

Engineering Release Notice (ERN)	Change Location	Change Description A = Added W = Was U = Deleted	Document Release Status Version 3.1	
			Release Date 22MAR2014	Change. Count 7

SYSTEM REQUIREMENT DESCRIPTION

“5.9GHz DSRC Aftermarket Safety” Device Specification

Approved by (dept, name, phone)	Issued by (dept, name, phone) US DOT, Walton Fehr, (202) 366-0278 walton.fehr@dot.gov
---------------------------------	---

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC Aftermarket Safety” Device Specification			
	Document Type: System Requirement Description			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 1

Table of Contents

1	INTRODUCTION.....	4
1.1	WHAT IS THE PURPOSE OF THIS DOCUMENT?	4
1.2	WHO SHOULD READ THIS DOCUMENT?	4
1.3	HOW IS THIS DOCUMENT ORGANIZED?.....	4
1.4	HOW DO YOU RECEIVE MORE INFORMATION?	4
1.5	REVISION HISTORY.....	4
1.6	REQUISITE DOCUMENTS	5
2	TERMINOLOGY.....	6
2.1	DEFINITIONS	6
2.2	CONCEPTS	7
2.2.1	<i>Identification of Requirements</i>	7
2.3	ABBREVIATIONS	8
3	SYSTEM DESCRIPTION.....	11
3.1	FUNCTIONAL DESCRIPTION.....	11
3.2	SYSTEM DESIGN	11
3.3	SYSTEM LAYOUT	12
4	SYSTEM REQUIREMENTS.....	13
4.1	MECHANICAL REQUIREMENTS.....	13
4.1.1	<i>Device Installation</i>	13
4.1.2	<i>Device Size</i>	14
4.2	PERFORMANCE REQUIREMENTS.....	14
4.3	ENVIRONMENTAL REQUIREMENTS	15
4.3.1	<i>Operating Voltage</i>	15
4.3.2	<i>Operating Current</i>	15
4.3.3	<i>Temperature and Humidity</i>	16
4.3.4	<i>Shock and Vibration</i>	16
4.3.5	<i>Electrostatic Discharge</i>	16
4.3.6	<i>Conducted Electrical Transients</i>	16
5	FUNCTIONAL REQUIREMENTS	17
5.1	INTERFACE REQUIREMENTS.....	17
5.2	OPERATIONS, MANAGEMENT AND CONTROL.....	18
5.2.1	<i>Operational States</i>	19
5.2.2	<i>Operational Configuration</i>	19
5.2.3	<i>Communications Message Log</i>	19
5.2.4	<i>Device Positioning and Timing</i>	26
5.2.5	<i>Device Security</i>	27
5.2.6	<i>System Status Log</i>	28
5.3	DSRC RADIO SUBSYSTEM	34
5.3.1	<i>FCC Compliance</i>	34
5.3.2	<i>DSRC Radio Count</i>	34

5.3.3	<i>IEEE 802.11</i>	35
5.3.4	<i>IEEE 802.11p</i>	35
5.3.5	<i>IEEE 1609.2</i>	35
5.3.6	<i>IEEE 1609.3</i>	40
5.3.7	<i>IEEE 1609.4</i>	42
5.3.8	<i>Radio Performance</i>	44
5.3.9	<i>Congestion Control</i>	44
5.4	OTHER COMMUNICATIONS	44
5.5	WSMP MESSAGE PROCESSING	44
5.5.1	<i>SAE J2735 Message Types</i>	44
5.5.2	<i>SAE J2735 Basic Safety Message Type – Details</i>	46
5.5.3	<i>SAE J2735 Traveler Information – Details</i>	46
6	TEST REQUIREMENTS	46
6.1	RADIO TRANSMISSION	46
6.2	VEHICLE LOCATION.....	46
APPENDIX A: VEHICLE POWER CONNECTOR		47
APPENDIX B: CONFIGURATION FILE FORMAT		48
APPENDIX C: SECURITY PROFILE		49
APPENDIX D: FIREWALL RULES		50

1 INTRODUCTION

1.1 What is the purpose of this document?

This document will set the requirements for an aftermarket automotive grade mobile device that will be installed in light vehicles, which will be used in the vehicle communication safety pilot.

1.2 Who should read this document?

Suppliers interested in building devices based on the requirements provided in this document.

1.3 How is this document organized?

The Structure of this document is as follows:

- Section 1 – Introduction: Document’s scope, revision history and requisite specifications.
- Section 2 – Terminology: describes the definitions, concepts, and abbreviations used throughout the document.
- Section 3 – System Description: Describes the system layout and the allocation of responsibilities and communication for the system components.
- Section 4 – System Requirements: Describes the System level requirements.
- Section 5 – Functional Requirements: Describes the functional requirements.
- Section 6 – Test Requirements: Describes the testing requirements of the device.

1.4 How do you receive more information?

Additional information is available in the documents listed in section 1.6. Questions are answered by the person responsible for this document (see section 1.5).

1.5 Revision History

Rev.	Vers.	Date	Description	Approved by	Responsible
001	001	12/16/10	First Issue	Walt Fehr	M. Marshall
002	001.1	01/12/11	Walkthrough Updates	Walt Fehr	M. Marshall J. Marousek
003	001.2	2/11/11	Modification to requirement ReqMPS005v001 to address upcoming modifications to SPaT Message		Kevin Gay
004	002.0	08/03/11	1. Revised to incorporate comments received from Device Vendors 2. Revised to align with the recently released Version 2.3 of the aftermarket safety Device Specification	Walt Fehr	J. Marousek
005	002.1	08/04/11	Reference to solicitation Appendix B System Level Tests added	Walt Fehr	Walt Fehr

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 4

Rev.	Vers.	Date	Description	Approved by	Responsible
006	003.0	12/26/11	<ol style="list-style-type: none"> 1. Removed any “ASD” requirement for which there is an “OBE” equivalent requirement and inserted references to the latest version (v3.5) of the Vehicle Awareness Device (VAD) Specification in each affected section of the document. The VAD Specification currently contains all shared onboard equipment (ASD, RSD and VAD) requirements. 2. Restructure document organization to match VAD Specification, enabling easier cross-referencing to OBE requirements. 3. Renumbered all requirements based on removal of duplicate (OBE) requirements. 4. Updated references to CAMP Security Design Document and Draft 9.3 of IEEE 1609.2. 5. Added Appendix C – Security Profile 6. Added Appendix D – Firewall Rules 	Walt Fehr	J. Marousek
007	003.1	03/22/14	<ol style="list-style-type: none"> 1. Removed references to “CAMP VSC3 – Model Deployment Safety Device DSRC BSM Communication Minimum Performance Requirements” 2. Removed references to “CAMP VSC3 – Congestion Control Document” 3. Reference to USDOT 5.9GHz DSRC Vehicle Awareness Device Specification updated to version 3.8 	Walton Fehr	Walton Fehr

1.6 Requisite Documents

This section contains reference documents, and their appropriate versions, required to meet the requirements described in this document. The Standard\Documents listed in the “Reference” portion of the requirements relate to the Standards\Documents listed here:

- USDOT Security Credential Management System Design, January 24, 2012.
- Federal Communications Commission (FCC) 47 Code of Federal Regulations (CFR) Parts 0, 1, 2, & 95 Amendments for Dedicated Short Range Communications Services and Mobile Service for Dedicated Short Range Communications of Intelligent Transportation Service in the 5.850-5.925 GHz Band (5.9 GHz Band).
- IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09
- IEEE 1609.3-2010, August 2010
- IEEE 1609.4-2010, August 2010
- IEEE P1609.12, Draft 20
- IEEE 802.11-2007
- IEEE 802.11p- 2010

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 5

- SAE J551: Vehicle Electromagnetic Immunity – Electrostatic Discharge
- SAE J1113-11 2007-06: Immunity to Conducted Transients on Power Leads
- SAE J1211: Handbook for Robustness Validation of Automotive Electrical/Electronic Modules
- SAE J2735 2009-11: Dedicated Short Range Communication (DSRC) Message Set Dictionary
- USCAR18-2 FAKRA SMB RF Connector Supplement
- USDOT “5.9GHz DSRC Roadside Equipment” Device Specification, version 2.3
- USDOT 5.9GHz DSRC Vehicle Awareness Device Specification, version 3.8
- USDOT DTFH61-11-RA-00003 Solicitation Appendix B. System Level Test Procedures

2 TERMINOLOGY

2.1 Definitions

Definition	Description
Alternating mode	The device switches between the Control Channel and the Service Channel
Authorized Entity	An approved entity (person or software application) with security credentials that authorize attempted operations or activities.
Automotive Grade	End-application solutions, devices, and development tools supporting the automotive industry
Certificate	An electronic document which uses a digital signature, typically from a Certificate Authority to bind a public key with an identity of the person or organization holding the certificate.
Continuous mode	The device does not switch radio channels. It only uses 1 channel
Digital Signature	A digital signature (created using a mathematical algorithm) gives a recipient of an electronic message assurance that the message was created by the sender, and that it is unaltered.
Latency	The latency of a J2735 BSM data element/frame is defined as the maximum age of the data in the outgoing BSM
Meaningful Value	A Valid Value for a data element within a Basic Safety Message which is not “Unavailable” value.
Multiple Channel	TBD
Non-DSRC	Communications protocol outside of the 5.9GHz DSRC band
Public Key	Part of a mathematically related public/private key pair, and used to digitally sign and / or encrypt electronic messages or documents.
Service and Maintenance	TBD
Sign	Digitally signing a electronic message or document using
Valid Value	A value for a data element within a Basic Safety Message that has the correct data type and is within the limits of the value as defined in SAE J2735. A value of “Unavailable” is defined as valid.
WAVE Short Message Protocol	Networking protocol specifically designed for V2X communications.
Wi-Fi	Generic term for communications technologies including wireless local area network (WLAN) which are based on the IEEE 802.11 standards.

2.2 Concepts

2.2.1 Identification of Requirements

The following table explains how the requirements nomenclature is constructed and numbered:

[Document type]-[system]-[issue number]-Req[requirement section][requirement number]v[requirement version number]

Field	Content Description																						
document type	This is a constant text string set to “SRD”, which is an acronym for “System Requirements Description”																						
system	This is a constant text string set to “USDOTASD”.																						
issue number	This is set to the current issue number of this Systems Requirements Description.																						
requirement section	This is set to the functional category of the requirement and will be one of the following: <table border="1" data-bbox="706 877 1458 1297"> <tbody> <tr> <td>BSM</td> <td>Basic Safety Messaging</td> </tr> <tr> <td>CML</td> <td>Communications Message Log</td> </tr> <tr> <td>COM</td> <td>Communications</td> </tr> <tr> <td>DRS</td> <td>DSRC Radio Subsystem</td> </tr> <tr> <td>INT</td> <td>Interface Requirements</td> </tr> <tr> <td>OMC</td> <td>Operations, Management & Control</td> </tr> <tr> <td>POS</td> <td>Positioning</td> </tr> <tr> <td>SEC</td> <td>Security</td> </tr> <tr> <td>SSL</td> <td>System Status Log</td> </tr> <tr> <td>SYS</td> <td>System</td> </tr> <tr> <td>TST</td> <td>Testing</td> </tr> </tbody> </table>	BSM	Basic Safety Messaging	CML	Communications Message Log	COM	Communications	DRS	DSRC Radio Subsystem	INT	Interface Requirements	OMC	Operations, Management & Control	POS	Positioning	SEC	Security	SSL	System Status Log	SYS	System	TST	Testing
BSM	Basic Safety Messaging																						
CML	Communications Message Log																						
COM	Communications																						
DRS	DSRC Radio Subsystem																						
INT	Interface Requirements																						
OMC	Operations, Management & Control																						
POS	Positioning																						
SEC	Security																						
SSL	System Status Log																						
SYS	System																						
TST	Testing																						
requirement number	This is a numeric identifier for each requirement ranging from 001 up to 999 and each filed value will be unique within a defined <i>requirement section</i> (see above).																						
requirement version number	This is set to the current version number of the individual requirement.																						

The following examples illustrate the requirement nomenclature used within this SRD:

SRD-USDOTASD-003-ReqSYS004v001

This requirement was introduced in the first issue of the SRD for system USDOTASD. It is the fourth requirement in the System Requirements section within the document and it is the first version of the requirement.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 7

SRD-USDOTASD-003-ReqDRS001v002

This requirement was updated in the third issue of the SRD for system USDOTASD. It is the first requirement in the *DSRC Radio Subsystem* Requirements section within the document and it has been updated to a second version.

SRD-USDOTASD-003-ReqTST009v001

This requirement was introduced in the third version of the SRD for system USDOTASD. It is the ninth requirement in the *Test Requirement* section within the document and it is the first version of the requirement.

2.3 Abbreviations

Abbr.	Description	Definition
AC	Access Category	See IEEE 802.11-2007
ACL	Access Communications Link	
AIFS	Arbitration Interframe Space	See IEEE 802.11-2007
ASN.1	Abstract Syntax Notation One	Standard and flexible notation that describes structures for representing, encoding and decoding data.
BSM	Basic Safety Message	
C	Celsius	Unit of temperature
CA	Certificate Authority	
CAMP	Crash Avoidance Metrics Partnership	
CCH	Control Channel	
CFR	Code of Federal Regulations	
CONUS	Continental United States	
COTS	Commercial Off the Shelf	
CRL	Certificate Revocation List	
CWmin	Contention Window Minimum	See IEEE 802.11-2007
dB	Decibel	
DC	Direct Current	
DSRC	Dedicated Short Range Communications	
EDCA	Enhanced Distributed Channel Access	
EEBL	Electronic Emergency Brake Light	
EMI	Electromagnetic Interference	
ESD	Electrostatic Discharge	
FCC	Federal Communications Commission	
GB	Gigabytes	Units of storage, each unit consisting of approximately 10 ⁹ 8-bit characters
GHz	Gigahertz	
GPS	Global Positioning System	
HMI	Human Machine Interface	
IEEE	Institute of Electrical and Electronic Engineers	
IP	Internet Protocol	
km	Kilometer	

Abbr.	Description	Definition
LSI	Local Systems Interface	
mA	Milliamp	Unit of electrical current
MAC	Media Access Control	
MB	Megabyte	Units of storage, consisting of approximately 106 8-bit characters
Mbps	Megabytes per second	
MHz	Megahertz	
MIB	Management Information Base	
MPDU _s	MAC Protocol Units	
Ms	Millisecond	
MTBF	Mean Time Between Failure	
OFDM	Orthogonal Frequency-Division Multiplexing	
OSI	Open Systems Interconnection	
OTA	Over-the-Air	
PHY	Physical Layer	Refers to a specific layer in the Open Systems Interconnection (OSI) reference model
PSID	Provider Service Identifier	
QOS	Quality of Service	
RF	Radio Frequency	
RF	Radio Frequency	
RSU	Roadside Unit	
SAE	Society of Automotive Engineers	
SCH	Service Channel	
SD	Secure Digital	
SRD	System Requirements Description	Describes requirements for a given system
SVC	Service Channel	
TXOP	Transmission Opportunity	See IEEE 802.11-2007
USB	Universal Serial Bus	
UTC	Universal Time, Coordinated	
V2I	Vehicle-to-Infrastructure	
V2V	Vehicle-to-Vehicle	
V2X	Vehicle-to-(Infrastructure and/or Vehicle)	
VSC3	Vehicle Safety Communications 3 (Consortium)	
WAAS	Wide Area Augmentation System	
WAVE	Wireless Access in Vehicular Environments	
WiMAX	Worldwide Interoperability for Microwave Access	
WSM	WAVE Short Message	
WSMP	WAVE Short Message Protocol	
WSMP-S	WSMP safety supplement	



Research and Innovative Technology Administration

Document Title: **“5.9GHz DSRC “Aftermarket Safety” Device Specification**

Document Type: **System Requirement**

Document #: **USDOTASD**

Issue Index: **3.1**

Volume No: **01**

Page: **10**

3 SYSTEM DESCRIPTION

3.1 Functional Description

The device discussed in this document is an aftermarket safety device for automotive use that will be installed in light vehicles, which will be used in the vehicle communication safety pilot that must be capable of both transmitting and receiving using dedicated short range communications (DSRC) radios, using the 5.9 Gigahertz (GHz) band approved for DSRC use by the Federal Communications Commission (FCC), and implement the appropriate Institute of Electrical and Electronics Engineers (IEEE) and Society of Automotive Engineers (SAE) standards (IEEE 802.11p, IEEE 1609 family, and SAE J2735).

3.2 System Design

The aftermarket safety device is intended for installation in light vehicles (i.e., vehicles whose weight is less than 10,000 pounds). The device will need to be safely mounted within the vehicle in such a position that does not distract the driver nor increase the risk to both driver and passenger safety while at the same time meeting the placement requirements (i.e. stationary positioning). It will also need to account for the difference in the location between the antenna, itself, and the vehicle location (center) as described in the Basic Safety Message.

This device is an aftermarket safety device installed in a vehicle that may also need to draw power from the vehicle; however, the installation of the device may not void the vehicle’s warranty or cause any harmful effect to the vehicle. It must be capable of sending and receiving the basic safety message as defined in SAE J2735, over a DSRC 5.9 GHz wireless communications link. The aftermarket safety device shall have a working human-machine interface (HMI); be capable of broadcasting and receiving messages, as defined in SAE J2735; and process the content of received messages (through resident software applications) to provide warnings and/or alerts to the driver of the vehicle in which it is installed. The aftermarket safety device shall have internal permanent storage capability. The aftermarket safety device must incorporate self-diagnostics that will alert the driver in case of a device failure. Finally, the positioning requirements are currently being defined by USDOT and will be addressed in subsequent releases of this specification.

The ASD will have a set of operational states as illustrated in the following diagram.

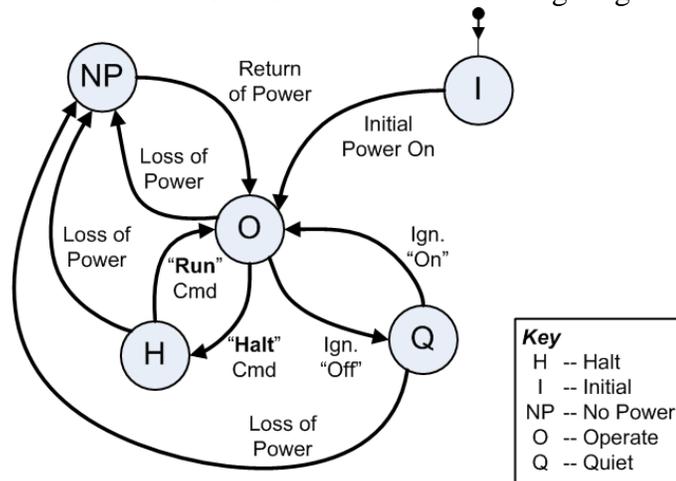


Figure 1.0 Aftermarket Equipment State Diagram

3.3 System Layout

The diagram below is for reference only. Only the shaded blocks are discussed in this document.

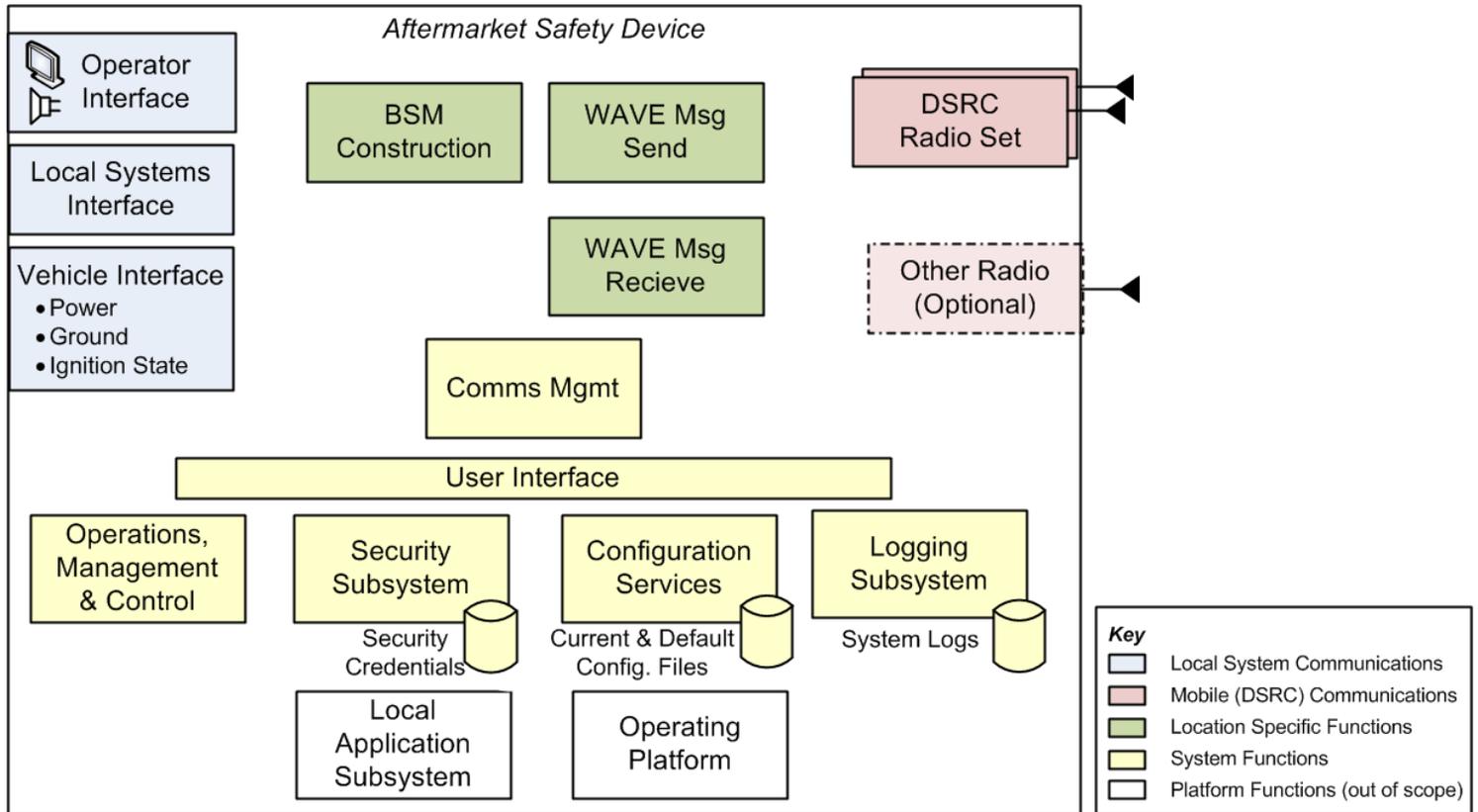


Figure 2.0 Aftermarket Equipment Diagram

4 SYSTEM REQUIREMENTS

4.1 Mechanical Requirements

The device shall meet all of the indicated quality requirements listing within this section.

4.1.1 Device Installation

Included by reference. Refer to the “OBE” requirements in Section 4.1.1 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqSYS001v001 Vehicle Installation Types

Description: The aftermarket safety device shall be installable in light vehicles (i.e., vehicles whose weight is less than 10,000 pounds).

Reference: None

Purpose: Provides for a large, diverse, field of Test Vehicles

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSYS002v001 Device Mounting Location - Driver

Description: The mounted aftermarket safety device shall not impede the driver’s required range of motion to operate a vehicle safely.

Reference: None

Purpose: Ensures driver’s safety in operating vehicle.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 13

Verification

Method: Analysis

SRD-USDOTASD-003-ReqSYS003v001 Device Mounting Location – Passenger Ingress and Egress

Description: The mounted aftermarket safety device shall not impede passengers’ ability to enter or depart the vehicle.

Reference: None

Purpose: Ensures passenger’s safety in entering or departing vehicle.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Analysis

4.1.2 Device Size

Included by reference. Refer to the “OBE” requirements in Section 4.1.2 of the Vehicle Awareness Device Specification, v3.5.

4.2 Performance Requirements

Included by reference. Refer to the “OBE” requirements in Section 4.2 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqSYS004v001 Device Receiver Failure

Description: If the aftermarket safety device is operating in the “Run” state and any DSRC radio stops receiving radio signals; then the device shall signal to the vehicle operator that the device needs servicing, in the manner of signaling as specified in the device’s operating manual.

Reference: None

Purpose: Ensures to inform the operator that the device is malfunctioning and no longer operating currently.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 14

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSYS005v001 Software Installation

Description: The aftermarket safety device shall support installing and maintaining authorized software additions or modifications components by authorized entitles over the LSI.

Reference: None

Purpose: Enables system installation and maintenance updates both remotely and locally.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

4.3 Environmental Requirements

The aftermarket safety device and all equipment shall have the capability to operate without failure under all environmental conditions experienced in the United States and its territories. The device shall also meet all the defined requirements in this section.

4.3.1 Operating Voltage

Included by reference. Refer to the “OBE” requirements in Section 4.3.1 of the Vehicle Awareness Device Specification, v3.5.

4.3.2 Operating Current

Included by reference. Refer to the “OBE” requirements in Section 4.3.2 of the Vehicle Awareness Device Specification, v3.5.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 15

4.3.3 Temperature and Humidity

The aftermarket safety device shall be designed to withstand long exposure to nearly constant high relative humidity and high temperature defined within this document.

Included by reference. Refer to the “OBE” requirements in Section 4.3.3 of the Vehicle Awareness Device Specification, v3.5.

4.3.4 Shock and Vibration

Included by reference. Refer to the “OBE” requirements in Section 4.3.4 of the Vehicle Awareness Device Specification, v3.5.

4.3.5 Electrostatic Discharge

Included by reference. Refer to the “OBE” requirements in Section 4.3.5 of the Vehicle Awareness Device Specification, v3.5.

4.3.6 Conducted Electrical Transients

Included by reference. Refer to the “OBE” requirements in Section 4.3.6 of the Vehicle Awareness Device Specification, v3.5.

5 FUNCTIONAL REQUIREMENTS

5.1 Interface Requirements

Included by reference. Refer to the “OBE” requirements in Section 5.1 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqINT001v001 DSRC Paired Radio Set

Description: The aftermarket safety device shall have two (2) 5.9GHz DSRC radios as called out in IEEE 802.11p and IEEE 1609 (see Figure 2.0)

Reference: None

Purpose: Application support

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Inspection

SRD-USDOTASD-003-ReqINT002v001 Optional Radio

Description: The aftermarket safety device equipment shall include one or more non-DSRC radios of the following types.

- 3G Cellular
- WiMAX (non-mobile)

Note: The actual radio medium will be determined by the future test site.

Reference: None

Purpose: Support ASD communications to back office services.

Disposition: Optional

Performance

Criteria: Pass\Fail

	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 17

Verification

Method: Inspection

SRD-USDOTASD-003-ReqINT003v001 Display

Description: The aftermarket safety device shall have a display for use as a human machine interface.

Reference: None

Purpose: Enables visual communication to the user

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Demonstration

SRD-USDOTASD-003-ReqINT004v001 Speaker

Description: The aftermarket safety device shall have a speaker capable of playing recorded or synthesized human speech for use as a human machine interface.

Note: Speech is required to support some of the applications (eg. CSW, CICAS-V)

Reference: DTFH61-11-RA-00003 Solicitation Appendix B System Level Test Procedures

Purpose: Enables audible communication to the user

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Demonstration

5.2 Operations, Management and Control

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 18

5.2.1 Operational States

For an overview of the following requirements, please refer to the operational state diagram (Figure 1.0) in Section 3.2.

Included by reference. Refer to the “OBE” requirements in Section 5.2.1 of the Vehicle Awareness Device Specification, v3.5.

5.2.2 Operational Configuration

Included by reference. Refer to the “OBE” requirements in Section 5.2.2 of the Vehicle Awareness Device Specification, v3.5.

5.2.3 Communications Message Log

SRD-USDOTASD-003-ReqCML001v001 Communications Message Storage

Description: The aftermarket safety device shall accept and store (log) transmitted and received communications messages to/from all interfaces in formatted files generically called Communications Message Log (CML).

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML002v001 Communications Message Timestamp

Description: The aftermarket safety device shall ensure that each logged communications message contains a UTC timestamp for each logged communications message. (i.e. Transmitted and/or recieved 802.11p frames).

Reference: None

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 19

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML003v001 Communications Message Separation by Interface

Description: The aftermarket safety device shall store messages to/from each communications interface (eg. each DSRC radio) in separate files or a combined file based on configuration parameters (default to Separate) in the Configuration File.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML004v001 Communications Message Separation by Direction

Description: The aftermarket safety device shall store communications messages sent to (outbound) and received from (inbound) each interface in separate files or a combined file based on a configuration parameter (default to Combined) in the Configuration File.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 20

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML005v001 Communications Message Log Time Threshold

Description: The aftermarket safety device shall close the active CML file when configurable time threshold (default to no time limit) is reached.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML006v001 Communications Message Log Size Threshold

Description: The aftermarket safety device shall close the active CML file when configurable size threshold (default to no size limit) is reached.

Reference: None

Purpose: Enables efficient access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 21

SRD-USDOTASD-003-ReqCML007v001 Communications Message Log Close when Halted

Description: The aftermarket safety device shall close the active CML file when transitioning to a “Halt” state.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML008v001 Communication Message Log Creation

Description: The aftermarket safety device shall create and use a new active CML file upon closing the previously active CML file.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML009v001 Communications Message Log Filename

Description: The aftermarket safety device shall create CML files with unique filenames consisting of a UTC date-stamp and a sequence number.

Reference: None

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 22

Purpose: Enables access to information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML010v001 Communications Message Log Retention

Description: The aftermarket safety device shall retain CML files indefinitely provided that sufficient storage is available.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML011v001 Communications Message Log Purge

Description: The aftermarket safety device shall, if there is insufficient storage available for additional CML files or records to be generated; purge the oldest of the currently stored CML files or records until sufficient storage is made available.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 23

Verification

Method: Test

SRD-USDOTASD-003-ReqCML012v001 Communications Message Log Access

Description: The aftermarket safety device shall enable authorized entities to access and review CML files stored (locally) on the device.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML013v001 Communications Message Log Off-Load

Description: The aftermarket safety device shall enable authorized entities to transfer CML files from the device to a (remote) back end system.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML014v001 Communications Message Log Deletion

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 24

Description: The aftermarket safety device shall enable authorized entities to delete CML files stored on the device.

Reference: None

Purpose: Enables access to communications information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML015v001 Logging Transmitted and Received 802.11p Frames

Description: The aftermarket safety device shall store all transmitted and received 802.11p frames in dedicated CML files.

Reference: None

Purpose: Enables comparison of transmitted and received packets during post test analysis

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML016v001 Communications Message Log Format

Description: All transmitted and received 802.11p frames shall be stored (in CML files) in pcap format file (using libpcap, v1.1.1 or later for Unix based systems; or WinPcap v4.1.2 or later for Microsoft Windows based systems, or equivalent for other operating systems).

Reference: None

Purpose: Determines the format of the communications message in the CML.

Disposition: Mandatory

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 25

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqCML017v001 Communications Message Log Storage Space

Description: The aftermarket safety device shall provide at least 4GB of storage space for the logging of transmitted and received 802.11 frames in CML files.

Reference: None

Purpose: Provides estimated file storage space for storing log data for 60 days.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.2.4 Device Positioning and Timing

Included by reference. Refer to the “OBE” requirements in Section 5.2.4 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqPOS001v001 Vehicle Speed Publishing

Description: The aftermarket safety device shall provide current vehicle speed and vehicle heading information to applications running on the aftermarket safety device.

Reference: None

Purpose: To make vehicle speed and position data available for device applications.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 26

SRD-USDOTASD-003-ReqPOS002v001 Vehicle Position Publishing

Description: The aftermarket safety device shall provide current vehicle position information to applications running on the aftermarket safety device.

Reference: None

Purpose: To make vehicle speed and position data available for device applications.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.2.5 Device Security

This section of the specification contains the requirements securing the device and controlling access to the device. Please note that the requirements relating to security of DSRC communications are located in a separate section (5.3.5) of the document.

SRD-USDOTASD-003-ReqSEC001v001 Secure Non-DSRC Communications Account Password Reset

Description: All system accounts for any non-DSRC communications interfaces shall have resettable passwords.

Note: All default Passwords **must** be provided to USDOT.

Reference: None

Purpose: Enables secure communications over IP enabled (non-DSRC) links in support of operations and maintenance.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 27

SRD-USDOTASD-003-ReqSEC002v001 Failed Access Attempt Reporting

Description: The aftermarket safety device shall log an error system message for each failed access attempt to any non-DSRC communications interface which is configured for IP.

Reference: None

Purpose: Enables secure communications over IP enabled (non-DSRC) links in support of operations and maintenance.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.2.6 System Status Log

SRD-USDOTASD-003-ReqSSL001v001 System Message Storage

Description: The aftermarket safety device shall accept and store messages generated by internal components in formatted files generically called System Status Log (SSL).

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL002v001 System Message Timestamp

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 28

Description: The aftermarket safety device shall ensure that each logged message contains a UTC timestamp for each logged message.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL003v001 System Status Log Time Threshold

Description: The aftermarket safety device shall close the active SSL file when configurable time threshold (default to no time limit) is reached.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL004v001 System Status Log Size Threshold

Description: The aftermarket safety device shall close the active SSL file when configurable size threshold (default to no size limit) is reached.

Reference: None

Purpose: Enables efficient access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 29

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL005v001 System Status Log Close when Halted

Description: The aftermarket safety device shall close the active SSL file when transitioning to a “Halt” state.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL006v001 System Status Log Creation

Description: The aftermarket safety device shall create and use a new active SSL file upon closing the previously active SSL file.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 30

SRD-USDOTASD-003-ReqSSL007v001 System Status Log Filename

Description: The aftermarket safety device shall create SSL files with unique filenames consisting of a UTC date-stamp and a sequence number.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL008v001 System Status Log Retention

Description: The aftermarket safety device shall retain SSL files indefinitely provided that sufficient storage is available.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL009v001 System Status Log Purge

Description: The aftermarket safety device shall, if there is insufficient storage available for additional SSL files or records to be generated; purge the oldest of the currently stored SSL files or records until sufficient storage is made available.

Reference: None

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 31

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL010v001 System Status Log Access

Description: The aftermarket safety device shall enable authorized entities to access and review SSL files stored (locally) on the device.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL011v001 System Status Log Off-Load

Description: The aftermarket safety device shall enable authorized entities to transfer SSL files from the device to a (remote) back end system.

Note: The off-load operation could result in the transfer of the System Status Log file directly to a remote back end system or to an intermediate device (e.g., laptop), which would then transfer the logs to the remote system.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 32

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL012v001 System Status Log Deletion

Description: The aftermarket safety device shall enable authorized entities to delete SSL files stored on the device.

Reference: None

Purpose: Enables access to status information required to support system operations, such as diagnosis, troubleshooting and support of wider Safety Pilot objectives.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqSSL013v001 System Status Log Entry Format

Description: All status message log entries shall be stored in pcap format file (using libpcap, v1.1.1 or later for Unix based systems; or WinPcap v4.1.2 or later for Microsoft Windows based systems, or equivalent for other operating systems).

Reference: None

Purpose: Determines the format of the message in the SSL.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 33

SRD-USDOTASD-003-ReqSSL014v001 System Status Log Storage Space Minimum

Description: The aftermarket safety device shall provide at least 250 Mb of storage space for the logging of system status messages in SSL files.

Reference: None

Purpose: Provides estimated file storage space for storing log data for 60 days.

Disposition: Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.3 DSRC Radio Subsystem

5.3.1 FCC Compliance

Included by reference. Refer to the “OBE” requirements in Section 5.3.1 of the Vehicle Awareness Device Specification, v3.5.

5.3.2 DSRC Radio Count

SRD-USDOTASD-003-ReqDRS001v001 Number of DSRC Radios

Description: The aftermarket safety device shall support two radios that are configured to operate at 5.9GHz (DSRC).

Reference: None

Purpose: Increased DSRC radio coverage and performance.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 34

5.3.3 IEEE 802.11

Included by reference. Refer to the “OBE” requirements in Section 5.3.3 of the Vehicle Awareness Device Specification, v3.5.

5.3.4 IEEE 802.11p

Included by reference. Refer to the “OBE” requirements in Section 5.3.4 of the Vehicle Awareness Device Specification, v3.5.

5.3.5 IEEE 1609.2

Included by reference. Refer to the “OBE” requirements in Section 5.3.5 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqDRS002v001 IEEE 1609.2 Certificate Storage

Description: The aftermarket safety device shall be able to simultaneous store at least two hundred thousand (200,000) 1609.2 certificates.

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09.

Purpose: Store sufficient security credentials to support 5 minute life span for approximately two years (12/hr x 24 hr/day x 60 days).

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqDRS003v001 IEEE 1609.2 Certificate Request

Description: The aftermarket safety device shall request new 1609.2 certificates, at a configurable set threshold level.

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 35

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqDRS004v001 IEEE 1609.2 Certificate Threshold

Description: The aftermarket safety device shall have a configurable threshold to understand when to request new 1609.2 certificates (default value 1 month).

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Support for 1609.2 operations.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-001ReqDRS005v001 IEEE 1609.2 Certificate Request Response Processing

Description: The aftermarket safety device shall accept and process responses to 1609.2 certificate requests as defined in IEEE P1609.2.

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Support for 1609.2 operations.

Disposition: Mandatory

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 36

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqDRS006v001 IEEE 1609.2 Certificate Decryption Key Request

Description: The aftermarket safety device shall request the decryption key for the next sequential batch of encrypted 1609.2 certificates, at a configurable set threshold level (default to 1 month).

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09, CAMP Security System Design Specification. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-001ReqDRS007v001 IEEE 1609.2 Certificate Decryption Key Processing

Description: The aftermarket safety device shall accept and process responses to 1609.2 certificate decryption key requests.

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09, CAMP Security System Design Specification. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Support for 1609.2 operations.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 37

Verification

Method: Test

SRD-USDOTASD-003-ReqDRS008v001 IEEE 1609.2 Certificate Revocation List (CRL) Request

Description: The aftermarket safety device shall request a 1609.2 Certificate Revocation List (CRL) at a configurable set threshold level (default to daily).

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09, CAMP Security System Design Specification. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-001ReqDRS009v001 IEEE 1609.2 (CRL) Processing

Description: The aftermarket safety device shall accept and process 1609.2 CRLs as defined in IEEE P1609.2.

Reference: IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09, CAMP Security System Design Specification. CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Support for 1609.2 operations.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 38

SRD-USDOTASD-003-ReqDRS010v001 IEEE 1609.2 Message Authentication

Description: Upon request from an (typically co-located on the device) application, the aftermarket safety device shall allow authentication of received digitally signed messages from a DSRC communications interface.

Note: Any validly formed message must be logged, irrespective of any application decision to authenticate or not. If an application chooses to authenticate a message, then it must reject a message that fails authentication.

Reference: None

Purpose: Support for 1609.2 operations.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-001-ReqDRS011v001 Unauthenticated Message Rejection

Description: The aftermarket safety device shall reject all messages from unidentified or uncertified sources, as controlled by the application.

Note: Any validly formed message must be logged, irrespective of any application decision to authenticate or not. If an application chooses to authenticate a message, then it must reject a message that fails authentication.

Reference: None

Purpose: Enables data integrity and security.

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 39

SRD-USDOTASD-003-ReqDRS012v001 IEEE 1609.2 Secure IP Data Exchange (Under Development)

Description: The aftermarket safety device shall support the exchange of secure data over DSRC-based IPv6 communications links.

Note: At a minimum, secure IP based communications over DSRC will be used for the exchange of data between the aftermarket safety device and the 1609.2 security credential management system. To date, it has not been determined if the communication path or just the payload is to be secured.

Reference: IEEE P1609.3-2010, IEEE P1609.2, Draft 9.3, Posted as 1609.2-v2-d9_3-2011-09 and CAMP VSC3 – Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) – Task 5: Security Management - Subtask 2: Security System Design Specification, September 14, 2011.

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.3.6 IEEE 1609.3

Included by reference. Refer to the “OBE” requirements in Section 5.3.6 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqDRS013v001 IP Firewall Rules

Description: The onboard equipment device shall comply with the IP Firewall Rules as defined in Appendix D of this specification for all DSRC Radios.

Reference: None

Purpose: Secure IP Communications

Disposition: Mandatory

Performance

Criteria: Pass\Fail

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 40

Verification
Method: Test

SRD-USDOTASD-003-ReqDRS014v001 IEEE 1609.3 IP Data

Description: The aftermarket safety device shall process both transmitted and received IPv6 packets.

Note: At a minimum, secure IP based communications over DSRC will be used for the exchange of data between the aftermarket safety device and the 1609.2 security credential management system. To date, it has not been determined if the communication path or just the payload is to be secured.

Reference: IEEE P1609.3-2010

Purpose: Standards Conformance

Disposition: Mandatory

Performance
Criteria: Pass\Fail

Verification
Method: Test

SRD-USDOTASD-003-ReqDRS015v001 IEEE 1609.3 WSMP Data

Description: The aftermarket safety device shall process (both transmit and receive) WAVE Short Message Protocol (WSMP) messages.

Reference: IEEE P1609.3-2010

Purpose: Standards Conformance

Disposition: Mandatory

Performance
Criteria: Pass\Fail

Verification
Method: Test

SRD-USDOTASD-003-ReqDRS016v001 IEEE 1609.3 Send Basic Safety Messages over R1C

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 41

Description: The aftermarket safety device shall send transmit generated Basic Safety Messages over DSRC R1C (as defined in SRD-USDOTASD-003-ReqDRS019, below).

Reference: IEEE P1609.3-2010, SRD-USDOTASD-003-ReqDRS019.

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.3.7 IEEE 1609.4

Included by reference. Refer to the “OBE” requirements in Section 5.3.7 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqDRS017v001 IEEE 1609.4 Radio Channel Usage

Description: Each DSRC radio in the aftermarket safety device shall be configurable to send messages either on Channel 178 during the Control Channel (CCH) interval, or on any of the 10 MHz or 20 MHz channels with no time interval restrictions.

Reference: IEEE P1609.4-2010

Purpose: Standards Conformance

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqDRS018v001 Continuous Mode – Default Configuration

Description: The aftermarket safety device shall have a default configuration of operating one (hereinafter referred R1C) of the paired DSRC radios in continuous mode on a configurable service channel with a default to Channel 172.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 42

Reference: IEEE P1609.4-2010

Purpose: DSRC Radio Operations.

Disposition: Mandatory

Performance
Criteria: Pass\Fail

Verification
Method: Test

SRD-USDOTASD-003-ReqDRS019v001 Alternating Mode – Default Configuration

Description: The aftermarket safety device shall have a default configuration of operating one (hereinafter referred to as R1A) of the paired DSRC radios in alternating (or channel switching) mode.

Reference: None

Purpose: Support for other messages.

Disposition: Mandatory

Performance
Criteria: Pass\Fail

Verification
Method: Test

SRD-USDOTASD-003-ReqDRS020v001 DSRC Radio Pair - Default Configuration

Description: The aftermarket safety device shall have a default DSRC radio configuration mode for the paired radios to support the following modes, as defined in IEEE 1609.4:

- R1A - Alternating Mode
- R1C - Continuous Mode; channel 172

Note: In addition to the default mode described above, it is possible that the paired radios will be configured with both radios set to Continuous mode, presumably on different channels. The aftermarket safety device will not be expected to support a configuration with both radios in Alternating mode.

Reference: IEEE 1609.4-2010

Purpose: Device functionality

Disposition: Mandatory

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.3.8 Radio Performance

Included by reference. Refer to the “OBE” requirements in Section 5.3.8 of the Vehicle Awareness Device Specification, v3.5.

5.3.9 Congestion Control

Included by reference. Refer to the “OBE” requirements in Section 5.3.9 of the Vehicle Awareness Device Specification, v3.5.

5.4 Other Communications

Included by reference. Refer to the “OBE” requirements in Section 5.4 of the Vehicle Awareness Device Specification, v3.5.

5.5 WSMP Message Processing

5.5.1 SAE J2735 Message Types

Included by reference. Refer to the “OBE” requirements in Section 5.5.1 of the Vehicle Awareness Device Specification, v3.5.

SRD-USDOTASD-003-ReqMPS001v001 SAE J2735 Map Data

Description: The aftermarket safety device shall conform to the section 5.6 (Map Data) SAE J2735 2009-11, implementing ASN.1 format.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 44

Note: The format of the Map Data Message, as provided by J2735, will be revised to account for open architecture. The actual data will not substantially change, but the format in which it is presented may change by up to 20 percent. Manufacturers will be notified when a draft revision to J2735 is available, which is anticipated in January 2012.

Reference: SAE J2735 2009-11 Section 5.6

Purpose: Enables interoperability by using industry standard message definitions.

Disposition: Mandatory if required by co-resident applications; otherwise Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqMPS002v001 SAE J2735 SPaT Message

Description: The aftermarket safety device shall conform to the section 5.12 (SPaT Message) SAE J2735 2009-11, implementing ASN.1 format.

Note: The format of the SPaT Message, as provided by J2735, will be revised to account for open architecture. The actual data will not substantially change, but the format in which it is presented may change by up to 20 percent. Manufacturers will be notified when a draft revision to J2735 is available, which is anticipated in January 2012.

Reference: SAE J2735 2009-11

Purpose: Enables interoperability by using industry standard message definitions.

Disposition: Mandatory if required by co-resident applications; otherwise Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

SRD-USDOTASD-003-ReqMPS003v001 SAE J2735 Traveler Information Message

Description: The aftermarket safety device shall conform to the section 5.15 (Traveler Information Message) SAE J2735 2009-11, implementing ASN.1 format.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 45

Reference: SAE J2735 2009-11, Appendix D of the Roadside Equipment Specification, v2.3.

Purpose: Enables interoperability by using industry standard message definitions.

Disposition: Mandatory if required by co-resident applications; otherwise Optional

Performance

Criteria: Pass\Fail

Verification

Method: Test

5.5.2 SAE J2735 Basic Safety Message Type – Details

Included by reference. Refer to the “OBE” requirements in Section 5.5.2 of the Vehicle Awareness Device Specification, v3.5.

5.5.3 SAE J2735 Traveler Information – Details

Included by reference. Refer to the Traveler Information Message details in Appendix D of the Roadside Equipment Specification, v2.3.

6 TEST REQUIREMENTS

6.1 Radio Transmission

Included by reference. Refer to the “OBE” requirements in Section 6.1 of the Vehicle Awareness Device Specification, v3.5.

6.2 Vehicle Location

Included by reference. Refer to the “OBE” requirements in Section 6.2 of the Vehicle Awareness Device Specification, v3.5.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 46

Appendix A: Vehicle Power Connector

Included by reference. Refer to the Appendix A of the Vehicle Awareness Device Specification, v3.5.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 47

Appendix B: Configuration File Format

(Under Development)

This appendix will define the structure and format of the Configuration File to be used by all aftermarket safety devices. This structured Configuration File will identify all configuration items required for the aftermarket safety device. Each configuration item will have specified default value. The format of the Configuration File will tentatively be a CSV text file.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 48

Appendix C: Security Profile

Included by reference. Refer to the Appendix C of the Vehicle Awareness Device Specification, v3.5.

 Research and Innovative Technology Administration	Document Title: “5.9GHz DSRC “Aftermarket Safety” Device Specification			
	Document Type: System Requirement			
	Document #: USDOTASD	Issue Index: 3.1	Volume No: 01	Page: 49

Appendix D: Firewall Rules

This section defines the Firewall Rules for the Aftermarket Safety Device.

Table D.1: — ASD Protected IP Interfaces

Interface	Purpose
DSRC Radios	Wireless communications with other DSRC enabled mobile devices and with DSRC enabled infrastructure devices.
Optional Radio	Wireless Communications with Local Management Device (LMD)
Local System Interface	Configuration and management interface

Table D.2: — Method of Assigning IP Addresses to Protected IP Interfaces

Interface	Address Scope
DSRC Radio	IPv6 link-local, non-routable
Optional Radio	IPv6 link-local, non-routable
	IPv4 non-routable
Local System Interface	IPv6 link-local, non-routable
	IPv4 non-routable

Table D.3 — Protected IP Interface Security Configuration

Interface	Rule	Protocol	Direction	Firewall Policies
DSRC Radios	Allow	IPv6	Ingress	Safety Pilot Security System to Safety Pilot ASDs ...ONLY after initial connection initiated by ASD
			Egress	Safety Pilot ASD to Safety Pilot Security System
		IPv4	Ingress	N/A
			Egress	N/A
	Deny	IPv6	Ingress	All sources except those defined in the “Allow” section
			Egress	All sources except those defined in the “Allow” section
		IPv4	Ingress	N/A
			Egress	N/A
Optional Radio	Allow	IPv6	Ingress	Traffic from LMD to ASD (TCP/IP Port – TBD)
			Egress	Traffic from ASD to LMD (TCP/IP Port – TBD)
		IPv4	Ingress	Traffic from LMD to ASD (TCP/IP Port – TBD)
			Egress	Traffic from ASD to LMD (TCP/IP Port – TBD)
	Deny	IPv6	Ingress	All sources except those defined in the “Allow” section
			Egress	All sources except those defined in the “Allow” section
		IPv4	Ingress	All sources except those defined in the “Allow” section
			Egress	All sources except those defined in the “Allow” section
Local	Allow	IPv6	Ingress	TELNET over TLS v1.2 traffic from LMD , TCP port 992

System Interface				IPSEC (for IPv6) traffic from LMD IPv6 Secure-Shell (SSH-2, SFTP) traffic from LMD, TCP, port 22
			Egress	Traffic from LMD to ASD (TCP/IP port TBD)
		IPv4	Ingress	TELNET over TLS v1.2 traffic from LMD, TCP/IP port 992 IPSEC (for IPv4) traffic from LMD IPv4 Secure-Shell (SSH-2, SFTP) traffic from LMD, TCP port 22
	Egress		Traffic from LMD to ASD (TCP/IP port TBD)	
	Deny	IPv6	Ingress	All sources except those defined in the “Allow” section
			Egress	All sources except those defined in the “Allow” section
		IPv4	Ingress	All sources except those defined in the “Allow” section
			Egress	All sources except those defined in the “Allow” section