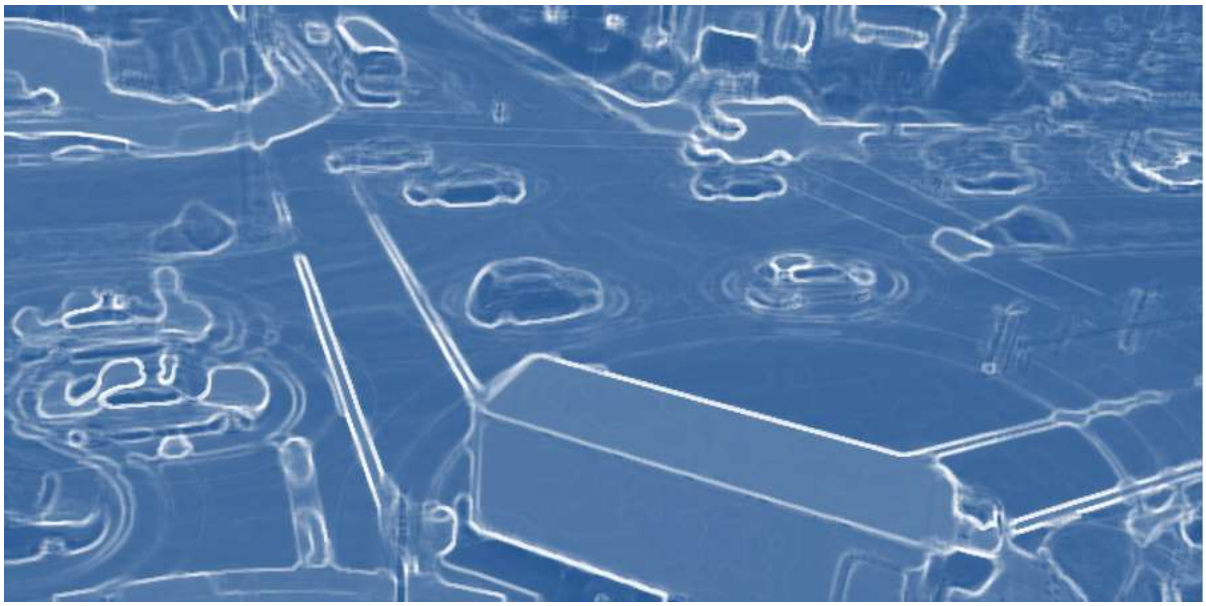

Plug Fest Interoperability Test Cases

Version:	1.1
Revision Date:	11/9/2016

Table of Contents

1 Scope

This document provides the test cases expected to be conducted as a part of the Plugfest interoperability that will be held at Danlaw's facilities in Novi, Michigan in November of 2016. Some test cases may not be applicable if certificates are not available by the time of the Plugfest.

1.1 References

The following referenced documents are necessary for the application of the present document.

[1] SAE J2945/1 D5.0: "On-board System Requirements for V2V Safety Communications". Latest issue.

[2] SAE J2735, January 2016 issue. DSRC Message Set Dictionary.

[3] IEEE Std. 802.11™-2012: "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". Latest issue.

[4] IEEE Std. 1609.2-2016: "IEEE Draft Standard for Wireless Access in Vehicular Environments - security Services for Applications and Management Messages".

[5] IEEE Std 1609.3-2016 "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Network Services"

[6] P1609.4™/D5 Draft Standard for Wireless Access in Vehicular Environments – Multi-Channel Operation. Latest issue.

[7] Test System Interface. Latest issue available on GitHub at: https://github.com/certificationoperatingcouncil

2 Abbreviations

SAE Society of Automotive Engineers
IEEE Institute of Electrical and Electronics Engineers
MAC Media Access Control
PHY Physical Layer
WAVE Wireless Access in Vehicular Environments
V2V Vehicle-to-Vehicle
DSRC Dedicated Short Range Communications
LAN Local Area Network
IUT Implementation Under Test
COC Certification Operating Council
RSU Road Side Unit
TCI Test Control Interface
IOP Interoperability
CFG Configuration
STD Standard
WSM WAVE Short Message
TPID Transport Protocol Identifier
PSID Provider Service Identifier
BSM Basic Safety Message
ID Identifier
WSA Wave Service Advertisement
TX Transmit
UDP User Datagram Protocol
IP Internet Protocol
IPv6 Internet Protocol Version 6
I/F Interface

3 Prerequisites and Test Configurations

3.1 Test Configurations

IOP CFG 1: Two IUTs are placed a short distance away from each other to allow for easy communication. One IUT may be replaced by a system provided by the COC specifically when an RSU functionality is required.

IOP CFG 2: One IUT is connected to a test apparatus cable of automatically testing the IUT through the TCI and returning a pass/fail verdict

4 WSM Packet Validation

Identifier:	IOP TC 1		
Summary:	Transmit WSM with version number and ethertype		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM
	2	Stimulus	Device A transmits WSM
	3	Verify	Reception of WSM by Device B
	4	Verify	Received WSM contains version number and ethertype
	5	Verify	Repeat Step 1-4 for Device B

4.1 Transmit WSM with N Header / T Header

- Optional (check contents)

Identifier:	IOP TC 2		
Summary:	Transmit WSM with N Header		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM
	2	Stimulus	Device A transmits WSM
	3	Verify	Reception of WSM by Device B
	4	Verify	Received WSM contains Subtype, Wave Info Element, and Count
	5	Verify	Repeat Step 1-4 for Device B

Identifier:	IOP TC 3		
Summary:	Transmit WSM with T Header		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM
	2	Stimulus	Device A transmits WSM
	3	Verify	Reception of WSM by Device B
	4	Verify	Received WSM contains TPID, PSID, WSM Length, and WSM Data
	5	Verify	Repeat Step 1-4 for Device B

4.2 WSM Transmission Parameters

- Tested in WSM Packet Validation

4.3 Reception of WSM

- Tested in WSM Packet Validation

4.4 WSM communications with continuous channel

Identifier:	IOP TC 4		
Summary:	Transmit WSMs in continuous operation on selected channel		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs. Channel and WSM Repeat Rate to be defined between two parties.		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM
	2	Stimulus	Device A transmits WSM at defined channel and repeat rate
	3	Verify	Reception of WSM by Device B
	4	Verify	Device B receives continuous streams of WSMs and verifies channel used.
	5	Verify	Repeat Step 1-4 for Device B

4.5 WSM communication with alternation channel access

Identifier:	IOP TC 5		
Summary:	Transmit WSMs in alternating operation on selected channels		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs. Channels and WSM Repeat Rate to be defined between two parties.		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit 2 WSMs, each WSM is transmitted on a different channel.
	2	Stimulus	Device A transmits WSM at defined channels and repeat rate
	3	Verify	Reception of WSMs by Device B
	4	Verify	Device B detects WSMs on defined channels and time slots
	5	Verify	Repeat Step 1-4 for Device B

4.6 Transmission of WSMs with payload exceeding WsmMaxLength

Identifier:	IOP TC 6
Summary:	Transmit WSM with payload exceeding WsmMaxLength

Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs. Channels and WSM Repeat Rate to be defined between two parties.		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM with payload exceeding WsmMaxLength
	2	Stimulus	Device A transmits WSM at defined channels and repeat rate
	3	Verify	Device B does not detect/receive WSM from Device A
	4	Verify	Repeat Step 1-3 for Device B

5 BSM

5.1 Transmissions of packets

Identifier:	IOP TC 7		
Summary:	Generate valid BSM security header		
Configuration:	IOP CFG 1		
References:	[4]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive BSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit BSM
	2	Stimulus	Device A transmits BSM
	3	Verify	Reception of BSM by Device B
	4	Verify	Received BSM contains protocol version and content in Ieee1609Dot2Data. Contains hashId in signedData. Contains protocol version, content in tbsData. Contains psid, generationTime and does not include expiryTime, generationLocation in headerInfo
	5	Procedure	Repeat Step 1-4 for Device B

Identifier:	IOP TC 8		
Summary:	Test transmission and reception of “generic” BSMs		
Configuration:	IOP CFG 1		
References:	[2]		
Pre-test conditions:	2 independent devices (Device A and Device B) are able to be configured to transmit and receive BSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit BSM
	2	Stimulus	Device A transmits BSM
	3	Verify	Reception of BSM by Device B
	4	Verify	Received BSM is successfully received and parsed
	5	Procedure	Repeat Step 1-4 for Device B

Identifier:	IOP TC 9		
Summary:	Test transmission of BSMs with vehicle event flags		
Configuration:	IOP CFG 2		
References:	[3]		
Pre-test conditions:	An independent device (Device A) can connect to the test interface		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is placed in the test system
	2	Stimulus	The test system begins the vehicle event flag test
	3	Verify	Device A passes the test

Identifier:	IOP TC 10		
Summary:	Test message number rollover and Temporary ID of BSMs		
Configuration:	IOP CFG 2		
References:	[4]		
Pre-test conditions:	An independent device (Device A) can connect to the test interface		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is placed in the test system
	2	Stimulus	The test system begins the vehicle event flag test
	3	Verify	Device A passes the test

Identifier:	IOP TC 11		
Summary:	Test data randomization of BSMs		
Configuration:	IOP CFG 2		
References:	[5]		
Pre-test conditions:	An independent device (Device A) can connect to the test interface		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is placed in the test system
	2	Stimulus	The test system begins the data randomization test
	3	Verify	Device A passes the test

5.2 Reception of packets

Tested in Transmission of packets

5.3 Reception of packets – invalid behavior tests

Identifier:	IOP TC 12
Summary:	Detection of invalid BSM
Configuration:	IOP CFG 1
References:	[4]
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSAs

Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit BSM
	2	Stimulus	Device A transmits BSM
	3	Verify	Reception of BSM by Device B
	4	Verify	BSM signature contains ecdsaP256Signature indicating r and s not verifiable using (KEY)
	5	Verify	Device B identifies BSM holds invalid security credential
	6	Procedure	Repeat Step 1-5 for Device B

Identifier:	IOP TC 13		
Summary:	Test whether IUT continues sending valid BSMs after receiving invalid data frames/elements		
Configuration:	IOP CFG 2		
References:	[6]		
Pre-test conditions:	An independent device (Device A) can connect to the test interface		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is placed in the test system
	2	Stimulus	The test system sends a series of improper BSMs through the TCI
	3	Verify	Device A continues sending valid BSMs throughout the test

6 WSA

6.1 Transmission of packets

Identifier:	IOP TC 14		
Summary:	Transmit 1609.2 WSA security header		
Configuration:	IOP CFG 1		
References:	[4]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSAs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSA
	2	Stimulus	Device A transmits WSA
	3	Verify	Reception of WSA by Device B
	4	Verify	Received WSM contains protocolVersion and content in Ieee1609Dot2Data. Contains protocolVersion and content in tbsData. Contains psid, generationTime, expirtyTime and generationLocation in headerInfo
	5	Procedure	Repeat Step 1-4 for Device B

6.2 Reception of packets

Tested in Transmission of packets

6.3 Reception of packets -invalid behavior tests

Identifier:	IOP TC 15		
Summary:	Detection of invalid WSA		
Configuration:	IOP CFG 1		
References:	[4]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSAs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSA
	2	Stimulus	Device A transmits WSA
	3	Verify	Reception of WSA by Device B
	4	Verify	WSA signature contains ecdsaP256Signature indicating r and s not verifiable using (KEY)
	5	Verify	Device B identifies WSA holds invalid security credential
	6	Procedure	Repeat Step 1-4 for Device B

6.4 WSA packet validation

- Transmit WSM with valid header for WSA message
  - Optional (contents of N-Header can also be verified)

Identifier:	IOP TC 16		
Summary:	Transmit WSM with valid WSM header for WSA message		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs.		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSM
	2	Stimulus	Device A transmits WSM with N-Header containing Subtype, TPID, PSID and WSM Length
	3	Verify	Reception of WSM by Device B
	4	Verify	Device B confirms the presence of content of N-Header
	5	Verify	Repeat Step 1-4 for Device B

- Transmit WSA with version and valid WSA Header
  - Optional (Contents of WSA Header can also be verified)

Identifier:	IOP TC 17		
Summary:	Transmit WSM with version number and valid WSA header		
Configuration:	IOP CFG 1		
References:	[5]		
Pre-test conditions:	2 independent devices (Device A and Device B) configured to transmit and receive WSMs		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to transmit WSA with version, option indicator, identifier and content count

	2	Stimulus	Device A transmits WSA
	3	Verify	Reception of WSA by Device B
	4	Verify	Device B confirms the presence of WSA header information
	5	Verify	Repeat Step 1-4 for Device B

6.5 WSA reception

- Tested in WSA Packet Validation
-

6.6 WSA transmission parameters

- Tested in WSA Packet Validation
-

6.7 WSA changes

Identifier:	IOP TC 18		
Summary:	Change WSA Contents		
Configuration:	IOP CFG 2		
References:	[5]		
Pre-test conditions:	2 devices, Device A running the TCI Message Generator software and Device B (Device under test))		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to send Start WSA TX Periodic message.
	2	Stimulus	Device A sends a UDP message with the selected WSA parameters.
	3	Verify	Reception of message by Device B
	4	Verify	Device B transmits WSA over the air with the proper parameters as contained in the UDP message.
	5	Stimulus	Device A sends a modified Start WSA TX Periodic message.
	6	Verify	Reception of modified message by Device B
	7	Verify	Device B transmits the modified WSA over the air with the proper parameters as contained in the UDP message.

-

7 IPv6

7.1 IP Configuration

Identifier:	IOP TC 19
Summary:	Change IP address
Configuration:	IOP CFG 2
References:	[5]
Pre-test conditions:	2 devices, Device A running the TCI Message Generator software and Device B (Device under test))

Test Sequence:	Step	Type	Description
	1	Configure	Device A is configured to send Set IPv6 Address message.
	2	Stimulus	Device A sends a UDP message with Set IPv6 Address message.
	3	Verify	Reception of message by Device B
	4	Verify	Device B transmits a UDP message indicating an IPv6 configuration changed message to device A.
	5	Stimulus	Device A sends a Get IPv6 I/F Info message.
	6	Verify	Device B transmits a UDP message with the new IPv6 address.
	7	Verify	That the IPv6 address returned in step 6 is the same IPv6 address requested in

7.2 Communication using IPv6

Identifier:	IOP TC 20		
Summary:	IPv6 communications		
Configuration:	IOP CFG 2		
References:	[5]		
Pre-test conditions:	2 devices, Device A running the TCI Message Generator software and Device B (Device under test))		
Test Sequence:	**Step**	**Type**	**Description**
	1	Configure	Device A is configured to send Start IPv6 Ping message.
	2	Stimulus	Device A sends a UDP message with Start IPv6 Ping message with no repeat rate.
	3	Verify	Reception of message by Device B
	4	Verify	Device B pings the IPv6 address specified in the message once.

◙ End of Document ◙