EU-US Standards Harmonization Task Group Report: Testing for ITS Communications

Document HTG3-2

EU-US ITS Task Force
Standards Harmonization Working Group
Harmonization Task Group 3

November 12, 2012

Publication # FHWA-JPO-13-081

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-13-081		

4. Title and Subtitle EU-US Standards Harmonization Task Group Report: Testing for ITS Communications (Document HTG3-2)	**5. Report Date** November 12, 2012 **6. Performing Organization Code**
7. Author(s) Wolfgang Hoefs, Eric Koenders, Ola Martin Lykkja, John Moring, Steve Sill, Siebe Turksma	**8. Performing Organization Report No.**
9. Performing Organization Name And Address ITS Joint Program Office, Research and Innovative Technology Administration, U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Washington, DC 20590	**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.**
12. Sponsoring Agency Name and Address	**13. Type of Report and Period Covered** **14. Sponsoring Agency Code**
15. Supplementary Notes	

16. Abstract

Harmonization Task Group 3 (HTG3) was established by the EU-US International Standards Harmonization Working Group to attempt to harmonize standards (including ISO, CEN, ETSI, IEEE) on communications protocols to promote cooperative ITS interoperability. HTG3 worked in close coordination with HTG1 whose focus is on harmonization of security. In collaboration, the two HTGs developed an integrated set of technical reports including this report. This report describes a set of interoperability tests, the results of which are intended to provide confidence that ITS stations communicate cooperatively and are interoperable. It should be read in conjunction with HTG3-1— Status of ITS Communications Standards, which summarizes the analysis conducted to identify the necessary subset of available standards to provide assurance of interoperable communications in Cooperative ITS (C-ITS).

17. Key Words	18. Distribution Statement
intelligent transport systems, interoperability, tests, communications, standards, security, harmonization, safety	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		24	

Table of Contents

1. References

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

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

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

[4] HTG1-3:2012, Feedback to Standards Development Organizations

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

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

[7] HTG3-3:2012, Feedback to Standards Development Organizations

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

[9] ETSI EG 202 237 V1.2.1 (2010-08), Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); Generic approach to interoperability testing

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

See [5] for a complete list of references used by the HTG1&3 teams.

2. Glossary

Acronym	Definition
EUT	Equipment Under Test
PSID	Provider Service Identifier
AID	Application Identifier
ADU	Application Data Unit
TTCN	Testing and Test Control Notation
PICS	Protocol Implementation Conformance Statement
OBU	On Board Unit
RSU	Road Side Unit

See [5] for a complete list of terms and definitions used by the HTG1&3 teams.

3. Introduction

3.1 General

This document considers a set of tests in which ITS stations may be shown to operate in a common environment. It should be read in conjunction with other HTG reports [5]; and [1], section 7, Use Cases/Applications.

The tests described here are modular. They are tests of functional building blocks (termed basic functions – or basic communication functions – in this document). The tests in this document assume that harmonization efforts have led to application-level messages that can be generated and understood by all systems under test, or that such a message set has been selected for the test. Furthermore, they assume that harmonization at the access and network level layer has progressed such that systems can support the various protocols in these layers simultaneously, and that they are transparent to the facilities and application layer implementations.

Each test focuses on a Communication Scenario defined in [1] and is relevant to a number of topics in [5]. The test coverage of topics is described in Table 1.

The test descriptions are sufficiently developed and detailed to verify that devices resulting from protocol implementations are able to work together and provide the functionalities facilitated by the protocols. Detailed protocol checks are to be part of a separate conformance testing process and are thus avoided during interoperability tests.

This description may also be detailed further into a full formal conformance test specification. The descriptions are generic to enable implementation in other domains (e.g., ETSI CTI [10], OmniAir).

Interoperability testing is the activity of proving that end-to-end functionality between (at least) two communicating systems as is required by those systems' base standards. The goal of interoperability tests is to verify that devices claiming to be able to work together and also claiming to provide the functionalities described by the mechanisms and protocols published by the standards bodies contributing to co-operative ITS are truly able to interoperate with each other.

3.2 Testing overview

There are three levels of testing and verification:

- Basic function testing – for the basic communication and security functions.
- Testing communication scenarios – for full communication transactions including security.
- Testing complete application scenarios – using one or more communication scenarios.

3.2.1 Basic function testing

There are seven tests for the basic communication functions (see section 5). Associated with each of these basic communication functions there are one or more security function tests described in [3].

Two levels of rigour are recognised:

- Interoperability verification.
- Formal compliance tests.

The *interoperability verification* uses two communication nodes EUT-A and EUT-B. An elementary stimulus evokes certain behaviour in EUT-A involving communication to EUT-B with a possible response from EUT-B. Only well-formed stimuli are used. Valid data frames are communicated and communication is not interfered with. Details are described for each of the basic function tests. Figure 1 shows a typical test setup for an interoperability test.

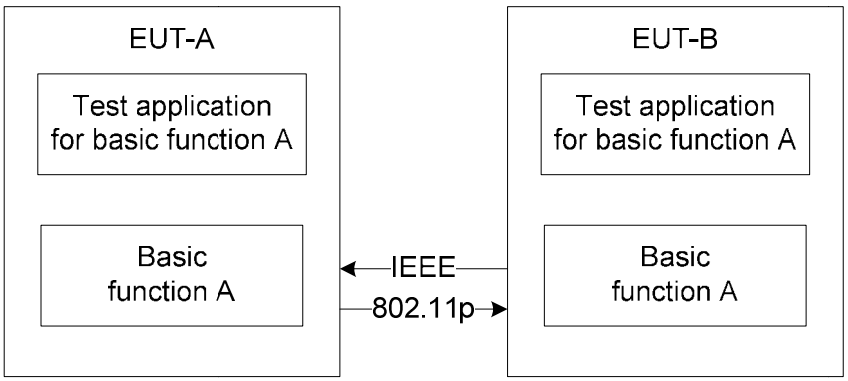

Figure 1: Interoperability test

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

The *formal compliance* test seeks to cover full functionality, boundary data and malformed stimuli and data. The test setup involves a Test System that can provide all possible stimuli and responses to the EUT. A full analysis of stimuli, responses and data must be done and transcribed into a formal compliance test set. Associated with the test set is a test coverage analysis. The compliance test may be performed with TTCN (Testing and Test Control Notation) or other tools after creating PICS (Protocol Implementation Conformance Statement) specifications based on the standards. Figure 2 shows a typical test setup for a formal compliance test. The current set of documents does not specify or describe formal compliance tests.

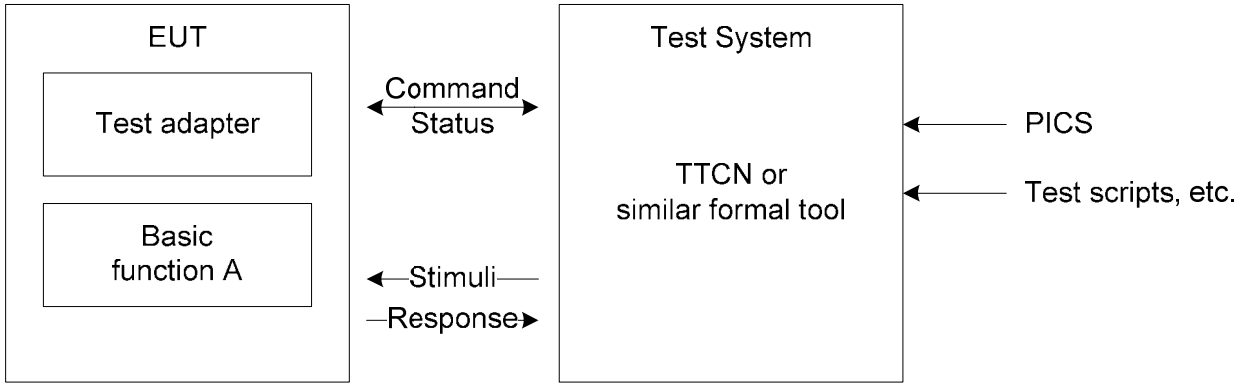

Figure 2: Formal compliance test setup

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

Note: The basic security functions are tested in combination with a basic communication function, see [3].

3.2.2 Communication scenarios

HTG1&3-1, *Overview of Harmonization Task Groups 1 & 3* [1] describes six communication scenarios that are representative of the communication needs within the scope of the HTG.

The following table has, as rows, the communication scenarios from [1], and, as columns, the associated basic communication functions (i.e., test cases described in section 5).

One test may provide coverage of multiple communication scenarios.

Table 1: Communication scenarios covered by test functions

Communication Scenario	CAM/BSM Broadcast	Service advertisement without application session	Application session (non-IP)	Service advertisement with application session	IPv6 Router Advertisement	Application session (IPv6)	Border Crossing—new regulatory domain
1. Vehicle-Originating Broadcast	Yes						Yes
2. Infrastructure-Originating Broadcast	Yes	Yes		Yes	Yes		Yes
3. Infrastructure – Vehicle Unicast			Yes	Yes			
4. Local time-critical session			Yes	Yes			
5. Local non-time-critical session				Yes	Yes	Yes	
6. Multi-RSU session				Yes		Yes	

The communication scenario testing is limited to interoperability verification – analogous to that for the basic communication and security tests.

Test description for the communication scenarios are outside of the scope of this document, but can be simple combinations of the basic function tests.

3.2.3 Complete application scenarios

Many real-life applications need no more than the presented communication scenarios. More complex applications, however, combine different scenarios in the course of a "cooperative transaction," potentially using many basic communication and security functions in a complex chain.

Test descriptions for mature safety application scenarios are outside of the scope of this document. However, one example will be given on the level of a complex application with safety aspects. See section 7.

3.3 Disclosure of test results

Tests are executed to improve the products of all participants. Uncontrolled disclosure of test results might harm the business of the companies involved. Therefore it is advised that all partners (companies) in the test sign an NDA and lodge it with the organizer, the purpose of which is to ensure that each partner may only disclose their own results without revealing any results from any other explicitly or implicitly identified partner. The organizer may publish information about the overall results of the test only provided it is with the consent of all partners and if anonymity with regard to specific results is afforded to all of the partners.

4. Interoperability tests

Note that the interoperability tests described in this document are not rigorous formal compliance tests; they are only intended to verify interoperability.

4.1 Structure of this section

Section 5 has a list of interoperability tests for ITS protocols. The entry for each topic has the following structure:

- The name of the test including a general description.
- A detailed test description.
- An outline of how the test will be carried out. This is currently not a full or formal specification.

Table 2 and Table 3 show how the test cases cover the use cases and the interoperability topics in the status document [5].

4.2 Test Descriptions

The test session will be executed between devices from different suppliers. Each device can play different roles (sender, receiver) during the test sessions. The information about the test configuration and the roles required are indicated in the test descriptions below.

For each test the following test actions are considered during the test execution:

- **S:** a **stimulus action** corresponds to an event that enforces an EUT to proceed with a specific protocol action, for instance sending a message.
- **V:** a **verify action** consists of verifying that the EUT behaves according to the expected behaviour (for instance, the EUT behaviour shows that it receives the expected message).
- **M:** a **configure action** corresponds to an action to modify the EUT configuration.
- **C:** a **check action** ensures correct operation on intermediate reference points.

4.3 Test Tools

During the execution of the tests, the following test tools can be used:

- **Radio network traces**. Every test should be accompanied by a trace of the radio network interface activity (pcap files). The traces can be recorded at the receiving party, or by a separate receive-only device (sniffer), documenting the content of the frames transmitted over the air.
- **Spectrum analyzer**. The channel use—centre frequency and bandwidth—should be checked during the testing process. A spectrum analyzer can be used to confirm this.
- **GPS location simulator**. Some tests (in particular regulatory border crossing) can only be executed with valid positions. Valid positions can be provided by using tools that can play back GPS location data from a recorded or simulated track.
- **Test applications**. The required actions as listed in section 4.2 can be supported with dedicated test applications. The requirements for test applications are described in more detail below.

A test application must be available that can send and receive the relevant messages. Each test application must be configurable to use the relevant address, port number, PSID, data rate, payload, etc. Possibly existing implementations in the facilities and application layers can be used to execute these functions. The following test applications are foreseen to support the tests in section 5:

- **Message broadcast sender**. This application will send out a datagram with known contents to a known port number or PSID. It will send a predefined number of messages at a given rate.
- **Message listener**. This application will listen at a known port number and/or PSID. Each received message is logged with sender address information (if applicable), message size and content.
- **Service announcement sender** (service provider). This application will send out service advertisements (FSAP/WSA) with a predefined ITS-AID/PSID, optional port number, optional data body part and service channel information.

- **Service advertisement listener** (potential service user). This application will listen for service advertisements at a known ITS-AID/PSID, and possibly IPv6 Router Advertisement. Each received advertisement is logged with sender address information (if applicable) and content (the advertised service and its parameters).
- **Service user application**. This application reacts on certain service advertisements and enters a dialog with the service provider application.
- **Service provider application**. This application engages in a dialog with the service user application.

4.4 Test Scope and Prerequisites

This document describes a number of tests. Each test is to be executed by two partners, with one of them initiating the test. All tests are performed twice, where the partners switch roles in the second run. Not all equipment will be designed for symmetric testing and this is optional.

The following protocol stacks are used:

- IEEE 1609 WSMP/WSA.
- ISO FNTP/FSAP.
- IPv6 and TCP/UDP.

For application message exchanges, the non-IP test is applied to both (FNTP/WSMP) stacks. The active partner configures the stack to send first with WSMP and then with FNTP. The receiver should be able to listen to both without reconfiguration. For data exchange tests, partner B shall respond using the same stack that received the request.

Summarizing, each non-IP test may be executed up to four times:

Table 2: Test execution for multiple stacks

Test execution #	Partner A	Partner B
1	Sending WSMP/WSA	Receiving WSMP/WSA
2	Receiving WSMP/WSA	Sending WSMP/WSA
3	Sending FNTP/FSAP	Receiving FNTP/FSAP
4	Receiving FNTP/FSAP	Sending FNTP/FSAP

It might be the case that applications use multiple radio channels, which can change during operation. In this case, it is advised to use separate listen-only radio receivers (sniffers) to record all transmissions of messages on all applicable channels (as described in section 4.3).

4.5 Test coverage

The table shows the HTG3-xx-nn topics covered by each test.

Table 3: Protocol harmonization topics coverage

Interoperability Topic		CAM/BSM Broadcast	Service advertisement without application session	Application session (non-IP)	Service advertisement with application session	IPv6 Router Advertisement	Application session (IPv6)	Border Crossing—new regulatory domain
HTG3-AL-01	Physical channels	x	x	x	x	x	x	x
HTG3-AL-02	Mapping of logical channels onto physical channels	x	x	x	x	x	x	x
HTG3-AL-03	Time domain multi-channel (TDMC) switching							
HTG3-AL-04	Multiple radio technologies							
HTG3-AL-05	Channel congestion control mechanisms							
HTG3-AL-06	To DS/From DS							
HTG3-AL-07	Fragmentation at MAC layer							
HTG3-AL-08	EDCA parameter values							
HTG3-AL-09	Management of optional CIPs							
HTG3-AL-10	802.2 LLC header for type 1 operation	x	x	x	x	x	x	x
HTG3-AL-11	802.2 LLC types of operation	x	x	x	x	x	x	x
HTG3-AL-12	802.2 DSAP and SSAP usage	x	x	x	x	x	x	x
HTG3-AL-13	Ethertype values	x	x	x	x	x	x	x
HTG3-NT-01	Networking protocols	x	x	x	x	x	x	x
HTG3-NT-02	Transport protocols	x	x	x	x	x	x	x
HTG3-NT-03	Identification of endpoints	x	x	x	x	x	x	x
HTG3-NT-04	IPv6 support					x	x	
HTG3-NT-05	Maximum PDU size			x				
HTG3-FL-01	Facility layer functions							
HTG3-FL-02	Facilities Layer API							
HTG3-ME-01	Service advertisement		x		x	x		

Interoperability Topic		CAM/BSM Broadcast	Service advertisement without application session	Application session (non-IP)	Service advertisement with application session	IPv6 Router Advertisement	Application session (IPv6)	Border Crossing—new regulatory domain
HTG3-ME-02	SAM and CTX		x		x	x		
HTG3-ME-03	Delivery mechanism for service advertisement		x		x			
HTG3-ME-04	Identification of region of operation for service advertisements							
HTG3-ME-05	Application identifiers		x		x			
HTG3-ME-06	Router advertisement					x		
HTG3-ME-07	Features of service advertisement							
HTG3-ME-08	TX power indication							
HTG3-ME-09	SAM/WSA repetition rate		x		x		x	
HTG3-ME-10	Location of service provider antenna							
HTG3-ME-11	Station ID		x		x			
HTG3-ME-12	Delivery of generic management data							
HTG3-GE-01	Concept of bounded secured managed domain (BSMD)							
HTG3-GE-02	Concept of logical channels	x	x	x	x	x	x	x
HTG3-GE-03	Registries							
HTG3-GE-04	Timing Advertisement broadcast							
HTG3-GE-05	Management Information Bases (MIBs)							
HTG3-GE-06	Releases							
HTG3-GE-07	Testing	x	x	x	x	x	x	x

5. Interoperability Test Cases

5.1 CAM/BSM Broadcast

This test verifies that CAM/BSM messages can be sent to other systems via all available and relevant protocol stacks. The application protocols (CAM/BSM) are selected as test application. The scope of this test is to test all layers of the communication system, from physical to application layers.

The following steps are taken:

- A fully preconfigured CAM/BSM is created, with all relevant fields set to typical “non-null” values.
- **S**: The CAM/BSM is sent (broadcast) at a rate of 1-5 Hz.
- **V**: The CAM/BSM is received by the other system. The test is complete when a complete and correct CAM/BSM is received.
- **V**: The CAM/BSM is correctly decoded.
- **C**: The CAM/BSM is transmitted as a broadcast with the expected channel and bandwidth RF parameters, check PDU correctness by inspecting the network packet trace.

The test shall be repeated on different channel and channel configurations (i.e., using 10 MHz and 20 MHz bandwidth channels when applicable).

5.2 Service advertisement without application session

This test verifies that WSA messages/SAMs can be sent and received via all available non-IP protocol stacks. It does not include the IEEE 1609 IPv6 WSA Routing Advertisement, which is tested separately in section 5.5.

The following steps are taken:

- A known WSA message/SAM is created with relevant service access parameters.
- **S**: The WSA message/SAM is advertised (broadcast) at a rate of 1-5 Hz.
- **V**: The WSA message/SAM is received by the other system. Test is complete when a complete and correct WSA/SAM is received.
- **V**: The WSA message/SAM is correctly decoded.
- **C**: The WSA message/SAM is transmitted as a broadcast with the expected channel and bandwidth RF parameters, check PDU correctness by inspecting the network packet trace.

5.3 Application session (non-IP)

This test verifies that application unicast messages can be exchanged between two systems via all available protocol stacks.

The following steps are taken:

- Address setup is done (i.e., port numbers/PSID are known) and the networking and transport layer protocols are initialized, if applicable.
- **S**: A known data ADU is sent (unicast) to a destination identified by an address and port number/PSID.
- **V**: The ADU is received by the other system.
- **V**: The ADU is correctly decoded.
- **V**: The receiver replies to the sending ADU with a known response (unicast).
- **V**: The reply is received by the original sender.
- **V**: The reply is correctly received.
- **C**: The messages are transmitted in unicast with the expected channel and bandwidth RF parameters; check PDU correctness by inspecting the network packet trace.

5.4 Service advertisement with application session

This test verifies that WSA messages/SAMs can be sent and received and that a session with the advertised service can be established.

Send a WSA message/SAM with a known PSID/ITS-AID and port number. A service user application interprets this, and enters a session with the service provider application, optionally on a service channel, exchanging a few application messages.

The following steps are taken:

- A known WSA message/SAM is created with a known PSID/ITS-AID and port number and channel parameters.
- **S**: The WSA message/SAM is advertised (broadcast) by the provider station at a rate of 1-5 Hz.
- **V**: The WSA message/SAM is received by the user station.
- **V**: The WSA message/SAM is correctly decoded by the user station.
- **C**: The WSA message/SAM is transmitted as a broadcast with the expected channel and bandwidth RF parameters; check PDU correctness by inspecting the network packet trace. The above steps correspond to section 5.2.
- **S**: CTX is sent by the user station.
- **S**: A known data ADU is sent (unicast) by the user station using the advertised channel and PSID/port number.
- **V**: The ADU is received by the service provider station.
- **V**: The ADU received by the service provider station is correctly decoded.
- **V**: The service provider application replies to the sending ADU with a known response (unicast).
- **V**: The reply is received by the service user station.
- **V**: The reply is correctly received.

- **C**: The messages are transmitted in unicast with the expected channel and bandwidth RF parameters; check PDU correctness by inspecting the network packet trace.

5.5 IPv6 Router Advertisement

This test verifies the IEEE 1609 IPv6 WSA Router Advertisement.

The following steps are taken:

- A known WSA message/SAM is created containing IPv6 prefix information.
- **S**: The WSA message/SAM is advertised (broadcast) by the service provider station.
- **V**: The WSA message/SAM is received by the potential service user station.
- **V**: The WSA message/SAM is correctly decoded.
- **V**: IPv6 networking and routing is established according to the announced prefix.
- **C**: The WSA message/SAM is transmitted as a broadcast with the expected channel and bandwidth RF parameters, check PDU correctness by inspecting the network packet trace.

5.6 Application session (IPv6)

This test verifies the use of TCP/IPv6 for application to application communication.

The following steps are taken:

- An IPv6 network is manually set up before the test is started.
- **S**: A TCP/IPv6 session is established with a known server address and port number.
- **V**: Data is transferred over the TCP session (for example, a file transfer or HTTP session).
- **C**: The TCP/IPv6 messages are transmitted in unicast; check PDU correctness by inspecting the network packet trace.

5.7 Border Crossing—new regulatory domain

This test is used to verify that the communication parameters (channel, bandwidth) are changed correctly when crossing a border.

Achieving interoperability for mobile ITS stations (personal or vehicular) travelling between different operational regions (e.g., crossing the border between two neighbour 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 in case 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.

The following steps are taken:

- **S**: During the test, the mobile station sends out CAM messages.
- **C**: All CAM messages are transmitted as a broadcast with the expected channel and bandwidth RF parameters; check PDU correctness by inspecting the network packet trace.
- **S**: The roadside station advertises a border location in a WSA message/SAM (broadcast).
- **C**: All WSA message/SAM messages are transmitted as a broadcast with the expected channel and bandwidth RF parameters; check PDU correctness by inspecting the network packet trace.
- **V**: The mobile station receives the border location.
- **V**: The border location is decoded correctly.
- **V**: When the mobile station passes the border (based on the geographical location of the vehicle), the radio channels are modified as needed.
- **C**: All CAM messages are transmitted as a broadcast with the expected (modified) channel and bandwidth parameters.
- **V**: The CAM messages of the mobile station are sent using the correct default protocol stack.
- **V**: In case an unknown country code is received, the transmitter should stop transmitting and continue listening.

6. List of Parameters

The following table contains a list of communication parameters as they are currently described in the existing or proposed standards.

Table 4: Communication parameters

ID	Topic	EU config	US config
HTG3-AL-01	Physical channels	Any 10MHz, 5.9GHz channel	Any 10MHz, 5.9GHz channel
HTG3-AL-02	Mapping of logical channels onto physical channels	CCH and/or SCH	CCH and/or SCH
HTG3-AL-03	Time domain multi-channel (TDMC) switching	N/A	Continuous
HTG3-AL-04	Multiple radio technologies	5.9GHz	5.9GHz
HTG3-AL-05	Channel congestion control mechanisms	None	none
HTG3-AL-06	ToDS/FromDS	Set to 0	Set to 0
HTG3-AL-07	Fragmentation at MAC layer	Default (not allowed)	Default (allowed)
HTG3-AL-08	EDCA parameter values	Default (per 802.11)	Default (per 802.11)
HTG3-AL-09	Management of optional CIPs	No CIPs (equivalent to standard LLC header)	Default (standard LLC header)
HTG3-AL-10	802.2 LLC header for type 1 operation	Type 1	Default (Type 1)
HTG3-AL-11	802.2 LLC types of operation	Type 1	Default (Type 1)
HTG3-AL-12	802.2 DSAP and SSAP usage	SNAP	Default (SNAP)
HTG3-AL-13	Ethertype values	IPv6, FNTP(TBD)	FNTP, WSMP
HTG3-NT-01	Networking protocols	IPv6 or FNTP	IPv6 or WSMP
HTG3-NT-02	Transport protocols	None	None
HTG3-NT-03	Identification of endpoints	Port	PSID
HTG3-NT-04	IPv6 support	Default	Default
HTG3-NT-05	Maximum PDU size	Default (unlimited?)	Default (1500b)
HTG3-FL-01	Facility layer functions		
HTG3-FL-02	Facilities Layer API		
HTG3-ME-01	Service advertisement	SAM	WSA
HTG3-ME-02	SAM and CTX	No CTX	Default (no ack)
HTG3-ME-03	Delivery mechanism for service advertisement	Data	Vendor specification
HTG3-ME-04	Identification of region of operation for service advertisements	Not used	
HTG3-ME-05	Application identifiers	ITS-AID	PSID
HTG3-ME-06	Router advertisement	Per draft (?)	Default
HTG3-ME-07	features of service advertisement	Default (no security)	No security
HTG3-ME-08	TX power indication	Default (not present)	Default (not present)
HTG3-ME-09	SAM/WSA repetition rate	Default (not present)	Default (not present)
HTG3-ME-10	Location of service provider antenna	Default (not present)	Default (not present)
HTG3-ME-11	Station ID	Default (not present)	Default (not present)
HTG3-ME-12	Delivery of generic management data	Not used	Not used
HTG3-GE-01	Concept of bounded secured managed domain (BSMD)		
HTG3-GE-02	Concept of logical channels		
HTG3-GE-03	Registries		

ID	Topic	EU config	US config
HTG3-GE-04	Timing Advertisement broadcast	Not used	Not used
HTG3-GE-05	Management Information Bases (MIBs)	Not used	Not used
HTG3-GE-06	Releases	Not used	Not used
HTG3-GE-07	Testing		

7. Example scenario for a complete application

Once the test cases described in chapter 5 have been executed successfully, they can be used as building blocks to build real-life scenarios. Using this approach, an on-street demonstration of interoperability can be created.

This chapter describes an on-street scenario that demonstrates interoperability between systems of differing origins. The scenario has been chosen such that it demonstrates a primary secure interaction between two ITS stations that involves an exchange of broadcast and unicast messages, together with rear collision warning involving multiple vehicles.

7.1 The emergency vehicle at an intersection scenario

In this scenario a controlled intersection provides green light priority to emergency vehicles. Priority is only provided for vehicles that are on a time-critical mission. Priority with full clearance of the intersection might not be possible, in which case the emergency vehicle will ignore the red light and other vehicles have to be warned, either directly by the intersection controller or indirectly by other vehicles.

While approaching the intersection the emergency vehicle driver is informed on the priority provided (or not). Additionally, the remaining time to green is presented to the driver, which allows him/her to anticipate the upcoming green light. Additional information on hazardous situations on the crossing can be given.

When the intersection controller reaches the conclusion that the emergency vehicle cannot be accommodated within normal intersection safety parameters (either negating a red light or using exceptionally short clearance times), a warning is broadcasted to other vehicles. The other vehicles in their turn can warn surrounding vehicles.

For demonstration purposes, it is assumed that the emergency vehicle in the demonstration has been imported, and therefore carries a mobile ITS station that has been produced for a region that has a different communication profile. Moreover one or more of the other vehicles can be of non-local origin.

7.2 Detailed description of the interaction

The emergency vehicle is equipped with a mobile ITS station: an On-Board Unit (OBU). The intersection controller is equipped with a stationary ITS station: the Roadside Unit (RSU). Other vehicles might be equipped with OBU's of various origins.

The RSU sends out service advertisements for the emergency priority service and CAM messages containing its location and other parameters.

The OBU receives CAM messages and keeps track of nearby RSUs. Based on the heading of the vehicle, the closest upcoming RSU is selected. The OBU receives the service announcements from the RSU.

If the upcoming RSU announces the priority service application, an emergency priority request is sent from the emergency vehicle identifying itself as an emergency vehicle.

The RSU receives CAM messages and stores their location in the Local Dynamic Map (LDM). For vehicle CAMs, the speed and heading are also stored. These are used to extrapolate the current vehicle position.

Vehicle locations are map-matched with plausible trajectories in the LDM. When a priority request is received, its contents are matched with the requirements given above. The priority request must be authenticated to ensure that only authentic emergency vehicles on a time-critical mission are considered. Then the vehicle location is retrieved from the LDM, and the distance to the stop line is calculated.

Based on this, the strategy is adjusted to:

a. Clear the intersection of other vehicles (practically putting all signals except the ones on the emergency vehicles trajectory to red).
b. If possible within the safety parameters, put the signals on the emergency vehicle trajectory to green in time for the emergency vehicle to arrive.

If the adjustment described above is not possible in time, the RSU broadcasts red-light-violation warning messages to warn other vehicles of the emergency vehicles. Depending on the braking behavior of vehicles, a V2V rear-end collision scenario can be invoked between other vehicles.

After the emergency vehicle has cleared the intersection, the intersection controller will adjust the control for a speedy resumption of normal operation and will withdraw warnings.

7.3 Test cases used

The emergency vehicle priority scenario uses the following test cases from chapter 5:

5.1 CAM/BSM

5.2 Service advertisement without application session

5.3 Application session (non-IP)

5.4 Service advertisement with application session

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-13-081

U.S. Department of Transportation