion issues (tx power levels, repetition rate, etc.).

- Joint test specifications for demonstrating/checking interoperability.

D.2 Task description

- Agree on a common set of parameters, protocols and specifications from scope as listed above, and:
  - **Limit the initial work to that required to enable interoperability demonstrations, but with a vision for full deployment!**
  - Noting that most prototype 5.9 GHz radio implementations available today have dual radios, decide whether a single or dual-channel implementation is feasible in the time constraints and create specifications accordingly, noting that the single channel implementation would be defined as the 5.9 GHz "Control Channel," carrying both BSM/CAM/Service Announcement/Event messages and sustainability app messages.
  - Primary target is to agree on one common protocol stack profile. If this is not possible, alternative dual stack profile implementations shall be defined.
- Scope limitation for a possible joint demonstration or early implementation specification,
  - Other protocols and interfaces, such as 3G, are excluded from this joint demonstration.
  - No multi-hop or IPv6 data transfer will be defined.

Note that these scope limitation issues are still highly relevant for the generic SDO feedback process and for a quick deployment. These issues, therefore, need to be handled afterwards or in parallel, involving the SDOs and national/regional authorities.

D.3 Group composition

HTG3 will need three experts from each region to cover PHY/MAC, mid-level protocols, vehicle specific interfaces and roadside specific interfaces, and communications policy/management/architecture experience from both an OEM and system supplier perspective. The candidates must be acknowledged hands-on experts with in-depth knowledge of current (international) test implementations, and must be highly motivated to complete this task. It is essential that the experts are deeply involved in the standardization effort; preferably in a leading technical role such as editors of standards. Some of the experts should be involved in the implementation and showcase events to achieve continuity. Overlap between HTG1 and HTG3 is beneficial.

D.4 Proposed structure and candidates

- U.S. lead: Steve Sill <Steve.Sill@dot.gov>
  - Co-manager: Steve Shladover <steve@path.berkeley.edu>
  - OBU Supplier expert: John Moring <john@MORING.NET>
  - OEM expert: Paul Eichbrecht <peichbrecht@yahoo.com>
  - IEEE/Architecture expert: Dick Roy (Richard Roy <dickroy@alum.mit.edu>)

- EU lead: Wolfgang Höfs <Wolfgang.HOEFS@ec.europa.eu>
  - PM: Knut Evensen <knut.evensen@q-free.com>
  - ETSI/CALM protocol expert: Hans-Joachim Fischer <HJFischer@fischer-tech.eu>
  - RSU Supplier expert: Eric Koenders <eric.koenders@peektraffic.nl>
  - System/Architecture expert: Ola Martin Lykkja <Ola.Lykkja@q-free.com>
- Japan is represented by Takaaki Sugiura <takaaki@mri.co.jp>

D.5 Time plan and milestones

- HTG3 will have three face-to-face meetings during the first half of 2012 (see HTG Schedule document).
- Work will continue between meetings, based on email exchange, web meetings and project management tool (WebMeeting).
- The first meeting will have a kick-off session jointly with HTG1, and then focus on drafting a straw man for a technical report with two sections:
  - Recommendations for completing communications standards.
  - Technical details for minimum demonstration interoperability between the U.S. and European Cooperative ITS.
  - The meeting will also agree on responsibilities and homework for the experts.
- Second meeting will continue the work, and will include a joint session day between HTG1 and HTG3. Very beneficial if HTG2 can join. The goal of the week is to have a stable draft with final tasks that can be done as homework.
- One week after the second meeting, a final draft of the technical report should be produced. This draft should be circulated to selected experts for comment and feedback. Feedback due one week before third meeting.
- Third meeting will finalize all agreements on the technical report, so that editorial homework is the only remaining part.
- Completion of technical report within two weeks after third meeting.
- Review and concurrence by Standards Harmonization Working Group principals.
- Distribution to relevant SDOs and R&D projects.

D.6 Resources required

Each expert is expected to supply 5 to10 person weeks of effort. The actual amount of time to be negotiated depending on expert time availability and actual tasks assigned to this expert.

The experts should be available for the three meetings in Europe and U.S.

Annex E ITS Communication and Security Issues Related to Border Crossing

E.1 Introduction

Issues related to border crossings are of particular importance in globally harmonized ITS communication systems since, by their very nature, transportation systems involve the movement of people and goods across large geographic areas that are composed of potentially many sovereign geopolitical regions.

http://upload.wikimedia.org/wikipedia/commons/d/da/Baarle-Nassau_fronti%C3%A8re_caf%C3%A9.jpg

Figure 10: Example of a European border that is crossed often.

Baarle-Hertog / Baarle-Nassau photo used with permission by Norbert Banhidi.

Figure 11: Example of a North American border that is crossed often.

San Ysidro Border Crossing, photo used with permission by Phil Konstantin.

Each sovereign region has the right to establish its own policies and procedures with regard to two very important issues related to ITS communications: 1) RF spectrum usage, and 2) information privacy and security including lawful intercept.

Note that while there are many other aspects that can be controlled by authorities, focus is on these two.

These issues are made more complex near regional boundaries because of the vagaries of RF communications. RF signals easily propagate across such boundaries and among other things, the question arises as to what rights and responsibilities the transmitter of information in one region has when the information transmitted is received in another. Such issues, while beyond the scope of the HTG effort, point out some interesting challenges that secure and regulated wireless communications face when operating near regional boundaries. For example, noting differences in ISM spectrum allocations (Wi-Fi at 2.4 GHz), the U.S. and Canada have entered into agreements as to how spectrum can and will be managed by Wi-Fi access points whose RF transits the border between the two countries.

For our purposes, it suffices to realize that:

> There will exist borders on each side of which there can and will be different regulations involving RF spectrum usage and different policies regarding security and protection of (personal) information.

It is important to recognize that the borders related to RF usage and security policies may be different. For example, a region may adopt the same RF regulations as its neighbor; however, it may choose a different set of security and privacy policies. In this case, there is effectively no RF boundary; however there is a security boundary. Furthermore, a regional authority may also choose to segment further its own region, either in terms of RF regulations or security policies. Segmentation may also arise from different operators in the private sector (e.g., different road operators, which again may use different RF, security, or privacy policies). Thus, for the purposes of this effort, it is important that each of the issues (RF and security) be considered and treated separately.

Additional complications in crossing a border arise when disparate lower-layer communication protocols (e.g., WSMP (IEEE 1609.3) vs. FNTP (ISO 29281-1)) are specified for use in the two regions. In the following sections, it is assumed that the lower layer communication protocols on both sides of the border are the same. While this issue can be avoided by having a single globally harmonized lower-layer communication protocol for safety-related applications, disparate protocols could be addressed in a manner similar to that used to address different RF parameters. by requiring all ITS stations crossing the border to support both lower layer protocol sets in addition to being required to support communications using the different RF parameters.

E.2 Border crossing scenarios

This section describes what is anticipated to be very common examples of information exchange at a border crossing on a road that conveys traffic between two regulatory (and security policy) domains (see Figure 11). Herein, the following equipment configuration is assumed:

- Border Crossing Mobile (vehicular/personal) ITS stations (BCM-ITS-S) are outfitted with GNSS receivers.
- Border Crossing Roadside ITS stations (BCR-ITS-S) know their coordinates and have detailed topological maps (TMs) of the area around the border crossing, including the location of the border itself.
- Border Crossing Roadside infrastructure has access to the latest RF regulations and security policies for both regions.

Additionally, ITS stations, both mobile and roadside, are assumed to have 5.9 GHz radios with a common lower-layer communication protocol stack and a globally harmonized message set containing the necessary message structures for distribution of RF and security-related

information throughout the ITS communication network. Examples of potential information exchange include:

1. A BCM-ITS-S knows its location and has regulatory information for both regions, which happens to be identical for both regions. It receives broadcasts from the nearby BCR-ITS-S containing version information and determines it has the latest regulatory and security information for operation in the next region as well as the latest border crossing TM. The BCM-ITS-S crosses the border with no change in configuration of its radios or security services.
2. A BCM-ITS-S knows its location and has regulatory information for both regions. It receives broadcasts from the nearby BCR-ITS-S containing version information and determines it has the latest regulatory and security information for operation in the next region as well as the latest border crossing TM. It uses its GPS location and the TM to assess when to switch the RF parameters of its 5.9GHz radios and change how it accesses the security services it may need (certificate requests, revocation list downloads, etc.). The RF switch occurs as it crosses the border. If the new security policies require the use of a specific set of credentials (e.g., certificates), the BCM-ITS-S starts using these credentials as well. The security service changes are instituted the first time the BCM-ITS-S detects the presence of infrastructure (on its 5.9GHz medium or any other) that provide security services.
3. A BCM-ITS-S knows its location and has regulatory information for both regions. It receives broadcasts from the nearby BCR-ITS-S containing version information and determines it does not have the latest regulatory and security information for operation in the next region, nor does it have the latest border crossing TM. The BCM-ITS-S and BCR-ITS-S engage in a unicast session on a service channel to update the BCM-ITS-S with all information necessary for proper operation in the next region. The BCM-ITS-S then uses its GPS location and the TM to assess when to switch the RF parameters of its 5.9GHz radios and change how it accesses the security services it may need (certificate requests, revocation list downloads, etc.). The RF switch occurs as it crosses the border. If the new security policies require the use of a specific set of credentials (e.g., certificates), the BCM-ITS-S ceases use of the previous credentials. The security service changes are instituted the first time the BCM-ITS-S detects the presence of infrastructure (on its 5.9GHz medium or any other) that provide security services, at which time it requests certificates from the appropriate authority that will allow it to continue authenticated/secure operation in the new region.

E.3 RF-related issues

Crossing of a border (regional boundary) with disparate RF regulations in the adjoining regions necessitates a change in configuration of the radios used to wirelessly communicate.

The decisions to be made as to when and where to make such changes may themselves be governed by mutual agreements between two regulatory bodies. In such situations, it is of primary importance to have information about "where am I and where am I going" and "what are the new rules when I get there" in order to make the appropriate changes at the appropriate time.

There are fundamentally two mechanisms by which an ITS station can ascertain the regulatory domain within which it is currently operating:

- GPS (or some similar autonomous location service) and a map of the appropriate regulatory regions.
- Information broadcast/transmitted from a fixed ITS station indicating the regulatory region of operation. (Note: stations on borders could use directional antennas to minimize RF overlap into adjacent regions if that were thought to be beneficial.)

Operationally, a combination of these two mechanisms would be preferred.

From the RF wireless communications standpoint, what would be required are:

- Mechanisms for supplying regulatory region information, including:
  - An identifier of the current (RF) regulatory region.
  - An identifier of the neighbor (RF) regulatory region if the fixed ITS station were near a border.
- Mechanisms for ensuring the mobile ITS station had access to the policies and regulations in the adjacent region using:
  - A push mechanism to broadcast such information (on a regulatory information advertisement channel).
  - A pull mechanism whereby a unicast session (on a regulatory information session channel) could be entered into between the fixed and the mobile ITS stations to download the required information.
  - Local storage in the mobile ITS station which is preloaded with information for all relevant regions.

While currently outside the scope of this effort, a globally harmonized message involving encoding of regulatory information is necessary to meet these requirements.

E.4 Security and privacy-related issues

Herein, "mobile devices" are defined to be any device that moves around while it's operating, such as vehicle-mounted devices, aftermarket devices, personal devices and even VMSs on a slowly moving vehicle. The following security and privacy issues may arise when mobile devices cross borders between two domains.

- Differing security mechanisms
- Differing privacy policies

- Trusting received messages
- Sending trustable messages
- Maintaining unlinkability

To address these issues, generally what would be required are:

- Mechanisms for supplying security and privacy region information, including:
  - An identifier of the current (security) regulatory region.
  - An identifier of the neighbor (security) regulatory region if the fixed ITS station were near a border.
- Mechanisms for ensuring the mobile ITS station has access to the policies and procedures in the adjacent region, such as:
  - A push mechanism to broadcast such information (in a regulatory information advertisement).
  - A pull mechanism whereby a unicast session could be entered into between the fixed and the mobile ITS stations to download the required information.
  - A push or pull mechanism to disseminate such information via cellular networks.
  - Local storage in the mobile ITS station, which is preloaded with information for all relevant regions.

> While outside the scope of this effort, a globally harmonized message set involving encoding of security and privacy related information is essential to meet these requirements.

E.5 Differing security mechanisms

Ideally, differing security mechanisms between two regions (e.g., different algorithms, different certificate formats or differences in security-related PDU contents) should be avoided. If they are unavoidable, then globally harmonized means for retrieval and dissemination of information about the security mechanisms are essential. Such means may include distribution using management messages sent to mobile devices. Information contained within security headers of PDUs (e.g., a security policies and procedures ID) can also be used to infer that different security mechanisms are used in the neighboring region. Current ITS standards do not support such distribution of security information.

Changes in the certificates used will require the device to have access to certificates. This requires some form of data connectivity to a CA at some point. The requirements are discussed in more detail in clause E.9.

E.6 Differing privacy policies

Different jurisdictions may have different privacy policies with regard to:

- Linkability of information for law enforcement.
- Requirements for a minimum level of privacy.

- Legality of certain law enforcement actions (e.g., automatically issuing speeding tickets).
- Enforcement of restrictions on movement (e.g., barring a particular person from leaving the country).

A change in privacy policy may result in changes to device behavior, including one or more of the following:

- Change in parameters and fields in messages sent over the air.
- Change in certificates used:
  - Contents.
  - Lifetime.
  - Change algorithm.
  - Resolvability.

Additionally, there may be a change in the legal environment that affects the user's situation without necessarily directly affecting device behavior. For example, law enforcement may have greater rights to link transmissions to drivers in region B than in region A. An open question is whether the system should alert a driver from region A that their privacy is at greater risk when they drive into region B, or take some other action (e.g., allowing the driver to opt out of transmission altogether, if region B allows opt-out).

E.7 Trusting received messages

The mobile device needs to be able to trust messages that it has received from other devices, both vehicle-based and other. This requires it to be able to trust the certificates that other units hold. This can be accomplished in a number of ways:

1. All certificates for all types of devices are issued by a chain back to a single root.
2. Mobile devices can be instructed to trust more than one root certificate.
   a. The set of trusted root certs may be updated over the air.
   b. The set of trusted root certs may be updated via physical contact.
   c. The set of trusted root certs is fixed at install time and may not be changed.

Approach (1) does not seem to be realistic, as it would require worldwide agreement and coordination. Messages should be defined to support (2a), allowing root authorities known to an ITS-S to introduce other root certs. OEMs and device manufacturers may define mechanisms to support (2b). Likewise, one might be able to implement (2b) at border crossings or dealerships where you would have to (or might choose to) stop anyway (e.g., to buy toll tickets). Finally, (2c) is not recommended as it would significantly reduce flexibility.

E.8 Sending trustable messages

The mobile device needs to be able to send messages that other vehicles will accept. This requires it to have a certificate that will be accepted by other vehicles. This can be accomplished in a number of ways:

1. All mobile device certificates are issued by a chain back to a single root certificate.
2. Mobile devices in one domain are instructed to trust certificates issued within a different domain.
3. When mobile devices cross from one domain to another, they are issued with certificates that are trusted within the new domain.

Approach (1) is probably not realistic for the reasons discussed in the previous section. Approach (2) above is the most flexible, but may affect privacy as the sender will be more easily identifiable in "foreign" regions (the anonymity set size will be reduced significantly). This is discussed further under "maintaining unlinkability" below. To provide better privacy, approach (3) should be supported in addition to approach (2).

Obtaining new certificates (i.e., approach 3) requires some form of data connectivity to the CA. The requirements are discussed in more detail under "maintaining unlinkability" below.

A regional authority may want to control which messages are trusted:

1. By vehicles physically within the region.
2. By vehicles originating or registered within the region, even if those vehicles are driving outside the region.

For example:

- Region A authorities say "only trust Region A certificates when you are in Region A" to Region A vehicles.
- Region A authorities say "only trust Region A certificates when you are in Region A" to non-Region A vehicles.
- Region A authorities say "only trust Region A certificates anywhere" to Region A vehicles.
- Region A authorities say "only trust Region A certificates anywhere" to non-Region A vehicles when they cross into Region A.

It is not clear which of these scenarios should be supported by an international ITS system. Case (1) above seems clearly legitimate, case (4) is clearly problematic, and the others are somewhere between. It may be necessary to define message sets to allow authorities to distribute trust policies to vehicles. The policies that can be communicated should be carefully scoped to prevent abuse.

E.9 Maintain unlinkability

If the mobile device only has certificates issued by its originating domain, and no certificates from its current domain, it will be distinguishable from the majority of the devices around it because its certificates have a different CA identifier. To preserve privacy against linking (or tracking), the device needs to obtain certificates appropriate for the current domain.

This can be approached in a number of ways:

1. The loss of privacy is not a significant matter; the mobile device does not get new certificates. (The ability to track devices from another domain may be a desirable feature under certain circumstances.) Certificates from region A must be acceptable in region B.
2. The loss of privacy is somewhat significant; the mobile device should obtain certificates after crossing into the domain but will be traceable until it can start using those new certificates. Certificates from region A must be acceptable in region B.
3. The loss of privacy is somewhat significant. There is a border zone within which certificates from both domains are accepted (say the area within 50 kilometers of the border in both regions). A device can request certificates for the second domain on entering the border zone, and start using the certificates at any point up to the point at which it leaves the border zone. Certificates from region A must be acceptable in the border zone within region B, but need not be acceptable outside the border zone.
4. The loss of privacy needs to be addressed immediately; the mobile device will obtain new certificates the moment that it crosses the border and use them as soon as possible. Certificates from region A must be acceptable close to the border in region B but need not be acceptable away from the border zone.
5. The loss of privacy needs to be addressed immediately; the mobile device provisionally obtains certificates before it crosses the border and starts to use them once it crosses the border. Certificates from region A need not be acceptable within region B.

The following issues should be taken into consideration. These issues are not unique to border crossings, but may gain additional significance in a border crossing setting. See HTG1 Report 1 for a more complete discussion of the background.

- Privacy against the PKI.
    - We assume that the act of requesting a certificate gives away some information about the requester's location, although this information may be very coarse (for example, if it simply identifies that the requester is somewhere near the US/Canadian border). In general, for certificate request, we recommend the use of mix networks/anonymous routing between the vehicle and the PKI to obscure the physical location of the vehicle at the time of the request.
    - If crossing or approaching a border results in a certificate request that would not otherwise have happened, this somewhat reduces the requester's privacy against the PKI (although the reduction may be very small).
    - If any component of the PKI knows the set of certificates that have been issued to a single vehicle, an insider at that component can track that vehicle. To reduce this risk, the CAMP design proposes that certificate requests from multiple vehicles are shuffled together before submission to the CA. This requires aggregating requests that have been received over some period of time. In the border crossing scenario, if it is important to obtain the new certificates quickly, this reduces the period of time available for aggregating certificate requests and so reduces the ability to obscure a particular vehicle's certificate set from the PKI.

- Sybil attacks: In a Sybil attack, a device that is compromised masquerades as multiple devices. If a mobile device that crosses borders obtains certificates for the new domain, and if certificates from one domain are acceptable in another, then the device can mount a Sybil attack by using the certificates from both domains at the same time in the same place. If certificates from one domain are not acceptable in another, then the device can send fake messages in multiple domains simultaneously but cannot pretend to be multiple devices in a single domain.
- Data connectivity to the CA: connectivity between the CA and a mobile device is not guaranteed.
- Acceptability of certificates across domains: do receivers in region B need to trust certificates issued by region A?
- Limited storage space on mobile devices: it is not clear how many certificates a mobile device is able to store simultaneously. If a device is issued with additional certificates, it may have to delete existing certificates to store the new ones.

Based on these considerations, we evaluate the alternatives for unlinkability as follows:

1. **No new certificates**: The device loses a lot of privacy against eavesdroppers, but maintains privacy against the CA, has no increased ability to mount Sybil attacks, and does not need data connectivity to the CA to support obtaining new certificates. Certificates must be acceptable across domains. The solution is consistent with poor data connectivity to CAs.
2. **Certificates after crossing**: The device has reduced privacy against eavesdroppers for a limited time. There is a trade-off between privacy against eavesdroppers and privacy against the CA – the longer the device waits to apply for new certificates, the less clear it is to the CA where the device is, and the longer the device can wait between applying for new certificates and receiving them, the more the system can mix its request with others, but both of these delays come at the expense of privacy against eavesdroppers. Certificates must be acceptable across domains. This allows a device to mount Sybil attacks unless its old certificates are revoked (which in turn means that it needs another set of certificates if and when it returns to its original domain). The solution is consistent with poor data connectivity to CAs. The device only has to store one set of certificates at a time, assuming that the certificates from the old domain can be either discarded or reissued when the device crosses back. (Reissued is better.)
3. **Border zone**: Within the border zone, the anonymity set size of a vehicle is somewhat reduced, although it is reduced less than in the other alternatives. The device may choose not to request new certificates at the instant when it passes into the border zone, which allows it to control the privacy loss to the CA; it may also choose the time at which it passes out the other side of the border zone, allowing more time for the system to mix its request with others. Certificates from both domains must be acceptable within the border zone. The device may mount Sybil attacks within the border zone unless its old

certificates are revoked (which in turn means that it needs another set of certificates if and when it returns to its original domain). The solution is consistent with poor data connectivity to CAs. The device may choose only to store one set of certificates at a time, assuming that the certificates from the old domain can be either discarded or reissued when the device crosses back, or to store two.

4. **Certificates immediately upon crossing**: The device has privacy against eavesdroppers, but loses privacy against the CA. Certificates need not be acceptable across domains, limiting the scope of Sybil attacks. The solution is not consistent with poor data connectivity to CAs. The device only has to store one set of certificates at a time, assuming that the certificates from the old domain can be either discarded or reissued when the device crosses back.
5. **Certificates before crossing**: The device has privacy against both eavesdroppers and the CAs, but may have to store certificates for multiple domains simultaneously (how does it decide which domains to request and store certificates for?). This means that this approach needs more storage space than others (assuming that the total length of time for which certificates must be obtained is fixed). Certificates need not be acceptable across domains. The solution is somewhat consistent with poor data connectivity to CAs, except that if a vehicle crosses a lot of domains quickly, it may not be able to get certificates for the later domains.

E.10 Maintaining application functionality

As discussed in the previous sections, a mobile station crossing a border may have to change its RF parameters to comply with the new local regulations. This would mean that from that moment on, application messages would be transmitted using different RF parameters. Clearly, mobile stations on the other side of the border would no longer be able to receive these messages unless they had transceivers tuned to the correct RF parameters. This clearly has a significant impact on the effectiveness of safety-related applications (cf. CAMs, DENMs, BSMs) at border crossings.

To ensure application functionality at a border:

- Mobile stations could be required to receive and send using both the local RF parameters and those required on the other side of the border. This would require onboard systems to support from two to four radio channels simultaneously.
- A roadside station at the border could relay relevant application messages from one side of the border to the other, translating them from one set of RF parameters to the other. For this purpose, the road side station would have to be equipped with as many radio channels as necessary. Directional antennas could be used to reduce the transmission of messages with non-local RF parameters into each region.

Note that if different lower-layer communication protocols were specified for use on each side of the border, protocol translation in addition to RF parameter translation would be required in the

road side station, and mobile stations would be required to support both lower-layer communication protocols as well.

E.11 Conclusions

While a single globally harmonized set of RF regulations and security policies and procedures would be ideal for ITS communication systems, it is more realistic to assume that there will be regional variations in these two critical features of ITS communications. To address these variations, globally harmonized mechanisms for exchange of higher-layer regional regulatory and security-related information and flexible ITS-S implementations (e.g., ability to operate with different RF parameters) are essential to ensure that ITS stations that move from one region to another can continue to function in a safe and secure manner as seamlessly as possible. Such mechanisms also accommodate future changes in these regulations and policies, as well as changing border configurations. To achieve these goals, the following are necessary:

- A globally harmonized message containing all RF parameters subject to regulation
- A globally harmonized message containing all security, privacy, and authenticity related parameters subject to change
- A globally harmonized protocol for exchange (push and pull) of such information between ITS stations and the appropriate regulatory authorities

Annex F References

References without a date in the title refer to documents that are currently under development and thus not publicly available.

F.1 ISO

[1] NWI 16444, Intelligent transport systems—Communications access for land mobiles (CALM)—Geo-Routing

[2] ISO 16788, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 networking security

[3] ISO 16789, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 optimization

[4] ISO 21210:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 Networking

[5] ISO 21215:2010, Intelligent transport systems—Communications access for land mobiles (CALM)—M5

[6] ISO 21217:2010, Intelligent transport systems—Communications access for land mobiles (CALM)—Architecture

[7] Revision of ISO 21217, Intelligent transport systems—Communications access for land mobiles (CALM)—Architecture

[8] ISO 21218:2008, Intelligent transport systems—Communications access for land mobiles (CALM) —Medium service access points

[9] DIS 21218:2012, Intelligent transport systems—Communications access for land mobiles (CALM) —Access technology support

[10] ISO 24102:2011, Intelligent transport systems—Communications access for land mobiles (CALM) —Management

[11] DIS 24102-1:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 1: ITS station management

[12] ISO/NP 24102-2:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 1: Remote management

[13] DIS 24102-3:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 3: Management SAPs

[14] DIS 24102-5:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 5: Fast service advertisement protocol (FSAP)

[15] ISO 29281:2011, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking

[16] DIS 29281-1:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking—Part 1: Fast networking & transport layer protocol (FNTP)

[17] DIS 29281-2:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking—Part 2: ISO 15628 support

[18] PWI, Intelligent transport systems—Communications access for land mobiles (CALM)—Conformance Requirements

[19] Draft TR 17465 1Intelligent transport systems—Terms, definitions and guidelines for Cooperative ITS standards documents—Part 1: Terms, definitions and outline guidance for standards documents

[20] ISO/IEC 7498-1, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model

F.2 CEN

[21] Draft CEN ISO 17419, Classification and management of ITS applications in a global context

[22] Draft CEN ISO 17423, Intelligent Transport Systems—Cooperative Systems—Application requirements for selection of communication profiles

F.3 ETSI

[23] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture

[24] 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

[25] ETSI TS 102 860 V1.1.1 (2011-05), Intelligent Transport Systems (ITS); Classification and management of ITS application objects

[26] Draft ETSI TS 102 965, Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list

[27] Online registry for ITS-AID: http://aid.its-standards.info/ITS-AID Registry/ITSaidRegistrationIndex.html

[28] ETSI TR 102 962 V1.1.1 (2012-02). Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)

[29] 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

[30] ETSI TS 102 636-x, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking
Part 1: Requirements (2010-03)
Part 2: Scenarios (2010-03)
Part 3: Network architecture (2010-03)
Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications
- Sub-part 1: Media-Independent Functionality (2011-06)
- Sub-part 2: Media dependent functionalities for ITS-G5A media (draft)
Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol (2011-02)
Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols (2011-03)

[31] ETSI EN 302 931 V1.1.1(2011-07), Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition

[32] ETSI TS 102 890-2, Intelligent Transport Systems (ITS); Facilities layer function Part 2: Services announcement specification

[33] 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

F.4 IEEE

[34] IEEE 802™:2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture

[35] ISO/IEC 8802-2:1998, ANSI/IEEE Std 802.2™:1998, IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 2: Logical Link Control

[36] IEEE Std 802.3™:2000, IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 3: Carrier senses multiple access with collision detection (CSMA/CD) access method and physical layer specifications

[37] Ethertype registry:
http://standards.ieee.org/develop/regauth/ethertype/public.html

[38] IEEE Std 802.11™:2012, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[39] IEEE P1609.0™ D3, Draft Guide for Wireless Access in Vehicular Environments (WAVE)—Architecture

[40] IEEE P1609.2™ D15, Draft Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages

[41] IEEE Std 1609.3™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services

[42] IEEE Std 1609.4™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation

[43] IEEE Std 1609.11™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transport Systems (ITS)

[44] IEEE P1609.12™:D6, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Identifier allocations

F.5 Regulations

[45] FCC 47 CFR 90 Telecommunications, Private land mobile radio services, 371 – 377: Regulations governing the licensing and use of frequencies in the 5850–5925 MHz band for dedicated short-range communications service (DSRCS)

[46] FCC 06-110 Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band); MOO to designate channels 172 and 184 for safety of life and property usage

[47] FCC 47 CFR 15 Telecommunications, Radio frequency devices

[48] ETSI EN 302 571 V1.2.1: 2008, Intelligent Transport Systems (ITS); Radio communications 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

[49] ETSI EN 301 893 V1.7.1: 2012, Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

F.6 Testing

[50] ETSI EG 202 798V1.1.1 (2011-01), Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing

[51] ETSI TS 102 985-1 V1.1.1 (2012-07), 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) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

[52] ETSI TS 102 797-1 V1.1.1 (2012-08), 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
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

[53] ETSI TS 102 868 V1.1.1 (2011-03), Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM)
Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)

[54] 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)
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)

F.7 Other references

[55] HTG1&3-1:2012, Overview of Harmonization Task Groups 1&3

[56] HTG1&3-3:2012, Observations on GeoNetworking

[57] HTG1-1:2012, Status of ITS Security Standards

[58] HTG1-2:2012, Testing for ITS Security

[59] HTG1-3:2012, Feedback to Standards Development Organizations – Security

[60] HTG3-1:2012, Status of ITS Communications Standards

[61] HTG3-2:2012, Testing for ITS Communications

[62] HTG3-3:2012, Feedback to Standards Development Organizations – Communications

[63] IANA, Port number registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

[64] SAE J2735: DEDICATED SHORT RANGE COMMUNICATIONS (DSRC) MESSAGE SET DICTIONARY

ANNEX G Glossary

Table G.**4** below lists acronyms used in documents produced by HTG1 and HTG3.

Table G.4: Acronyms

Acronym	Meaning	Reference
API	Application Programming Interface	[7]
BRAN	Broadband Radio Access Networks	[49]
BSM	Basic Safety Message (from SAE)	
BSMD	Bounded Secured Managed Domain	[7]
BSS	Basic Service Set	[38]
BTP	Basic Transport Protocol	[30]
CA	Certificate Authority	
CAM	Cooperative Awareness Message (from ETSI)	
CCH	Control Channel	[21, 24, 41]
CEN	Comité Européen de Normalisation	http://www.cen.eu
CI	Communication Interface	[9]
CIP	Communication Interface Parameter	[16]
C-ITS	Cooperative ITS	[7, 19]
CTX	Context message	[14]
DCC	Distributed Congestion Control	[29]
DENM	Decentralized Environmental Notification Messages (from ETSI)	
DIS	Draft International Standard	ISO
DSAP	Destination SAP address	[35]
eCall	European initiative to aid motorists involved in collision	
ECU	Electronic control unit	
EDCA	Enhanced Distributed Channel Access	[38]
EEBL	Emergency Electronic Brake Light	

Acronym	Meaning	Reference
EN	European Norm	ETSI
ETSI	European Telecommunications Standards Institute	http://www.etsi.org
EU	European Union	general
FCC	Federal Communications Commission	http://www.fcc.gov/
FNTP	Fast Networking & Transport layer Protocol	[16]
From DS	Field in the IEEE Std 802.11 MAC header	[38]
FSAP	Fast Service Advertisement Protocol	[14]
GeoNet	Name of an EU research project	www.geonet-project.eu
GeoNetworking	Name of a protocol developed at ETSI based on the results from GeoNet	[30]
GNSS	Global navigation satellite system	
GPS	Global positioning system	
HTG	Harmonization Task Group	-
I2V	Infrastructure to Vehicle	
IANA	Internet Assigned Numbers Authority	http://www.iana.org
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org
IETF	Internet Engineering Task Force	http://www.ietf.org
iOS	Apple mobile operating system (previously iPhone OS)	
IP	Internet Protocol	IETF
IPv6	Version 6 of the Internet Protocol	IETF
ISO	International Standards Organization	http://www.iso.org
ITS	Intelligent Transport Systems (CEN, ETSI, ISO) Intelligent Transportation Systems (US)	[7]
ITS-AID	ITS Application Identifier	[25]
ITS-S	ITS Station	[7]
LLC	Logical Link Control	[34]

Acronym	Meaning	Reference
MAC	Medium Access Control	[34]
MIB	Management Information Base	[34]
OBU	Onboard Unit	
OSI	Open Systems Interconnection	[20]
PDU	Protocol Data Unit	[34]
PSID	Provider Service Identifier	[41]
RSU	Roadside Unit	
SACH	Service Advertisement Channel	[21]
SAE	Society of Automotive Engineers	http://www.sae.org/
SAM	Service Advertisement Message	[14]
SAP	Service Access Point	[13]
SCH	Service Channel	[21, 41, 24]
SCHx	Service Channel number x	[24]
SDO	Standards Development Organization	general
SDU	Service Data Unit	[34]
SfCH	Safety Channel	[21]
SNAP	Sub-Network Access Protocol	[34]
SNMP	Simple Network Management Protocol	IETF, [34]
SPaT	Signal Phase and Timing (from SAE)	
SSAP	Source SAP address	[35]
SSP	Service specific permissions From 802.11:2012 subscription service provider (SSP): An organization (operator) offering connection to network services, perhaps for a fee. From 1609.2 service specific permissions (SSP): A field that encodes permissions relevant to a particular certificate holder.	[40]

Acronym	Meaning	Reference
Std	Standard	IEEE
TDMC	Time Domain Multiple Channel switching	-
To DS	Bit field in the IEEE Std 802.11 MAC header	[38]
TS	Technical Specification	ETSI / ISO
U-NII	Unlicensed National Information Infrastructure	**[47]**
US	United States	general
V2I	Vehicle to Infrastructure	
V2V	Vehicle to Vehicle	
VCI	Virtual Communication Interface	[9]
VSA	Vendor Specific Action	[38]
WAVE	Wireless Access in Vehicular Environments	[39, 40, 41, 42, 43, 44]
WG	Working Group	general
WM	Windows Mobile	
WSA	WAVE Service Advertisement	[41]
WSMP	WAVE Short Message Protocol	[41]
XID	eXchange IDentification IEEE Std 802.2 LLC service	[35]
4G/LTE	Fourth generation mobile communications – Long-Term Evolution	

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-13-073

U.S. Department of Transportation