US Department of Transportation

Office of the Secretary of Transportation for Research and Technology (OST-R)

Intelligent Transportation Systems --Joint Program Office

SOUTHEAST MICHIGAN TEST BED 2014 CONCEPT OF OPERATIONS

Version 1.0

December 29, 2014

Version History

#	Date	Author (s)	Summary of Changes
1.0	12/29/2014	Walton Fehr	Initial Version

Table of Contents

Table of Figures

Table of Tables

1 Scope

This document describes the Concept of Operations (ConOps) for the U.S. Department of Transportation (USDOT) Southeast Michigan Test Bed supporting connected vehicle research and development. This ConOps describes the current state of test bed operations, establishes the reasons for change, and defines operations for the 2014 version of the test bed in terms of functions/features and supporting operations.

The intended audience for this document includes the following:

- SEMI Test Bed Project Engineering Team
- ITS-JPO Program Leads and Support Staff
- ITS-JPO Program Engineering Teams
- Affiliated Test Bed Community
- Potential Pilot Deployment Teams
- Academic and Research Teams

2 References

The following table lists the references used to develop the concepts in this document. Any hyperlinks provided are accurate as of the date of publication.

Table 1 – References

#	Document (Location)
1	*Principles for a Connected Vehicle Environment*, U.S. Department of Transportation ITS Joint Program Office-HOIT, April 18, 2012 http://www.its.dot.gov/connected_vehicle/pdf/ConnectedVehiclePrinciples_final4-18-2012.pdf
2	*Connected Vehicle Reference Implementation Architecture Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. http://www.iteris.com/cvria/
3	*Core System Concept of Operations*, US Department of Transportation, Research and Innovative Technology Administration, October24, 2011 http://www.its.dot.gov/docs/CoreSystemConOpsRevE2.pdf
4	*Core System Architecture Document*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011 http://www.its.dot.gov/docs/CoreSystemArchitectureDoc_revC.pdf
5	*Core System Requirements Specification*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011 http://www.its.dot.gov/docs/CoreSystem_SE_SyRS_RevF.pdf
6	*Core System Deployment Critical Risk Assessment Report*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011 http://www.its.dot.gov/docs/CoreSystem_RiskReport_RevB.pdf
7	*Core System Standards Recommendations*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011 http://www.its.dot.gov/docs/CoreSystem_StdsRecommendations_RevA.pdf
8	*Connected Vehicle Technology - Test Bed Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. http://www.its.dot.gov/testbed.htm
9	Safety Pilot Model Deployment – "5.9GHz DSRC Aftermarket Safety" Device Specification, US Department of Transportation, Research and Innovative Technology Administration, Version 3.0, December 26, 2011
	Safety Pilot Model Deployment – *"5.9GHz DSRC Roadside Equipment" Device Specification*, US Department of Transportation, Research and Innovative Technology Administration, Version 3.0, March 1, 2012 http://www.its.dot.gov/safety_pilot/pdf/T-10001-T2-05_RSE_Device_Design_Specification_v30.pdf
11	Safety Pilot Model Deployment – *"5.9GHz DSRC Vehicle Awareness Device" Specification*, US Department of Transportation, Research and Innovative Technology Administration, Version 3.5, December 12, 2011 http://www.its.dot.gov/safety_pilot/pdf/Vehicle_Awareness_Device_Specification-r3-5--20111202.pdf
12	*1609.0-2013 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture* http://standards.ieee.org/findstds/standard/1609.0-2013.html
13	*1609.2-2013 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages* http://standards.ieee.org/findstds/standard/1609.2-2013.html
14	*1609.3-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services* http://standards.ieee.org/findstds/standard/ 1609.3-2010-Cor_1-2012.html
15	*1609.4-2010 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation*

http://standards.ieee.org/findstds/standard/1609.4-2010.html

16 *SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary™*, November 19, 2009 http://standards.sae.org/j2735_200911/

17 *SAE J3067 - Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods*, August 26, 2014 http://standards.sae.org/j3067_201408/

18 *SAE J2945 - Dedicated Short Range Communication (DSRC) Minimum Performance Requirements™*, Work in Progress http://standards.sae.org/wip/j2945/

19 USDOT Security Credential Management System. , US Department of Transportation, Research and Innovative Technology Administration, April 13, 2012. http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf

3 Acronyms and Definitions

The following table defines selected project specific terms used throughout this Concept of Operations document.

Table 2 – Acronyms

Term	Definition
3G	Third Generation
3P	Third Party
4G	Fourth Generation
ACL	Access Control List
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASD	Aftermarket Safety Device
ASN.1	Abstract Syntax Notation.1
ATIS	Advanced Traveler Information System
BSM	Basic Safety Message
C	Current
C2C	Center to Center
C2F	Center to Field
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
ConOps	Concept of Operations
CRL	Certificate Revocation List
CV	Connected Vehicle
CVRIA	Connected Vehicle Reference Implementation Architecture
DD	Data Distribution
DNS	Domain Name System
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
EVSD	Enhance Vehicle Situation Data
Gbps	Gigabits per second
GHz	Gigahertz
GID	Geographic Intersection Description
GPS	Global Positioning System
H	Historical
HC	Hyper Current

Term	Definition
HL	Hyper Local
HMI	Human Machine Interface
HTTPS	Hypertext Transfer Protocol (Secured)
I2V	Infrastructure to Vehicle
IP	Internet Protocol
ISD	Intersection Situation Data
ITS	Intelligent Transportation System
JPO	Joint Program office
L	Local
MAP	Map Data Message
MOA	Memorandum of Agreement
NHTSA	National Highway Traffic Safety Administration
O&M	Operations & Maintenance
OST-R	Office of the Assistant Secretary of Transportation for Research and Technology
OBE	On-Board Equipment
ORDS	Object Registration & Recovery Service
P2P	Peer-to-Peer
PDU	Protocol Data Unit
PDU	Protocol Data Unit
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
POC	Proof of Concept
R	Regional
RA	Registration Authority
RF	Radio Frequency
RSE	Roadside Equipment
SAE	Society of Automotive Engineers
SCM	Security & Credential Management
SCMS	Security & Credential Management System/Service
SDC	Situation Data Clearinghouse
SDPC	Situation Data Processing Center
SDW	Situation Data Warehouse
SM	Service Monitor
SPaT	Signal Phase and Timing
SPMD	Safety Pilot Model Deployment

Term	Definition
SSL	Secure Sockets Layer
TBD	To Be Determined
TCP	Transmission Control Protocol
TPAC	Third Party Application Center
TSD	Traveler Situation Data
UDP	User Datagram Protocol
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WAID	Wide Area Information Distributor
WAVE	Wireless Access in Vehicular Environments
Wi-Fi	Wireless Fidelity (short to mid-range wireless network)
WiMAX	Worldwide Interoperability for Microwave Access
WSM	WAVE Short Messages
WSMP	WAVE Short Message Protocol
XML	eXtensible Markup Language

Table 3 – Definitions

Term	Definition
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Aggregation	The process of combining data elements of similar format into a single data element that is a statistical representation of the original elements.
Analysis	The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other.
Anonymity	Lacking individuality, distinction, and “recognizability” within message exchanges.
Anonymous Certificate	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
APDU	Application Protocol Data Unit. This is a defined data structure that is transferred at a peer level between two applications.

Term	Definition
Application	One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task.
Application User	A user who interfaces with Application Layer software for a desired function or feature.
Assumption	A judgment about unknown factors and the future which is made in analyzing alternative courses of action.
Authenticate	The process of ensuring that an APDU originated from a source identified within the message
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticability	The ability of the receiver of information to authenticate the sender's identity or trustworthiness to send data within the domain. If required, this can be accomplished by verifying the incoming message has been digitally 'signed' by the sender.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.
Authorization	The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.
Available	Ready or able to be used
Backup	The ability of one System Element replacing another System Element's functionality upon the failure of that System Element.
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.
Boundaries	The area of management and control for a System or Object. It could be by latitude/longitude or by county or by regional jurisdictions.
Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog.
Cardinality	The characterization of the relationship between the number of sender(s) and receiver(s) of a data exchange. (e.g. broadcast (one-to-many) unicast (one to one))
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of this ConOps Specification these are considered the same.
Concept of Operations (ConOps)	A user-oriented document that describes a system's operational characteristics from the end user's viewpoint.
Confidentiality	The property of being unable to read PDU contents by any listener that is not the intended receiver
Configurable Parameter	Non-static data that can be adjustable and updated when needed.

Term	Definition
Configuration	Data that is used to customize the operational environment for a System Element or System User, or the System as a whole
Configure	The process of selecting from a set of option(s) or alternative values in order to create a specific operational environment.
Constraint	An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.
Contract	In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project.
Control	To exercise influence over.
Coverage Area	A geographic jurisdiction within which the System provides services.
Current (C)	Data that is current (relevant at the time of reporting for applications that do not require sub-second response).
Cyber Address	The cyber or network address of a test bed object.
Data Consumer	1) A user or system that is receiving or using data from another user or system. 2) Any test bed object that registers with and subsequently requests and receives delivery of data from a data warehouse.
Data Provider	1) Any test bed object that registers with and subsequently deposits data into a data warehouse 2) A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data.
Data Warehouse	A data storage facility that supports the input (deposit) and retrieval (delivery) of clearly defined data objects. This can be design and implemented in a variety of ways, including publish/subscribe and a traditional query based database.
Decrypt	To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access. See Encryption.
Digital Certificate or Signature	A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute - www.sans.org website.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it.

Term	Definition
Extensibility	The ability to add or modify functionality or features with little or no design changes.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSE and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Forwarding	The process of forward sending data onto another entity (system user) without modifying or storing the data for any substantial length of time.
Functionality	The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product.
Geo-Fence	An electronic set of geo reference points that form a bounded geographic region.
Geo-Referencing	The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Historic (H)	Data that is historical (relevant at the time of reporting for an indefinite interval).
Hyper Current (HC)	Data that is hyper current (relevant at the time of reporting for applications that require sub-second response).
Hyper Local (HL)	Data that is hyper local (relevant to a geographic area within ~1 minute travel distance)
Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Integrity	(1) To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible. (2) The property of being certain that a message's contents are the same at the receiver as at the sender.
Interconnect	The communications link between two architectural objects.
Internet	An interconnected system of networks that connects computers around the world via the TCP/IP protocol.
Issuance	For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.

Term	Definition
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Local (L)	Data is local (relevant to a geographic area within ~10 minute travel distance)
Local Current (LC)	Data is local (relevant to a geographic area within ~10 minute travel distance) and current (relevant at the time of reporting for applications that do not require sub-second response).
Logical Security	Safeguards that include user identification and password access, authentication, access rights and authority levels.
Misbehaving user	A user who exhibits misbehavior.
Misbehavior	The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages. etc.; either purposeful or unintended
Misbehavior Information	Includes Misbehavior Reports from System Users, as well as other improper System User acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate System User behavior.
Misbehavior Report	Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior.
Mobile	These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information
Non-repudiation	The property whereby a PDU is constructed in such a way that the PDU sender cannot effectively deny having been the sender of that PDU; and the PDU receiver cannot effectively deny having received a particular PDU.
On-Board Equipment (OBE)	Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.
Operators	These are the day-to-day users of the System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.
Permission	Authorization granted to do something. From the System's perspective, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the System.
Persistent connection	A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection.
Physical Security	Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored

Term	Definition
	information. This can range from simply a locked door to badge entry. with armed security guards
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively.
Process	A series of actions, changes, or functions bringing about a result.
Protocol Data Unit (PDU)	A defined data structure that is transferred at a peer level between corresponding software entities functioning at the same layer in the OSI standard model which are operating on different computing platforms that are interconnected via communications media .
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).
Regional (R)	Data that is regional (relevant to a geographic area within ~30 minute travel distance)
Registry	A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.
Reliability	Providing consistent and dependable system output or results.
Repackage Data	Data that is broken down for aggregation, parsing or sampling.
Scalability	The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign.
Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Secure Transmission	To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications.
Secure/Securely	Referring to storage, which consists of both logical and physical safeguards
Session-oriented Connection	A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection.
Software	Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software.
States	A distinct system setting in which the same user input will produce different results than it would in other settings. The System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby.
Status	Anomalies, actions, intermittent and other conditions used to inform the System Operator for reparation or maintenance.

Term	Definition
Subsystem	An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
Synchronization	the act or results of occurrence or operating at the same time or rate
System	(A) A collection of interacting elements organized to accomplish a specified function or set of functions within a specified environment. Typically the System Elements within the System are operationally self- contained but are interconnected and collaborate to meet the needs of the System and its Users. (B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.
System Element	(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment. (B) An object and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system element includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
System Need	A capability that is identified and supported within the System to accomplish a specific goal or solve a problem
System Personnel	This represents the staff that operates and maintains the System. In addition to network managers and operations personnel, System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployment teams, and Testers.
System User	System Users refers to Mobile, Field, and Center Systems.
Testers	These users verify the System's operation when any changes are made to its operating hardware or software.
Time	A measurable period during which an action, process or condition occurs.
Time synchronization	Calibration adjustment of date, hour, minutes and seconds for keeping the same time within a system.
Time-of-Day	Current hours, minutes and seconds within a day.
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Transition	A passage from one state, stage, subject, or place to another
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.
Unicast	The sending of a message to a single network destination identified by a unique address.

Term	Definition
User	An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions.
User Need	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.
Valid	When data values within a message are acceptable and logical (e.g., numbers fall within a range, numeric data are all digits).
Validate	To establish or confirm the correctness of the structure, format and/or contents of a data object.

4 Current Situation

4.1 Background and Objectives

The USDOT Connected Vehicle Test Bed in Southeast Michigan was implemented in 2007 to serve as the test facility for the Proof of Concept (POC) testing by the US DOT and the auto industry, to determine the feasibility and technical limitations of Dedicated Short Range Communications (DSRC) operating at the 5.9 GHz bandwidth. Over the past few years, the Southeast Michigan Test Bed has gone through numerous enhancements, including geographical expansion and technical and architectural updates, designed to support the connected vehicle industry's evolving needs for a test and development environment.

The set of upgrades currently underway started as an update to the USDOT Intelligent Transportation System (ITS) Joint Programs Office (JPO) Test Bed in Oakland County, MI and grew to include serving as a reference design for the demonstrations at ITS World Congress in September of 2014. These upgrades may extend to other connected vehicle research test and development environments in Michigan if they are successful. In the interim, these upgrades provide an enhanced platform that can be used to test several new capabilities that will be needed for more extensive deployment pilots in 2015 and 2016.

4.2 Description of Current Situation

The USDOT ITS JPO Connected Vehicle (CV) Test Bed in Oakland County, Michigan (known as the Southeast Michigan Test Bed) was implemented in 2007 to serve as the development and test facility for the POC engineering project conducted by the USDOT and the auto industry, to determine the feasibility and technical limitations of DSRC operating at the 5.9 GHz bandwidth. Over the past few years, the Southeast Michigan Test Bed has gone through numerous enhancements, including geographical expansion and technical and architectural updates, designed to support the connected vehicle industry's evolving needs for a test and development environment.

The focus of the Connected Vehicle program over the last few years has been on research, development and assessment of the efficacy of "Vehicle-to-Vehicle" V2V communications using WAVE/DSRC technologies to support V2V safety applications. There has been some attempt to assess the viability of the generation and collection of probe data, both in the form as defined in an older version of SAE J2735 and in the form of Basic Safety Messages (BSMs) defined in the current version of SAE J2735. The lynchpin of this research is the USDOT Safety Pilot which was conducted in Ann Arbor, Michigan from 2012-2103; and which will directly support the National Highway Transportation Safety Administration (NHTSA) decision as to whether these V2V Safety systems should be required of all light vehicles.

The Southeast Michigan Test Bed is located in Oakland County, MI, with CV roadside equipment and interconnected back-office systems that provide continuous real-time connectivity among users supporting the capability for stakeholders to test prototype CV equipment, applications and services. It currently covers 45 miles (194 km) comprising 75 linear miles (121 km) of roadways. A planned

expansion will add 6 miles (10 km) of roadways. The Southeast Michigan Test Bed is currently operated and managed by a USDOT contractor team. For further information, please refer to the ITS-JPO Southeast Michigan Test Bed portal. Any hyperlinks provided are accurate as of the date of publication.

The Test Bed is currently in use by a diverse range of ITS stakeholders for a variety of research and development activities including:

- RF engineering and protocol testing
- Safety, mobility and environmental algorithm development
- Research data collection and analysis
- Positioning, navigation and timing refinement
- Electronic signal phase and timing propagation
- Electronic map generation and propagation
- Product and service testing

The USDOT has established a collaborative Southeast Michigan Test Bed Project portal operated by Vanderbilt University for the dissemination of documentation developed by the Southeast Michigan Test Bed project team. Access to the portal can be arranged by contacting Walt Fehr, USDOT at Walton.Fehr@dot.gov . The Southeast Michigan Test Bed is part of the USDOT sponsored Affiliated Test Bed community. Information on the Test Bed Affiliates can be found at the ITS-JPO Affiliated Test Beds website.

5 Justification For and Nature of Changes

The need for a revised (upgraded) Southeast Michigan Test Bed, as described in this Concept of Operations, started with a set of planned minor updates and subsequently grew to include serving as a reference platform for staging demonstrations at ITS World Congress in September of 2014. The upgrades may extend to other connected vehicle research test and development environments in Michigan if they are successful. In the interim, these upgrades provide an enhanced platform that can be used to test several new capabilities that will be needed for more extensive deployment pilots in 2015 and 2016.

There are a number of good reasons for refocusing the purpose and evolving the structure and functionality of the Southeast Michigan Test Bed and they are summarized below.

5.1 Evolving Program Objectives

- ***Expand Participation*** – With the maturation of the Test Bed operations and maintenance (O&M) efforts and the associated stability of the testing environments, it becomes increasingly viable and desirable to more aggressively increase the outreach efforts to potential users of the test beds. The Affiliated Test Beds initiative enhances this opportunity by providing physical resources, such as the Roadside Equipment (RSE) or Security Certificate Management System (SCMS), or technical expertise and support that encourages participation by road operators, certification entities, and research organizations that would otherwise be unable to use the facility in Southeastern Michigan.
- ***Expand the Role of Connected Vehicle Research*** – With the Safety Pilot Model Deployment well underway, the USDOT Connected Vehicle Research Program is increasing its focus on dynamic mobility and environmental applications, as well as additional vehicle-to-infrastructure (V2I) safety applications. The Southeast Michigan Test Bed should become a vital resource in supporting those efforts.
- ***Play a Key Role in Connected Vehicle Deployment*** – The Southeast Michigan Test Bed is positioned to provide more than a key contribution to research and development efforts by additionally supporting the deployment decisions that face major stakeholders. The Southeast Michigan Test Bed will provide important insight to the deployment of systems and enabled applications; support the evolution of the connected vehicle technologies as real-world issues and challenges are faced and overcome; and help build the practical experience of road operators, particularly those involved in the development of affiliated test beds, as they proceed toward implementation.

5.2 Enhanced Operations Support

- ***Support for the2014 ITS World Congress*** – The Southeast Michigan Test Bed is uniquely positioned to support the Connected Vehicle community during the 2014 ITS World Congress, and could potentially serve as the enabling infrastructure for a variety of demonstrations during

this event. To better serve this role, the Southeast Michigan Test Bed will require a number of functional upgrades and selected technology refreshes.

To addresses these needs, the Southeast Michigan Test Bed will undergo the following changes in addition to the additions and modifications necessary to realize the concepts of operations described in this specification.

- ***Technology Refresh*** – The Roadside Units in the Southeast Michigan Test Bed will receive upgraded hardware, firmware and software.
- ***Increased SPaT/Map Broadcast Coverage*** – A number of additional signalized intersections will be upgrade to support the DSRC broadcast of Signal Phase and Timing (SPaT) and Geographic Intersection Description (MAP) messages.
- ***Introduction of Data Distribution Services*** – Brokered data exchanges services based on a "publish and subscribe" paradigm. This will best characterized as data warehousing, where deposits (of data) are made to the warehouse by willing data providers; and deliveries (of data) are made by the warehouse to interested consumers. These deposits and deliveries are orthogonal and the data providers and consumers are unaware of each other, and therefore of the source of any data they consume, or the destination of any data they provide. The Southeast Michigan Test Bed will have two different data warehouses: the Situation Data Warehouse and the Situation Data Clearinghouse, which will be defined and described later in this document.

5.3 Research Supporting Future Deployments

The central mission of the Southeast Michigan Test Bed is to support research and development of concepts, technologies, services and applications supporting Connected Vehicle Deployments. To that end, the following concepts have been selected for evaluation.

5.3.1 Test Bed Geographic Reference

As with many warehouse-based distribution systems, each Situation Data Warehouse or Clearinghouse will have an exclusive (non-overlapping) geographic region for which it will accept or provide goods (e.g., Enhanced Vehicle Situation Data Type Bundles). These geographic regions will be defined and bounded in units of degrees. Given that, the initial Situation Data Warehouse and Clearinghouse will be located in the Southeast Michigan 2014 Test Bed and will serve the 2 degree by 3 degree geographic region shown below. It will be divided into a geographic grid of "tiles", each of which will be a 10 millidegree square. This will yield 60,000 tiles. Geographic reference points used to exercise the functions described in this ConOps should be expressed with 10 millidegree precision to align with this "tiled" grid overlay. Please note that while the initial service area will be constrained to the Novi, Michigan area, the relatively large geographic boundary was selected to allow for expansion into the surrounding areas in the near future.

As more data providers come on line, the Southeast Michigan 2014 Test Bed service area could be further divided into 1 degree rectangles to support the greater granularity needed for the increased

data volumes. This process of subdivision could be iterated to scale as necessary to support continually increasing data volumes as more and more vehicles become equipped and as more applications are deployed.

Figure 1 – Southeast Michigan Test Bed Geographic Boundary

As other Affiliated Test Beds come on line, additional situation data warehouses/clearinghouses could be created with respective defined geographic regions. Each of these affiliated test beds could, in turn, have their respective geographic boundaries divided or subsequently subdivided to scale with increased data volumes.

5.3.2 Characterizing Data Context

One of the fundamental concepts underpinning the 2014 Southeast Michigan Test Bed is that data and/or information generated, situational or otherwise, is characterized by two key state elements: its time context and its space context. These two characterizations determine the relevance of the data/information to the recipient based on the recipient's proximity (in time and/or space) to the source of the data. All data/information that is generated within the Southeast Michigan Test Bed will accordingly be time and location stamped at creation. This allows each data recipient to respectively adjudicate the relevance and value of the data. The diagram below illustrates this concept.

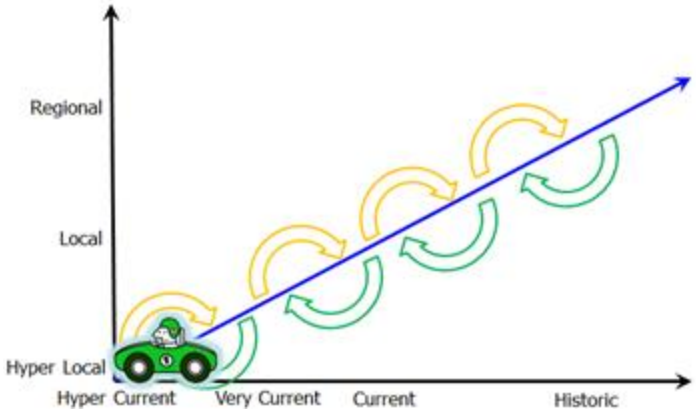

Figure 2 – Time Context of Test Bed Data/Information

The diagram below provides an illustrative scale identifying the respective values for the labels defined in the previous diagram.

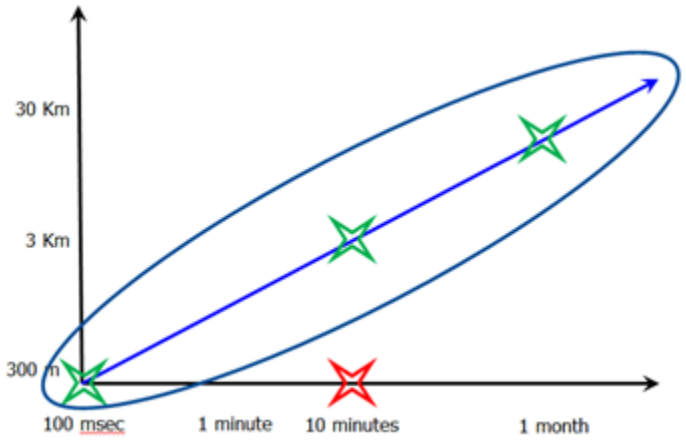

Figure 3 -- Space Context of Data/Information

5.3.3 Security/Privacy by Design

A fundamental concept that will pervade the design and development of the Southeast Michigan Test Bed is "Security/Privacy by Design". That is the Test Bed will be designed to protect the privacy of the users to the highest possible degree, while simultaneously protecting Test Bed assets and operations from cyber threats. This is especially challenging in a multi-application setting, because the user (mobile or fixed) may have higher privacy requirements than a specific application requires. There is an additional threat to the privacy of the user from correlations between applications. This is further complicated in that some CV applications, by their nature, will have to reveal sensitive or user-specific information: for example, BSMs reveal vehicle location. This makes it all the more important to ensure that:

- The 2014 Southeast Michigan Test Bed does not require applications to reveal this type of information unless it is absolutely necessary.

- Test Bed applications do not reveal this type of information unless it is absolutely necessary, as revealing the information within application A will allow it to be correlated with information from application B.

Further discussion of privacy and security for the multi-application setting can be found in EU-US ITS Task Force Standards Harmonization Working Group Harmonization Task Group 1 report 1-1, "Current Status of Security Standards", section 14 and Annex C.

The "Security/Privacy by Design" principle is limited to cyber security and does not consider the ancillary need for device physical security. It also does not address data protection at endpoints, for example encryption of databases. *It is assumed that endpoints that store Personal Identifiable Information (PII) shall take appropriate measures to protect all PII.*

5.3.4 Assessing Communications Characteristics

One of the fundamental objectives for the Southeast Michigan Test Bed is the assessment of communications performance and determination of their inherent suitability for supporting various Connected Vehicle applications. One of the key communications media supported in the Southeast Michigan Test Bed will be the 5.9 GHz Dedicated Short Range Communications (DSRC) band, using the IEEE 1609 - Wireless Access in a Vehicular Environment (WAVE) protocol suite. Interested readers are referred to those standards for more information. It is intended that all seven (7) DSRC channels be exercised within the Test Bed and that the following (at a minimum) communication characteristics be assessed:

- Congestion
- Interference (e.g. multipath, cross-channel)
- Performance (e.g. range)
- Data throughput
- Relative endpoint velocity

There are two types of communication patterns that support data exchanges between Connected Vehicle application objects (aka applications) in the Southeast Michigan Test Bed: broadcast and unicast (transactional, peer to peer).

Broadcast Communications

Typically sent as unencrypted messages with unencrypted data, Broadcast communications are intended to be "heard" by any receiver in the vicinity. These broadcast communications are sent without concern for how many (if any) receivers are actually in the vicinity, nor if the receivers are interested in the contents of the broadcast. It is up to the receiving device as to whether it wishes to interpret or act upon the received message. Well-known data structures are defined to facilitate broadcast communications between objects which do not have a pre-established relationship. The Southeast Michigan Test Bed will utilize the IEEE 1609.3 WAVE Short Message Protocol (WSMP) to broadcast WAVE Short Messages (WSM) encapsulating these pre-defined data structures. For the Southeast Test

Bed DSRC based communications, these pre-defined data structures will be adopted, adapted or developed based on the structures defined in the SAE J2735 Data Dictionary.

Examples of broadcast communications are SAE J2735 Basic Safety Messages (BSM) broadcast V2V over DSRC and SAE J2735 Signal Phase & Timing (SPaT) Messages broadcast I2V over DSRC. Please note that in the Southeast Michigan Test Bed, all broadcast messages will be digitally signed immediately by the transmitting device. In other words, if an informational message originates at a center-based service provider and is sent to an RSE for broadcast, it will be signed by the RSE as part of the complete transmission.

Unicast (Transactional) Communications

Unicast communications are typically exchanged between two Test Bed objects for the purpose of enacting a transactional data exchange. It is intended that any IP based communications path (e.g. 3G, 4G, Wi-Fi, WiMAX) can be used, provided both Test Bed objects are accordingly configured. IEEE WAVE over DSRC communications can be used as the sole hop between the two communication Test Bed objects (all V2V and some V2I); or it can be used as the first/last hop in a multi-hop routed communications path between two Test Bed objects using IP based communications.

For Southeast Michigan Test Bed objects, these transactions are usually small data transfers (up to approx. 10 Kbytes). However, depending upon operational circumstances and available communications paths, larger data transfers are possible. For unicast transactions conducted over DSRC/WAVE communications, it is strongly recommended that small size transactions be the norm, as there is no communications mechanism for maintaining transactions using adjacent RSE communications facilities. There is no functional support for anycast, multicast or groupcast communications. In addition to the fundamental assumption that each unicast transaction will be digitally signed, it is also assumed that virtually all unicast transactions will also be digitally encrypted. To that extent, the pictorial representations of the various transaction dialogs will have illustrative tags ("/s/" for signed and "/e/" for encrypted) for each transaction within the dialog. Solid lines indicate a request, and dashed lines indicate the corresponding response.

5.3.5 Development of Data Exchange Information Flow/Dialog Pattern

There will be a significant number of information flows between various Southeast Michigan Test Bed objects which are characterized as "peer to peer" data exchanges. Each information flow will be comprised of one or more information flow dialogs. It is the intent that all such information flow dialogs be developed using the following data exchange pattern as their basis. All Test Bed objects and Third Party objects that intend to interact with Test Bed objects will be required to follow the specific instantiation of this pattern as defined for the specific information flow dialog.

It is anticipated that there will be additional "peer to peer" information flow dialogs between third party objects operating as part of the Southeast Michigan Test Bed. It is anticipated and strongly encouraged that these Third Party application dialogs will be developed using the "Peer to Peer" Data Exchange Pattern described in below. Their specific usage and functionality is outside the scope of this document.

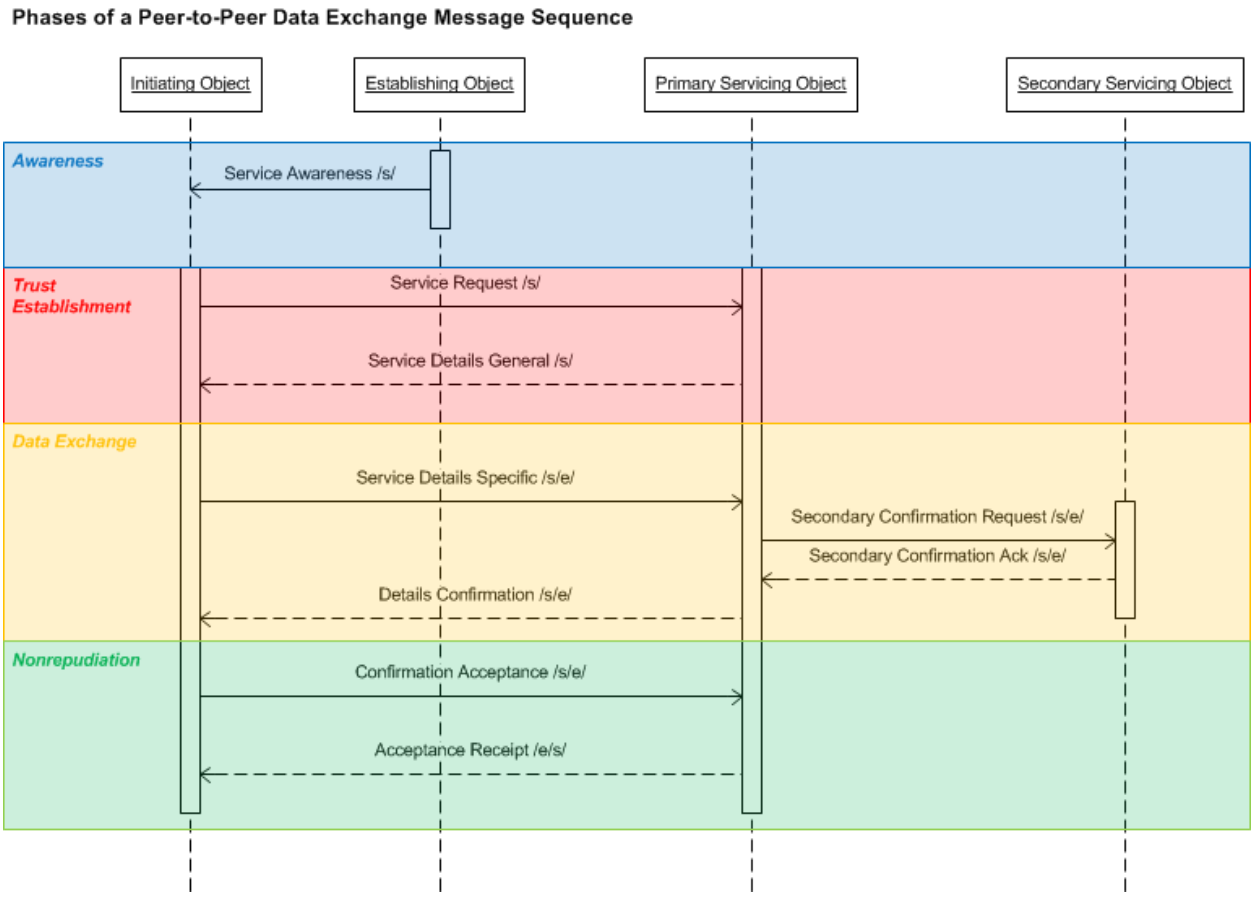

Figure 4 – Peer-to-Peer Data Exchange Sequence

The Information flow dialog pattern has four distinct phases as described below.

Phase 1: Service Awareness

As additional Test Bed objects are introduced (e.g. Connected Vehicle entering the Test Bed Area) into the Southeast Michigan Test Bed, they will need to become aware of other Test Bed objects which with the might wish to exchange data. This awareness must include sufficient information to allow the "interested" Test Bed object to determine where and when to reach out to for services that are currently or will be available. This awareness can be accomplished by several means:

1. The interested Test Bed object can have "a priori" knowledge, typically by hardcoding "well known" information or via a static or dynamic configuration mechanism.
2. The interested Test Bed object can request ("pull") the information from one or more "well known" service information repositories, which for the Southeast Michigan Test Bed will be the Object Registration and Lookup Service (ORDS). This obviously implies that all Test Bed objects wishing to be "advertised" need to register and maintain their service information with the ORDs and also need to have a "well known" identifier that can be used to query the ORDS.
3. The interested Test Bed object can receive ("push") the needed information from one or more service announcements provided by other Test Bed objects who have received the information

either "a priori" or from the ORDS. With respect to the Southeast Michigan Test Bed, these service advertisements will be provided by the Southeast Michigan Test Bed Roadside Equipment. It should be noted that the "interested" Test Bed objected must contain internal logic sufficient to determine whether to act on the service advertisement

It should be noted that "a priori" awareness can be minimized to just that for the ORDS. With that service awareness, all additional service awareness information can be obtained.

Phase 2: Trust Establishment

Trust Establishment is based on the premise that both parties participating in a "peer to peer" data exchange must trust the communications received from the correspondent Test Bed object and must be able to provide "trusted" communications in return. For the Southeast Michigan Test Bed, this is based on the foundation that all participating Test Bed objects shall have valid SCMS security credentials installed as necessary to support Test Bed operations in general, and specifically to support "peer to peer" data exchanges. It is also based on the premise that the "initiating" Test Bed object has already established service "awareness" of the corresponding Test Bed object to the extent that it is able to initiate the "peer to peer" data exchange.

The "initiating" Test Bed object shall initiate the communications dialog when logic dictates that this is the correct choice. To affect this data exchange, the "initiating" Test Bed object will format, construct and transmit a secure "Service Request" message in which it will both identify itself and declare its intent to initiate a "peer to peer" data exchange. This "Service Request" message will include sufficient security credential information so as to allow the correspondent Test Bed object to verify that the "initiating" Test Bed object is currently authorized to participate in Test Bed operations in general, and specifically to enter this specific "peer to peer" data exchange operation.

Upon receipt of the "Service Request" message, the correspondent Test Bed object will verify that the "initiating" Test Bed is currently authorized to participate in the specific "peer to peer" data exchange. Upon this verification, the correspondent Test Bed object will format, construct and transmit a secure "Service Response" message in which it will both confirm its identity and declare its agreement to participate in the specific "peer to peer" data exchange. This "Service Response" message will include sufficient security credential information so as to allow the "initiating" Test Bed object to verify that the correspondent Test Bed object is indeed the Test Bed object indicated in the service information obtained during the service awareness phase. It is possible that the "Service Response" message could also include informational elements that are relevant to the configuration of the specific data exchange session, configuration of all data exchanges with the correspondent object, or even system wide configuration elements.

At this point, either both Test Bed objects have respectively confirmed the validity of the other Test Bed Object, in which case trust has been established; or the "peer to peer" data exchange is effectively cancelled.

Phase 3: Data Exchange

The respective messages within the Data Exchange phase will, by necessity, be specific to each dialog of each information flow dialog. The respective data exchange phases of all information flow dialogs with or between Test Bed objects will be defined in a separate design document.

As mention previously, it is anticipated that there will be additional "peer to peer" information flow dialogs between third party objects operating as part of the Southeast Michigan Test Bed. The specific usage and functionality of the data exchange phase of these dialog is outside the scope of this document.

That being said, the following list of common concepts should be applied to each dialog.

1. Each Test Bed object participating in the dialog must utilize appropriate SCMS security credentials to send "sensitive information" using signed/encrypted communications.
2. The dialog will terminate upon expiration of the security credentials of either participant.

Non-Repudiation

The Non-Repudiation phase is intended to provide one or more of the following benefits:

1. Graceful termination of the dialog, which can be initiated by either participating Test Bed object.
2. Assurance that the dialog cannot later be denied by either of the participating Test Bed objects.
3. Confirmation of receipt of sensitive information using signed/encrypted communications.
4. Confirmation of dialog results, such as bundles sent/received, for accounting purposes.

The "terminating" Test Bed object shall initiate the non-repudiation phase of the communications dialog when logic dictates that this is the correct choice. To affect this phase change, the "terminating" Test Bed object will format, construct and transmit a secure "Confirmation Acceptance" message in which it declare its intent to terminate the "peer to peer" data exchange. This "Confirmation Acceptance" message will include sufficient information so as to allow the correspondent Test Bed to ensure non-repudiation.

Upon receipt of the "Confirmation Acceptance" message, the correspondent Test Bed object will format, construct and transmit a secure "Confirmation Receipt" message in which it will both confirm its agreement to terminate the "peer to peer" data exchange. This "Service Response" message will include sufficient information so as to allow the correspondent Test Bed to ensure non-repudiation.

At this point, either both Test Bed objects have respectively confirmed the completion of the "peer to peer" data exchange thus ensuring non-repudiation.

5.3.6 Data Bundling

For efficiency of bandwidth and expediency, individual data objects of the same type/classification will often be aggregated into a single data construct referred to as a "data bundle". A data bundle will typically have the following structure, with the respective bundle header fields and constituent messages varying for each type of bundle.

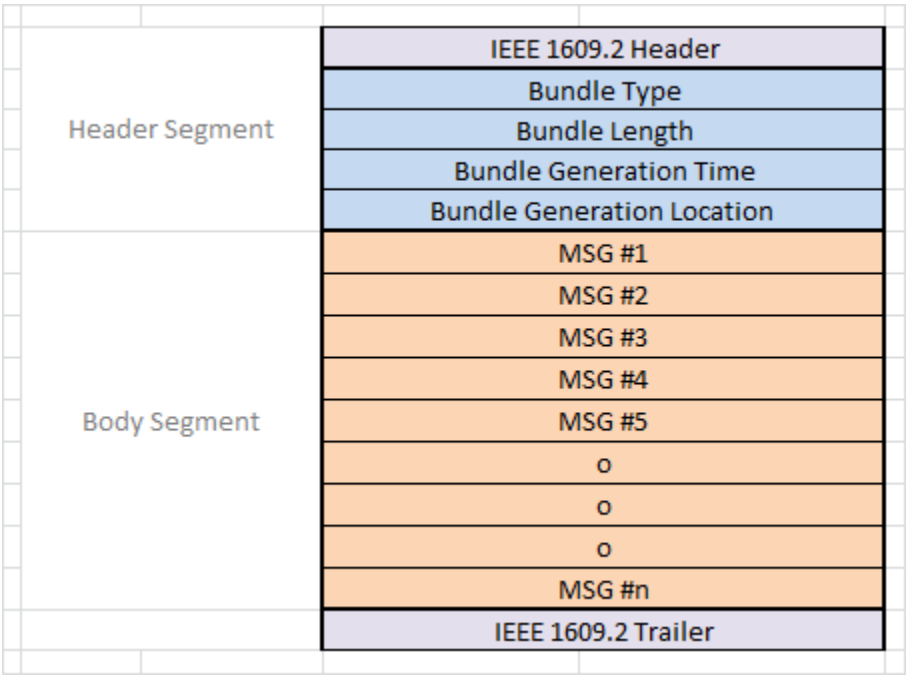

Figure 5 -- Example Data Bundle Structure

The structure and composition of the individual objects will be explicitly defined in other Test Bed specifications. The number of discrete data objects within each bundle will be dynamically determined based on the aggregate size of the messages and the underlying communications media characteristics.

5.4 System Needs

The System Needs listed below are designed to answer two basic questions:

- What does the System need to do?
- What do users need from the System?

They are categorized for ease of use.

5.4.1 System User Authorization

The System needs to manage the authorization mechanisms to define roles, responsibilities and permissions for System Users. This allows the Test Bed's system administrators to establish operational environments where different connected vehicle system users may have different capabilities.

Need ID	Need Description
CA-01	The System needs to manage authorization mechanisms to define roles, responsibilities and permissions for System Elements. This enables the System to establish operational environments where different System Elements may have different capabilities in terms of interacting with one another.

Need ID	Need Description
CA-02	The System needs to manage authorization mechanisms to define roles, responsibilities and permissions for System Users. This enables the System to establish operational environments where different System Users may have different capabilities in terms of accessing System Elements and interacting with one another. For instance, some mobile entities may be authorized to request signal priority, or some Centers may be permitted to use the geographic broadcast service, while those without those permissions would not.

5.4.2 Authorization Management

Security and Credentials Management (SCM) is a set of support applications that are used to ensure the trusted communications between mobile devices and other mobile devices or roadside devices and protect data they handle from unauthorized access. The applications grant trust credentials to qualified mobile devices so that those devices may be considered trusted by other devices that receive trust credentials from the SCM applications. The applications allow credentials to be requested and revoked, as well as to secure the exchange of trust credentials between parties, so that no other party can intercept and use those credentials illegitimately. The applications provide security to the transmissions between connected devices, ensuring authenticity and integrity of the transmissions. Additional security features include privacy protection, authorization and privilege class definition, as well as non-repudiation of origin.

Need ID	Need Description
AM-01	The System needs to grant trust credentials to System Elements so that they may be considered trusted by other System Elements that likewise receive trust credentials from the System.
AM-02	The System needs to be able to revoke the credentials it distributes, so that a misbehaving or malfunctioning System Element can be recognized as such.
AM-03	The System needs to secure the exchange of trust credentials between itself and its intended System Elements, so that no other party can intercept and use those credentials illegitimately.
AM-04	The System needs be constructed so that two or more System Elements are required to link the identity of a System User with a set of trust credentials, to protect user privacy.
AM-05	The System needs to be constructed so that two or more System Elements are required to associate multiple credentials that were distributed to a user, to protect user privacy.
AM-06	The System needs to accept misbehavior reports from users, so that malfunctioning and misbehaving System Users may be identified and their privileges revoked if necessary.
AM-07	The System needs to provide a mechanism for a System User without credentials to request credentials, so that the user may participate in Test Bed activities.

5.4.3 Infrastructure Management

Infrastructure management is a support application that maintains and monitors the performance and configuration of the infrastructure portion of connected vehicle. This includes tracking and management of the infrastructure configuration as well as detection, isolation, and correction of infrastructure service problems. The application also includes monitoring of performance of the infrastructure equipment, which includes the RSE as well as the communication link to back office functions.

Need ID	Need Description
IM-01	The System needs to track and manage of the configuration of infrastructure-based System Elements, which includes the RSE as well as the communication link to back office functions.
IM-02	The System needs to detect, isolate and correct infrastructure service problems of infrastructure-based System Elements.
IM-03	The System needs to monitor the performance of infrastructure-based System Elements.
IM-04	The System needs to monitor the physical and cyber security of infrastructure-based System Elements.
IM-05	The System needs to be designed to allow for sufficient configurability to support operational needs.
IM-06	The System needs to have sufficient internal operations and diagnostic message generation and logging capabilities to allow for operational monitoring, troubleshooting, and control.

5.4.4 Trusted Communications

Trusted communications is an essential foundation for all CV operations. These communications needs complement the Authorization Management needs to provide effective and secure communications between connected devices.

Need ID	Trusted Communications Need Description
TC-01	The System needs to provide a secure repository for the collection, storage and dissemination of the network addresses and services of System Elements. This is essentially a list of “what” services are supported, “who” provides each service and “where” to go to obtain these services.
TC-02	The System needs to provide a mechanism for System Elements to store their current cyber addresses and services into a secure repository.
TC-03	The System need to provide the trusted network addresses of System Elements located in a secure repository to other authorized System Elements

Need ID	Trusted Communications Need Description
TC-04	System Elements needs to provide secure communications mechanisms necessary to protect data it transmits and/or receives from unauthorized access. This is required to support applications that exchange sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.
TC-05	The System needs to facilitate and establish trust between authorized entities that communicate with the System and with each other. Such trust relationships are necessary so that applications can be assured that entities are who they say they are, and therefore trust the source and data it receives.
TC-06	The System needs to revoke the trust relationship they have with authorized entities when necessary. A trusted entity may operate in a fashion that indicates it should no longer be trusted, in which case applications must have a way of revoking that trust.
TC-07	All participants in the Southeast Michigan Test Bed need to operate on a common time base. Coordination of time between the entities that operate applications as well as those providing Test Bed services prevents internal errors and enables time-sensitive interactions between Test Bed Objects.
TC-08	The System needs to connect to the Internet. This allows the System to provide services to any entity capable of connecting to the Internet
TC-09	Every message sent by a System User or a System Element to any other System User or a System Element needs to be able to be authenticated by the receiver, so the receiver knows that the originator is a trusted source.
TC-10	Every broadcast (DSRC) message needs to specify the privilege class of the originator, for example to distinguish emergency vehicles from general vehicles.
TC-11	Messages need to be constructed in such a way as to make it difficult to associate messages with one another, to help maintain user privacy.
TC-12	Every broadcast (DSRC) message need to be constructed in such a way as to make replay attacks impractical, in order to minimize the number of such attacks.
TC-13	Every broadcast (DSRC) message from the System needs to be non-reputable in origin; that is, that the originator cannot deny having sent the message. This is so that when a received message invokes actions on the receiver it may be necessary to show that the behavior was in response to a specific transmitted message. Similarly messages may be received that indicate misbehavior of the transmitting vehicle or its equipment that will give rise to a misbehavior report. Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information.
TC-14	Every Broadcast (DSRC) message transmitted V2V need to use pseudonyms to help protect user's privacy.

5.4.5 Data Distribution

Data Distribution manages the distribution of data from data providers to data consumers and protects this data from unauthorized access. The system informs data providers of how to provide data, manages data subscriptions, and provides data forwarding capabilities. The System also maintains a directory of Data consumers that want data and supports multiple distribution mechanisms including publish-subscribe, data query directed to the System, and directly from data provider to data consumer. The System allows data consumers to specify (and change the specification of) data they wish to receive.

Need ID	Need Description
DD-01	The System needs to protect data it handles from unauthorized access. This is required to support the exchange of sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.
DD-02	The System needs to provide a mechanism for data providers to deposit “Store and Forward” data for subsequent retrieval by data consumers.
DD-03	The System needs to securely store all deposited data which is categorized as “Store and Forward”.
DD-04	The System needs to provide a mechanism for data consumers to retrieve “Store and Forward” data that has been previously deposited into the System by data providers. This is a single request for a certain set of data. Parameters include data type, time interval of when the data was generated, and location of where the data was generated. This enables the retrieval by interested data consumers of anonymously-provided data, without requiring them to enter into a relationship with data providers.
DD-05	The System needs to dispose of all received data which is categorized as “Store and Forward” after the configurable “lifespan” interval has expired.
DD-06	The System needs to provide a mechanism for data providers to deposit “Immediately Forward” data for subsequent distribution to data consumers.
DD-07	The System needs to provide a mechanism for data consumers to request “Immediately Forward” data that will be deposited into the System by data providers. This is a single request for a subscription to a certain type of data. Parameters include data type, time interval of when the data was generated, and location of where the data was generated. This enables the “real time” distribution of anonymously-provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example this includes data type, geographic range, frequency and sampling rate.
DD-08	The System needs to provide a mechanism for distribution of “Immediately Forward” data for subsequent distribution to data consumers.
DD-09	The System needs to dispose of all deposited data which is categorized as “Immediately Forward” upon completion of associated distribution.

Need ID	Need Description
DD-06	The System needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics need to include type, frequency and location where data was generated, so that users that have requested data (see need data request) can differentiate between available data. This need enables data providers to direct the data they create to data consumers, and serves as the provider-side corollary to the data request need. This supports a variety of applications, including those focused on the center provision of data to users. It also serves as the answer to the mobile entity's question of "I have data, how do I provide it and to whom?"
DD-07	Data Distribution needs to provide a mechanism to distribute data it receives. Data Distribution needs to provide this distribution mechanism, rather than relying on individual provider-consumer relationships, because multiple consumers may want access to the same data. By having Data Distribution distribute the data, data creators are relieved of the need to transmit the data multiple times. Also, some data that may be critical to the proper functioning of mandatory applications, such as data supporting geo-location of users (position corrections), time base data and roadway geometry data, all of which likely comes from a single source and needs to be distributed to large numbers of users. Additionally, mobile users may interact over resource-constrained communication links, so System-provided data redistribution reduces the potential load on those links.
DD-09	Data Distribution needs to provide the information necessary for applications that wish to communicate with a group of entities in a specific area to do so. This capability enables applications to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of applications that might use this include Amber Alerts, traffic information, and air quality alerts.

5.4.6 Signal Phase and Timing

Signal Phase and Timing Application is a support application that provides the current intersection signal light phases. The current state of all lanes at a single intersection are provided as well as any preemption or priority then follows in a structure for the whole intersection. This application is used to support a variety of V2I applications.

Need ID	Need Description
TSI-01	The System needs to provide an Interface for transfer of traffic signal information from a traffic signal controller. This includes the value of the time remaining until the next change in the state of each lane movement at the intersection.
TSI-02	The System needs to accept and process traffic signal information from a traffic signal controller.
TSI-03	The System needs to translate native traffic signal information into Signal Phase and Timing (SPaT) messages as defined in SAE J2735. It is assumed that this translation will be accomplished by a SPaT "black box" which will be procured and therefore will not be developed as part of this project.
TSI-04	The System needs to regularly provide wireless transmission the most recent SPaT message to Connected Vehicles and Connected Travelers approaching the signalized intersection.
TSI-05	The System needs to store generated SPaT messages in a bundled format for subsequent retrieval.
TSI-06	The System needs to provide an Interface for the transfer of geometric intersection design (GID) of intersections. The GID needs to include all allowed movements regardless of the number of approaches or complexity of the intersection from the roadside equipment in time for a mobile device to process and effectively use the information in corresponding applications.
TSI-07	The System needs to accept and process GID information.
TSI-08	The System needs to translate GID information into MAP messages as defined in SAE J2735.
TSI-09	The System needs to regularly provide wireless transmission the most recent MAP message to Connected Vehicles and Connected Travelers approaching the signalized intersection.
TSI-10	The System needs to store generated MAP messages in a bundled format for subsequent retrieval.

5.4.7 User Support

The mechanisms for access to this System's resources need to be documented to the extent that users can access those resources in a straightforward manner.

Need ID	Need Description
US-01	System Implementers need the Southeast Michigan Test Bed system and interface designs documented so that they can duplicate the Southeast Michigan Test Bed interfaces and systems without access to the original System Implementers.
US-02	System Owners need the Southeast Michigan Test Bed system and interface designs documented so that they can maintain the Southeast Michigan Test Bed interfaces and systems without needing ongoing support from the System Implementers.
US-03	System Operators need the Southeast Michigan Test Bed systems operational interfaces documented so that they may control all Southeast Michigan Test Bed equipment and operations without needing ongoing support from the System Implementers.
US-04	System Users need the Southeast Michigan Test Bed interfaces documented to the extent that they can use the Southeast Michigan Test Bed without needing ongoing support from the System Implementers.

6 Concepts for Proposed System

This section will describe the key concepts for the 2014 Southeast Michigan Test Bed. Although it will cover the Test Bed as a whole, it will primarily focus on the new concepts and features.

6.1 Operational Policies and Constraints

There following operational policies/constraint have been identified so far.

1. The upgraded Southeast Michigan Test Bed must be operationally ready for ITS World Congress in October 2014.
2. Privacy with respect to both the identity of users and of data exchanged will be "by design".
3. Electronic communications that need to be made secure (digitally signed and/or encrypted) will do so using a common process based on IEEE 1609.2.
4. Information flows between test bed objects, especially those that are characterized as a full round trip will be based on a common message sequence pattern.
5. Information flows between test bed objects, will be digitally signed.
6. Unicast Information flows between test bed objects will be encrypted.
7. All information flows that are unicast will be based on IPv6.
8. All unicast information flows that are characterized as "best effort" will utilize User Datagram Protocol (UDP).
9. ASN.1 encoding will be used for all data sent from an OBE or from an RSE.
10. A more vulnerable Test Bed object, from a security perspective, will always initiate any data exchange with a less vulnerable Test Bed object. For example vehicles always initiate exchanges with either roadside or center based objects, and roadside objects always initiate exchanges with center based objects. If two Test Bed objects are considered equally vulnerable, then either may initiate the data exchange.
11. The DSRC 5.9 GHz spectrum will be exercised on all seven radio (7) channels as defined by IEEE 1609.
12. Anyone can drive in the Southeast Michigan Test Bed geographic area, but they abide by FCC regulation in regards to 5.9 GHz bandwidth use. E.g. No harmful interference.
13. In order to participate collaboratively with others, participants must sign a Memorandum of agreement (MOA). Interested parties are referred to the ITS-JPO Affiliated Test Bed site.

6.2 Description of the Proposed System

The architecture presented in this section is directly based on the USDOT CVRIA and subsequently tailored to meet the needs and vision of the 2014 Southeast Michigan Test Bed. The Connected Vehicle Reference Implementation Architecture (CVRIA) described at the CVRIA website.

6.2.1 System Architecture

The Southeast Michigan 2014 Test Bed architecture is illustrated and defined below. Both the physical and enterprise architectures will be presented, along with accompanying tables identifying and describing the architecture objects and the connections between them. Three diagrams of this architecture are presented. The first is a comprehensive diagram in which Test Bed objects and Third Party objects are both shown. When virtually identical (with respect to their functionality) Test Bed and Third Party objects both exist; they have been shown as a consolidated "Connected Vehicle" object. The comprehensive diagram is followed by a "Test Bed" diagram which only depicts the Test Bed objects and does not depict any Third Party objects. The final "Third Party" diagram depicts placeholder objects indicating whereby Third Parties may develop custom objects (software and/or hardware) which will be able to leverage supporting Test Bed objects (also depicted in this diagram) to enable their Connected Vehicle systems.

6.2.1.1 Physical View

This section presents the physical view of the 2014 Southeast Michigan Test Bed architecture. The physical view starts with a top-level, called "Layer 0" drawing depicting all of the physical objects in the project followed by the lower or middle, "Layer 1" that adds application objects and their interconnects.

6.2.1.1.1 Physical – Layer 0

The following diagram provides a high-level conceptual architecture for the 2014 Southeast Michigan Test Bed. It is followed by two tables which provide definitions of the objects and physical interconnects.

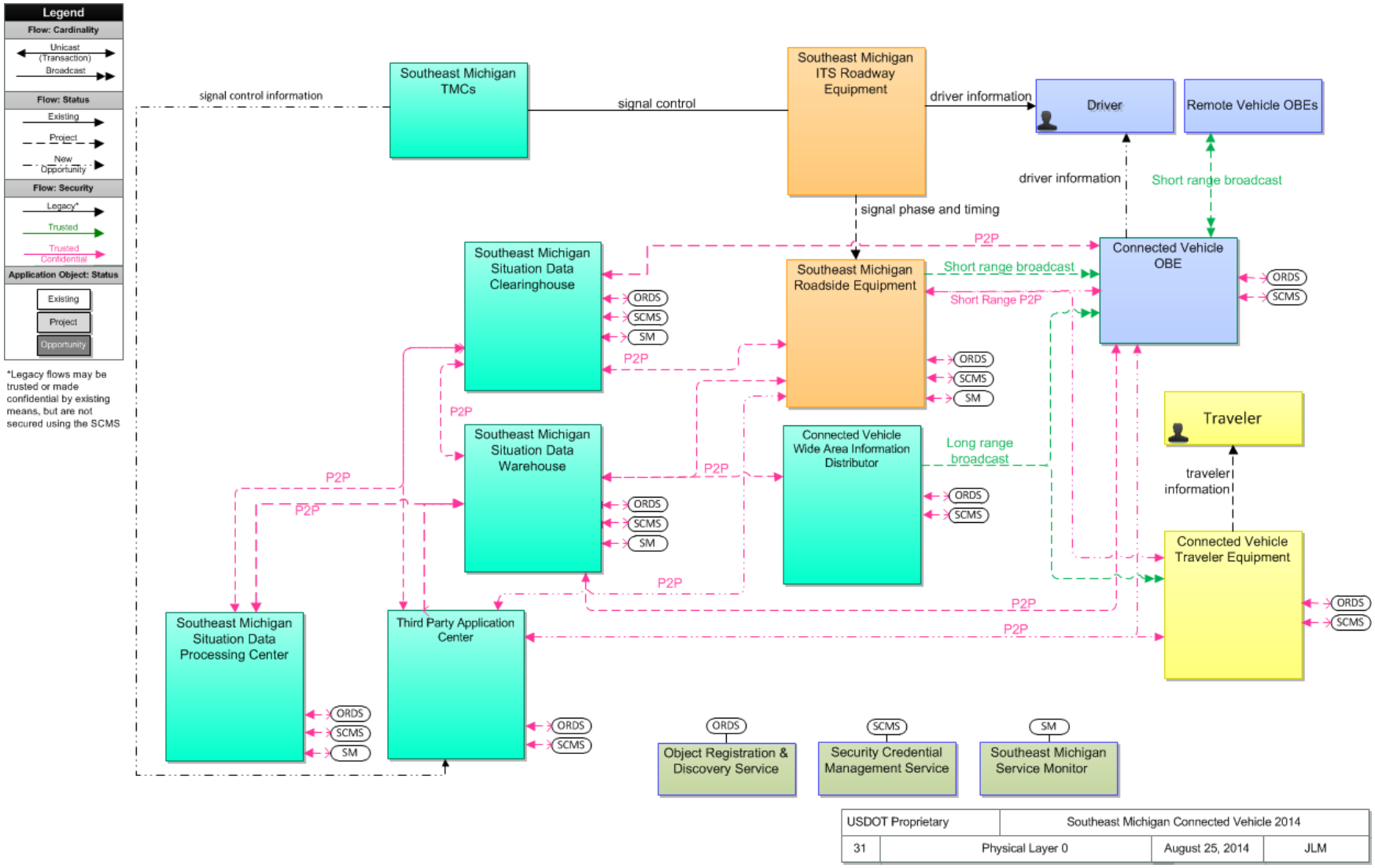

Figure 6 – Physical View – Layer 0

6.2.1.1.2 Physical – Layer 0 – Physical Objects

The table below includes the definitions of all of the physical objects shown in the Layer 0 and Layer 1 Physical View of the 2014 Southeast Michigan Test Bed. Many of these objects are identical or related to CVRIA objects, so the relationship is shown.

Table 4 – Physical View Layer 0 – Physical Objects

Physical Object	Physical Object Definition	CVRIA Relationship
Connected Vehicle OBE	The "Connected Vehicle OBE" represents on-board devices that provide the vehicle-based processing, storage, and communications functions necessary to support connected vehicle operations. It is a custom version of the CVRIA "Vehicle OBE" object. The radio(s) supporting V2V and V2I communications are a key component of the Vehicle OBE. This communication platform for the vehicle is supported by processing and data storage capability in the OBE that provide the basic communications functions and higher level connected vehicle applications. The Connected Vehicle OBE interfaces to other on-board systems through a vehicle bus (e.g., CAN). Represented in CVRIA as the Vehicle Platform, this interface provides access to on-board sensors, monitoring and control systems, and information systems that support connected vehicle applications. In addition to the vehicle bus interface, the Connected Vehicle OBE also provides an interface to a location data source. Finally, a driver interface is included that supports visual, audio, and haptic interaction with the driver. In CVRIA, the Vehicle OBE includes the functions and interfaces that support connected vehicle applications for passenger cars and trucks. Many of these applications (e.g., V2V Safety applications) apply to all vehicle types including personal automobiles, commercial vehicles, emergency vehicles, transit vehicles, and maintenance vehicles. In CVRIA, the Vehicle OBE is used to model the common interfaces and functions that apply to all of these vehicle types.	Custom version of CVRIA "Vehicle OBE"
Connected Vehicle Traveler Equipment	The "Connected Vehicle Traveler Equipment" is a customized version of the CVRIA "Personal Information Device" physical object. Among other things, it provides the capability for travelers and vehicles to receive formatted traveler information from the "Southeast Michigan Situation Data Warehouse" wherever they are. Capabilities include traveler information, trip planning, and route guidance. It provides travelers with the capability to receive route planning from the infrastructure at home, at work, or en route using personal devices that may be linked with connected vehicle on-board equipment.	Custom version of CVRIA "Personal Information Device"
Connected Vehicle Wide Area Information Distributor	"Wide Area Information Distributor" (WAID) represents the Connected Vehicle center based systems and satellite equipment that is used to send messages to equipped vehicles using proprietary FM radio protocols.	None Identified
Driver	The "Driver" represents the person that operates a licensed vehicle on the roadway. Included are operators of private, transit, commercial, and emergency vehicles where the interactions are not particular to the type of vehicle (i.e., interactions supporting vehicle safety applications). Thus, the Driver originates driver requests and receives driver information that reflects the interactions which might be useful to all drivers, regardless of vehicle classification. This object also supports interactions for mobility applications that are primarily intended for drivers of private passenger vehicles. Information and interactions which are unique to drivers of a specific vehicle type (e.g., fleet interactions with transit, commercial, or EV drivers) are covered by separate objects.	CVRIA Object

Physical Object	Physical Object Definition	CVRIA Relationship
Remote Vehicle OBEs	"Remote Vehicle OBEs" represents other connected vehicles that are communicating with the host vehicle. In CVRIA, this object provides a source and destination for information transfers between connected vehicles. The host vehicle on-board equipment, represented by the Vehicle OBE physical object, sends information to, and receives information from the Remove Vehicle OBEs to model all connected vehicle V2V communications in CVRIA.	CVRIA Object
Southeast Michigan ITS Roadway Equipment	"Southeast Michigan Test Bed ITS Roadway Equipment" represents the ITS equipment that is distributed on and along the roadway of the Southeast Michigan Test Bed that monitors and controls traffic and monitors and manages the roadway itself. This physical object represents all of the other ITS field equipment that interfaces with and supports the South Roadside Equipment (RSE). This physical object includes traffic detectors, environmental sensors, traffic signals, highway advisory radios, dynamic message signs, CCTV cameras and video image processing systems, grade crossing warning systems, and ramp metering systems. Lane management systems and barrier systems that control access to transportation infrastructure such as roadways, bridges and tunnels are also included. This object also provides environmental monitoring including sensors that measure road conditions, surface weather, and vehicle emissions. Work zone systems including work zone surveillance, traffic control, driver warning, and work crew safety systems are also included.	Custom version of CVRIA “ITS Roadway Equipment”
Southeast Michigan Roadside Equipment	"Southeast Michigan Test Bed Roadside Equipment" (RSE) represents the Southeast Michigan Test Bed Connected Vehicle roadside devices that are used to send messages to, and receive messages from, nearby vehicles using Dedicated Short Range Communications (DSRC). Communications with adjacent ITS Roadway Equipment (see the separate object) and back office centers that monitor and control the RSE are also supported. This device operates from a fixed position and may be permanently deployed or a portable device that is located temporarily in the vicinity of a traffic incident, road construction, or a special event. It includes a processor, data storage, and communications capabilities that support secure communications with passing vehicles, other roadside equipment, and centers that provide back office support.	Custom version of the CVRIA “Roadside Equipment”
Southeast Michigan Situation Data Clearinghouse	The "Southeast Michigan Situation Data Clearinghouse" is a Transportation Information Center that provides data collection, repacking functions, but only for data that is relevant in the immediate future. Data deposited at the warehouse is immediately delivered (“pushed”) to all registered and available delivery locations.	Currently unique
Southeast Michigan Situation Data Processing Center	The "Southeast Michigan Situation Data Processing Center" monitors and controls traffic and the road network. It represents centers that manage a broad range of transportation facilities including freeway systems, rural and suburban highway systems, and urban and suburban traffic control systems. It communicates with Southeast Michigan ITS Roadway Equipment and Southeast Michigan Roadside Equipment (RSE) to monitor and manage traffic flow and monitor the condition of the roadway, surrounding environmental conditions, and field equipment status. It manages traffic and transportation resources to support allied agencies in responding to, and recovering from, incidents ranging from minor traffic incidents through major disasters.	CVRIA Object

Physical Object	Physical Object Definition	CVRIA Relationship
Southeast Michigan Situation Data Warehouse	The "Southeast Michigan Situation Data Warehouse" is a Transportation Information Center that provides data collection, fusing and repacking functions. Examples of data handled by this Warehouse are speed limits, traffic signal locations and road restrictions. Data deposited at the warehouse is retained for a variable amount of time (based on the time context of the data) and is available for ad-hoc ("pull") queries	Currently unique
Southeast Michigan Traffic Management Center	The "Traffic Management Center" monitors and controls traffic and the road network. It represents centers that manage a broad range of transportation facilities including freeway systems, rural and suburban highway systems, and urban and suburban traffic control systems. It communicates with ITS Roadway Equipment to monitor and manage traffic flow and monitor the condition of the roadway, surrounding environmental conditions, and field equipment status. It manages traffic and transportation resources to support allied agencies in responding to, and recovering from, incidents ranging from minor traffic incidents through major disasters.	CVRIA Object
Support Services: Object Registration and Discovery Service	"Support Services: Object Registration and Discovery Service" represents one or more center-based applications that provide registration and lookup services necessary to allow Test Bed objects to locate other Test Bed objects operating within the SE Michigan Test Bed. These services are not transportation applications or transportation services, but facilitative actions that enable other applications to provide transportation services.	This is a unique SE MI Object.
Support Services: Security Credential Management Service	"Support Services: Security Credential Management Service" represents one or more center-based applications that provide Security credentialing services necessary to other applications and/or devices operating within the SE Michigan Test Bed. These services are not transportation applications or transportation services, but facilitative actions that enable other applications to provide transportation services.	This is a unique SE MI Object.
Support Services: Service Monitor	"Support Services: Service Monitor" represents one or more center-based applications that provide monitoring, management and control services necessary to other applications and/or devices operating within the SE Michigan Test Bed. These services are not transportation applications or transportation services, but facilitative actions that enable other applications to provide transportation services.	This is a unique SE MI Object.
Third Party Application Center	"Third Party Application Center" represents the private infrastructure used to develop, maintain and or host third party applications.	This is a unique SE MI Object.
Traveler	The "Traveler" represents any individual who uses transportation services provided by the Southeast Michigan Test Bed. The interfaces to the traveler provide general pre-trip and en-route information supporting trip planning, personal guidance, and requests for assistance in an emergency that are relevant to all transportation system users. It also represents users of a public transportation system and addresses interfaces these users have within a transit vehicle or at transit facilities such as roadside stops and transit centers.	CVRIA Object

6.2.1.1.3 Physical – Layer 0 – Physical Interconnects

The second table below includes the definitions of all of the physical and application interconnects shown in the Layer 0 and Layer 1 Southeast Michigan Test Bed Architecture (above). Each interconnect description will be accompanied by the source, destination, and its defining

characteristics. At Layer 2, that will be defined later, the information flows also have these same characteristics that are described in the table below.

Table 5 – Physical and Application Interconnect / Information Flow Characteristics

Interconnect / Flow Characteristics	CVRIA Values	Project Values	Characteristic Value Description
Spatial Context	Adjacent	Hyper Local	0-300 meters
	Local	Local	300 meters - 3 kilometers
	Regional	Regional	CVRIA: 3 kilometers – 30 Kilometers Project: Southeast Michigan Project Geographical Area
	National	Regional	CVRIA: Continental U.S. Project: Southeast Michigan Project Geographical Area
Time Context	Now	Hyper Current	Less than 1 Second
	Recent	Current	1 second – 30 minutes
	Historical	Historical	30 minutes – 1 month
	Static	Historical	Greater than 1 month
Acknowledgement	False	False	Information flow receiver acknowledgement is required
	True	True	Information flow receiver acknowledgement is not required
Encryption	True	True	Information flow encryption is required
	False	False	Information flow encryption is not required
Authenticability	True	True	Information flow signature is required
	False	False	Information flow signature is not required
Cardinality	Broadcast	Broadcast	Information is sent to all potential recipients that are within range
	Multicast	Multicast	Information is sent to multiple specific recipients
	Unicast	Unicast	Information is sent to a single specific recipient

Table 6 – Architecture Layer 0 – Physical Interconnects

L0 Information Flow	Definition	Object 1	Object 2	Space Context	Time Context	Acknowledgement	Authenticability	Encryption
Driver Information	Legacy flow. Regulatory, warning, and guidance information provided to the driver while en route to support safe and efficient vehicle operation.	ITS Roadway Equipment	Driver	R	H	No	No	No
		Connected Vehicle OBE	Driver					
Long Range Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog.	Wide Area Information Distributor	Connected Vehicle OBE	R	C	No	Yes	No
			Connected Vehicle Traveler Equipment	R	C	No	Yes	No
Peer to Peer (P2P)	A 'Peer-to-Peer' flow, where a dialog between the entities involved includes some data exchange. A P2P flow requires the initiator to know how to communicate with the recipient.	Any Test Bed physical object	Any other Test Bed physical object	N/A	N/A	Yes	Yes	Yes
Short Range Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog. Typically, this flow type is limited to short-range (1000m or less) communications media.	Connected Vehicle OBE	Southeast Michigan Roadside Equipment	HL	HC	No	Yes	No
		Connected Vehicle OBE	Remote Vehicle OBEs	HL	HC	No	Yes	No
		Southeast Michigan Roadside Equipment	Connected Vehicle Traveler Equipment	HL	HC	No	Yes	No
Short Range P2P	A P2P flow that is limited to short-range (1000m or less) communications media.	Connected Vehicle OBE	Southeast Michigan Roadside Equipment	HL	HC	Yes	Yes	Yes
		Southeast Michigan Roadside Equipment	Connected Vehicle OBE	HL	HC	Yes	Yes	Yes
		Southeast Michigan Roadside Equipment	Connected Vehicle Traveler Equipment	HL	HC	Yes	Yes	Yes

L0 Information Flow	Definition	Object 1	Object 2	Space Context	Time Context	Acknowledgement	Authenticability	Encryption
Support P2P	A 'Peer-to-Peer' flow, where a dialog between the entities involved includes some data exchange. A P2P flow requires the initiator to know how to communicate with the recipient.	Any Test Bed physical object	Any Test Bed Support Service Object	N/A	N/A	Yes	Yes	Yes
Signal Control	Legacy flow. Operational and status data of traffic signal control equipment including operating condition and current indications. Control of traffic signal controllers or field masters including clock synchronization.	Southeast Michigan TMCs	Southeast Michigan ITS Roadway Equipment	N/A	N/A	N/A	N/A	N/A
Signal Control Information	Adaptation of legacy flows containing the operational and status data of traffic signal control equipment including operating condition and current indications.	Southeast Michigan Traffic Management Centers	Third Party Application Center	HL	C	No	Yes	No
Signal Phase and Timing (SPaT)	Data describing the signal phase and timing information for all lanes at a signalized intersection. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable.	Southeast Michigan ITS Roadway Equipment	Southeast Michigan Roadside Equipment	N/A	N/A	N/A	N/A	N/A
Traveler Information	Regulatory, warning, and guidance information provided to the traveler while en route to support safe and efficient travel operation.	Connected Vehicle Traveler Equipment	Traveler	R, L, HL	H, C, HC	No	No	No

6.2.1.1.4 Physical – Layer 1

The following diagram provides a mid-level conceptual architecture for the Southeast Michigan Test Bed. It is also based on the Connected Vehicle Reference Implementation Architecture (CVRIA) described at the CVRIA website.

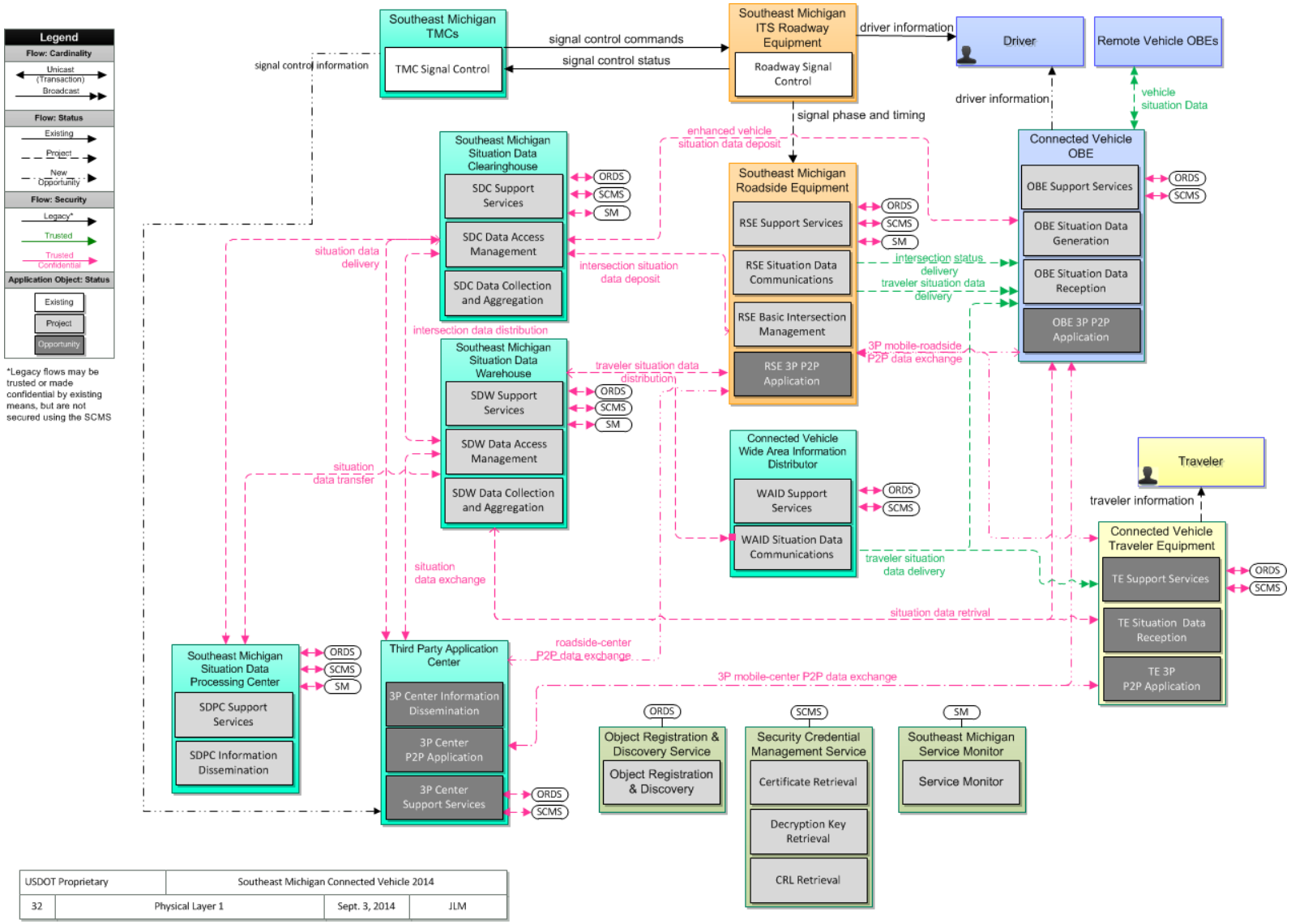

Figure 7 – Physical View – Layer 1

6.2.1.1.5 Physical – Layer 1 – Application Objects

The table below includes the definitions of all of the Layer 1 Application Objects shown in the Layer 1 Physical Architecture (above) which includes the Layer 0 Physical Objects are defined in Table 3 found in Section 6.1.1.2 above. Application objects represent collections of functionality within a physical object to deliver a set of requirements which could be implemented as software or hardware components. Many of these application objects are identical or related to CVRIA objects, so the relationship is shown.

Table 7 – Architecture Layer 1 – Application Objects

Application Object	Definition	CVRIA Relationship
Certificate Retrieval	"Certificate Retrieval" manages the distribution (both initial provisioning and refresh) of digital credentials used by Connected Vehicle objects to authenticate and preserve the integrity of information they exchange.	Under development in CVRIA.
CRL Retrieval	"CRL Retrieval" manages the creation and distribution of credential revocation lists for previously distributed digital credentials used by Connected Vehicle objects to authenticate and preserve the integrity of information they exchange.	Under development in CVRIA.
Decryption Key Retrieval	"Decryption Key Retrieval" manages the distribution of decryption keys for previously retrieved batches of digital credentials used by Connected Vehicle objects to authenticate and preserve the integrity of information they exchange.	Under development in CVRIA.
OBE Situation Data Generation	"OBE Situation Data Generation" creates vehicle situation data messages and shares those messages with other entities in the Vehicle's proximity, and also with the relevant situation data clearinghouse. This functionality is included in the CVRIA object "Vehicle Basic V2V Safety." The CVRIA object also includes safety application functionality (including driver-notification) however. Depending on the types of data included in the enhanced situation data message, this might also include some of the functionality of the "Vehicle Enhanced Data Collection" CVRIA Object.	Subset of the CVRIA object: "Vehicle Basic V2V Safety."
OBE Situation Data Reception	"OBE Situation Data Reception" receives advisories, vehicle signage data, and other driver information and presents this information to the driver using in-vehicle equipment. Information presented may include fixed sign information, traffic control device status (e.g., signal phase and timing data), advisory and detour information, warnings of adverse road and weather conditions, travel times, and other driver information.	CVRIA Object
OBE Support Services	"OBE Support Services" provides for the exchange of information with two (ORDS, SCMS) of the three Southeast Michigan Test Bed Support services.	Currently unique

Application Object	Definition	CVRIA Relationship
OBE Third Party P2P Application	"OBE Third Party P2P Application" is a high-level generic application that provides some service relevant to the vehicle or its occupants. It is topically a bidirectional communications between two entities. It is representative of many other CVRIA Application Objects; and has a hierarchical relationship to many CVRIA Vehicle-based Application Objects.	Currently unique.
Object Registration and Discovery	The "Object Registration and Discovery Service" is the first point of contact for new devices that wish to operate within the SE Michigan Test Bed. This service provides mechanisms for devices to register their existence, contact information (which could be an IP address, for example), what types of information services and data they provide, the mechanisms they use to provide data and information services, and over what time and spatial context those services and data are relevant. Subsequent to registration, devices may query this service to discover data provision and service information about other participants, enabling devices to learn about one another and interoperate in a relatively automated fashion.	Currently unique.
Roadway Signal Control	"Roadway Signal Control" includes the field elements that monitor and control signalized intersections. It includes the traffic signal controllers, signal heads, detectors, and other ancillary equipment that supports traffic signal control. It also includes field masters, and equipment that supports communications with a central monitoring and/or control system, as applicable. The communications link supports upload and download of signal timings and other parameters and reporting of current intersection status. It represents the field equipment used in all levels of traffic signal control from basic actuated systems that operate on fixed timing plans through adaptive systems. It also supports all signalized intersection configurations, including those that accommodate pedestrians.	CVRIA Object
RSE Basic Intersection Management	"RSE Basic Intersection Management" uses short range communications and interfaces to local field ITS devices to support connected vehicle applications at signalized intersections. It communicates with approaching vehicles and ITS infrastructure (e.g., the traffic signal controller) to provide intersection status (signal phase and timing) information both to vehicles and interested centers.	Streamlined version of the CVRIA Object "RSE Intersection Management."
RSE Situation Data Communications	"RSE Situation Data Communications" includes field elements that distribute information to vehicles for in-vehicle display. The information may be provided by a center (e.g., variable information on traffic and road conditions in the vicinity of the field equipment) or it may be determined and output locally (e.g., static sign information, ramp metering signals). This includes the interface to the center or field equipment that controls the information distribution and the short range communications equipment that provides information to passing vehicles.	CVRIA Object
RSE Support Services	"RSE Support Services" provides for the exchange of information with the three Southeast Michigan Test Bed Support services.	Currently unique

Application Object	Definition	CVRIA Relationship
RSE Third Party P2P Application	"RSE Third Party P2P Application" is a high-level generic application that provides some roadside service relevant to nearby vehicles or their occupants. It is topically a bidirectional communications between two entities. It is representative of many other CVRIA Application Objects; and has a hierarchical relationship to many CVRIA Vehicle-based Application Objects.	Currently unique.
SDC Data Access Management	"SDC Data Access Management" provides management and control of data collection and distribution, and the provision of data to other transportation entities. It allows for the creation of data distribution profiles, such as subscriptions and pipes, and the assignment of permissions and rights to provide and access this data.	Currently unique.
SDC Data Collection and Aggregation	"SDC Data Collection and Aggregation" provides for the collection of transportation-related information, the short-term storage and organization of this data, including categorization, aggregation and sampling.	Currently unique.
SDC Support Services	"SDC Support Services' provides for the exchange of information with the three Southeast Michigan Test Bed Support services.	Currently unique
SDPC Information Dissemination	"SDPC Information Dissemination" disseminates traffic and road conditions, closure and detour information, incident information, driver advisories, and other traffic-related data to other centers, the media, and driver information systems. It monitors and controls driver information system field equipment including dynamic message signs and highway advisory radio, managing dissemination of driver information through these systems. It may also register for, and accept deliveries of enhanced vehicle situation data from the Southeast Michigan Situation Data Warehouse.	CVRIA Object
SDPC Support Services	"SPDC Support Services" provides for the exchange of information with the three Southeast Michigan Test Bed Support services.	Currently unique
SDW Data Access Management	"SDW Data Access Management" provides management and control of data collection and distribution, and the provision of data to other transportation entities. It allows for the creation of data distribution profiles, such as subscriptions and pipes, and the assignment of permissions and rights to provide and access this data.	Currently unique.
SDW Data Collection and Aggregation	"SDW Data Collection and Aggregation" provides for the collection of transportation-related information, the short-term storage and organization of this data, including categorization, aggregation and sampling.	Currently unique.
SDW Support Services	"SDW Support Services' provides for the exchange of information with the three Southeast Michigan Test Bed Support services.	Currently unique
Service Monitor	"Service Monitor" provides for the monitoring, management and control of many of the other Southeast Michigan Test Bed objects, both individually and collectively.	Currently unique

Application Object	Definition	CVRIA Relationship
TE Situation Data Reception	"TE Situation Data Reception" receives advisories, vehicle signage data, and other driver information and presents this information to the driver using in-vehicle equipment. Information presented may include fixed sign information, traffic control device status (e.g., signal phase and timing data), advisory and detour information, warnings of adverse road and weather conditions, travel times, and other driver information.	CVRIA Object
TE Support Services	"TE Support Services" provides for the exchange of information with two (ORDS, SCMS) of the three Southeast Michigan Test Bed Support services.	Currently unique
TE Third Party P2P Application	"TE Third Party P2P Application" is a high-level generic application that provides some service relevant to the vehicle or its occupants. It is topically a bidirectional communications between two entities. It is representative of many other CVRIA Application Objects; and has a hierarchical relationship to many CVRIA Vehicle-based Application Objects.	Currently unique.
Third Party Center P2P Application	"Third Party Center P2P Application" is a high-level generic application that provides some center- based service relevant to vehicles or their occupants. It is topically a bidirectional communications between two entities. It is representative of many other CVRIA Application Objects; and has a hierarchical relationship to many CVRIA Vehicle-based Application Objects.	Currently unique.
Third Party Center Support Services	"3P Center Support Services" provides for the exchange of information with the three Southeast Michigan Test Bed Support services.	Currently unique
Third Party Information Dissemination	"Third Party Information Dissemination" disseminates traffic and road conditions, closure and detour information, incident information, driver advisories, and other traffic-related data to other centers, the media, and driver information systems. It monitors and controls driver information system field equipment including dynamic message signs and highway advisory radio, managing dissemination of driver information through these systems. It may also register for, and accept deliveries of enhanced vehicle situation data from the Southeast Michigan Situation Data Warehouse.	Currently unique.
TMC Signal Control	"TMC Signal Control" provides the capability for traffic managers to monitor and manage the traffic flow at signalized intersections. This capability includes analyzing and reducing the collected data from traffic surveillance equipment and developing and implementing control plans for signalized intersections. Control plans may be developed and implemented that coordinate signals at many intersections under the domain of a single traffic management subsystem and are responsive to traffic conditions and adapt to support incidents, preemption and priority requests, pedestrian crossing calls, etc.	CVRIA Object

Application Object	Definition	CVRIA Relationship
WAID Situation Data Communications	"WAID Situation Data Communications" includes field elements that distribute information to vehicles for in-vehicle display. Dynamic information (e.g., variable information on traffic and road conditions in the vicinity of the mobile equipment) and static information (e.g., static sign information) will be supplied by a center. This includes the interface to the center or field equipment that controls the information distribution and the satellite communications equipment that provides information to passing vehicles.	Currently unique
WAID Support Services	"WAID Support Services" provides for the exchange of information with two (ORDS, SCMS) of the three Southeast Michigan Test Bed Support services.	Currently unique

6.2.1.1.6 Physical – Layer 1 – Application Interconnects

The table below identifies and describes the application interconnects presented as arrows connecting the objects in the Layer 1 Physical Architecture illustrated in Figure 7 above. Each description will be accompanied by the source, destination, and defining characteristics. The definitions of the five characteristics (right most columns) of the Application Interconnects are defined in Table 5, above.

Table 8 – Architecture Layer 1 – Application Interconnects

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
Driver Information	Driver	ITS Roadway Equipment	Legacy flow. Regulatory, warning, and guidance information provided to the driver while en route to support safe and efficient vehicle operation.	HL,L,R	HC,C,H	No	No	No
Driver Information	Driver	OBE	Legacy flow. Regulatory, warning, and guidance information provided to the driver while en route to support safe and efficient vehicle operation.	HL,L,R	HC,C,H	No	No	No
Signal Phase and Timing	ITS Roadway Equipment	Roadside Equipment	Current signal phase and timing information for all lanes at a signalized intersection. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane.	N/A	N/A	N/A	N/A	N/A
Signal Control Status	ITS Roadway Equipment	Traffic Management Centers	Legacy flow. Operational and status data of traffic signal control equipment including operating condition and current indications.	N/A	N/A	N/A	N/A	N/A
Signal Control Commands	ITS Roadway Equipment	Traffic Management Centers	Legacy flow. Control of traffic signal controllers or field masters including clock synchronization.	N/A	N/A	N/A	N/A	N/A
Vehicle Situation Data	OBE	Remote Vehicle OBEs	Data describing the operational state at a specified location and specified time of the vehicle reporting the data. This may include vehicle position, speed, heading, acceleration and vehicle path history.	HL	HC	No	Yes	No

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
Traveler Situation Data Delivery	OBE	Roadside Equipment	Static and dynamic advisory information that is relevant to travelers in a small, well-defined area, including signage, information regarding incidents, unusual traffic conditions, transit issues, etc.	L	C	No	Yes	No
Third Party (3P) Mobile-Roadside Peer-to-Peer (P2P) Data Exchange	OBE	Roadside Equipment	Peer-to-peer information flow carrying data relevant to an [undefined] third party application operating on a mobile device and an [undefined] third party application operating on the roadside	N/A	N/A	N/A	Yes	Yes
Intersection Status Delivery	OBE	Roadside Equipment	Immediately relevant data describing the signal phase and timing information for all lanes at a signalized intersection near the source of the flow. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. This data also includes the latest version of the Intersection map containing detailed roadway geometry.	HC	HL	No	Yes	No
Enhanced Vehicle Situation Data Deposit	OBE	Situation Data Clearinghouse	This is Vehicle Situation Data plus additional elements including environmental and emissions-related situation data, relevant over a recent (~10-30 minutes) period and the area over which the vehicle traveled in that time.	L	C	No	Yes	Yes
Traveler Situation Data Retrieval	OBE	Situation Data Warehouse	Static advisory information that is relevant to travelers over the area they have requested. This typically includes, but may not be limited to, electronic versions of metal signs.	R	H	No	Yes	Yes
Third Party (3P) Mobile-Center Peer-to-Peer (P2P) Data Exchange	OBE	Third Party Application Center	Peer-to-peer information flow carrying data relevant to an [undefined] third party application operating on a mobile device and an [undefined] third party application operating within the infrastructure.	N/A	N/A	N/A	Yes	Yes

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
RC Traveler Situation Data Delivery	OBE	Wide Area Information Distributor	Static and dynamic advisory information that is relevant to travelers within roughly 30 minutes over a specific region. This includes signage, information regarding incidents, unusual traffic conditions, transit issues, etc.	R	C	No	Yes	Yes
Intersection Situation Data Deposit	Roadside Equipment	Situation Data Clearinghouse	Bundles of data describing the recent signal phase and timing information for all lanes at a signalized intersection near the source of the flow. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state would persist for each lane. This data also includes the latest version of the Intersection map containing detailed roadway geometry.	HL	C	Yes	Yes	Yes
Traveler Situation Data Distribution	Roadside Equipment	Situation Data Warehouse	Static and dynamic advisory information that is relevant to travelers in a small, well-defined area, including signage, information regarding incidents, unusual traffic conditions, transit issues, etc. This data is retrieved by the RSE from the Situation Data Warehouse	L	C	Yes	Yes	Yes
Third Party (3P) Roadside-Center Peer-to-Peer (P2P) Data Exchange	Roadside Equipment	Third Party Application Center	Peer-to-peer information flow carrying data relevant to “paired” applications operating respectively at the roadside and within the infrastructure.	N/A	N/A	N/A	Yes	Yes
Third Party (3P) Mobile-Roadside Peer-to-Peer (P2P) Data Exchange	Roadside Equipment	Traveler Equipment	Peer-to-peer information flow carrying data relevant to “paired” applications operating respectively at the roadside and on the mobile device.	N/A	N/A	N/A	Yes	Yes
Situation Data Delivery	Situation Data Clearinghouse	Situation Data Processing Center	The delivery of situation data which can include • Bundles of Enhanced Vehicle Situation Data and or Intersection Situation Data which match the TPAC’s subscription criteria and are then delivered by the Clearinghouse. These bundles contain	L,R	C,H	No	Yes	Yes

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
			information from the BSM plus additional elements including environmental and emissions-related situation data. • Bundles of Intersection Situation Data that describes the recent signal phase and timing information for all lanes at a signalized intersection. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. This data also includes the latest version of the Intersection map containing detailed roadway geometry					
Intersection Situation Data Distribution	Situation Data Clearinghouse	Situation Data Warehouse	The delivery of all intersection situation data bundles received by the Situation Data Clearinghouse. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. This data also includes the latest version of the Intersection map containing detailed roadway geometry.	L	C	No	Yes	Yes
Situation Data Delivery	Situation Data Clearinghouse	Third Party Application Center	The delivery of situation data which match the TPAC's subscription criteria and are then delivered by the Clearinghouse • Bundles of Enhanced Vehicle Situation Data and or Intersection Situation Data These bundles contain information from the BSM plus additional elements including environmental and emissions-related situation data. • Bundles of Intersection Situation Data that describes the recent signal phase and timing information for all lanes at a signalized intersection. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. This data also includes the latest	L,R	C,H	No	Yes	Yes

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
			version of the Intersection map containing detailed roadway geometry.					
Situation Data Exchange	Situation Data Processing Center	Situation Data Warehouse	The delivery of situation data which match the SDPC's subscription criteria and are then delivered by the Clearinghouse • Bundles of Enhanced Vehicle Situation Data and or Intersection Situation Data These bundles contain information from the BSM plus additional elements including environmental and emissions-related situation data. • Bundles of Intersection Situation Data that describes the recent signal phase and timing information for all lanes at a signalized intersection. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. This data also includes the latest version of the Intersection map containing detailed roadway geometry. • The SDPC depositing Intersection Situation Data bundles which have been generated or derived from intersections that do not have Roadside Equipment. The bundled data describes the signal phase and timing information for all lanes at a signalized intersection. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. • The SDPC depositing static and/or dynamic advisory information that is relevant to travelers in a small, well-defined area, including signage, information regarding incidents, unusual traffic conditions, transit issues, etc. This would be accompanied by dispatch instructions.	L,R	C,H	Yes	Yes	Yes

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
Situation Data Exchange	Situation Data Warehouse	Third Party Application Center	The exchange of situation data which can include • The TPAC retrieving specified bundles of Enhanced Vehicle Situation Data and or Intersection Situation Data from the Warehouse • The TPAC depositing Intersection Situation Data bundles which have been generated or derived from intersections that do not have Roadside Equipment. The bundled data identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable. • The TPAC depositing static and/or dynamic advisory information that is relevant to travelers in a small, well-defined area, including signage, information regarding incidents, unusual traffic conditions, transit issues, etc. This would be accompanied by dispatch instructions.	L,R	C,H	Yes	Yes	Yes
Situation Data Retrieval	Situation Data Warehouse	Traveler Equipment	The retrieval of Situation Data from the Warehouse • Static advisory information that is relevant to travelers over the area they have requested. This typically includes, but may not be limited to, electronic versions of metal signs. • Bundled data describing the signal phase and timing information for all lanes at a signalized intersection. This flow identifies active lanes and lanes that are being stopped and specifies the length of time that the current state will persist for each lane. It also identifies signal priority and preemption status and pedestrian crossing status information where applicable.	L,R	C,H	No	Yes	Yes
Traveler Situation Data Distribution	Situation Data Warehouse	Wide Area Information Distributor	The retrieval of Traveler Situation Data from the Warehouse for subsequent redistribution. This is static advisory information that is relevant to travelers over the area they have requested. This typically includes, but may not be limited to, electronic versions of metal signs.	R,C	H,C	No	Yes	Yes

L1 Application Interconnect	Object 1	Object 2	Definition	Space Context	Time Context	Acknowledgement	Authenticability	Confidential
P2P Support Data	Support Services: • ORDS • SCMS • SM	All Test Bed Objects	A 'Peer-to-Peer' flow, where a dialog between the entities involved includes some data exchange that is relevant to a support application.	N/A	N/A	Yes	Yes	Yes
Signal Control Information	Third Party Application Center	Traffic Management Centers	Adaptation of legacy flows containing the operational and status data of traffic signal control equipment including operating condition and current indications. This signal control information may be utilized by the TPAC to generate or derive Intersection Situation Data.	HL	C	No	Yes	No
Third Party (3P) Mobile-Center Peer-to-Peer (P2P) Data Exchange	Third Party Application Center	Traveler Equipment	Peer-to-peer information flow carrying data relevant to an [undefined] third party application operating on a mobile device and an [undefined] third party application operating within the infrastructure.	N/A	N/A	N/A	Yes	Yes
Traveler Information	Traveler	Traveler Equipment	Legacy flow representing the distribution of traveler information to end users. Flow control is not explicitly shown, however this flow supports general broadcast, interactive request/response, and publish/subscribe delivery of traveler information.	HL,L,R	HC,C,H	No	No	No
Traveler Situation Data Delivery	Traveler Equipment	Wide Area Information Distributor	The distribution of traveler situation data to the Traveler Equipment. This is static advisory information that is relevant to travelers over the area they have requested. This typically includes, but may not be limited to, electronic versions of metal signs.	R	C	No	Yes	Yes

6.2.1.2 Enterprise View

The Enterprise view describes the relationships between enterprises or stakeholders (organizations, agencies, users, etc.) and the roles those enterprises play within the Southeast Michigan Test Bed as well as their relationships with one another.

6.2.1.2.1 Enterprise – Layer 0

The following top-level drawing reflects the Layer 0 Enterprise view for the Southeast Michigan Test Bed architecture, showing the stakeholders that own or operate the physical objects shown in the last section and their relationships with one other. Tables that follow the diagram describe the objects, roles, and relationships.

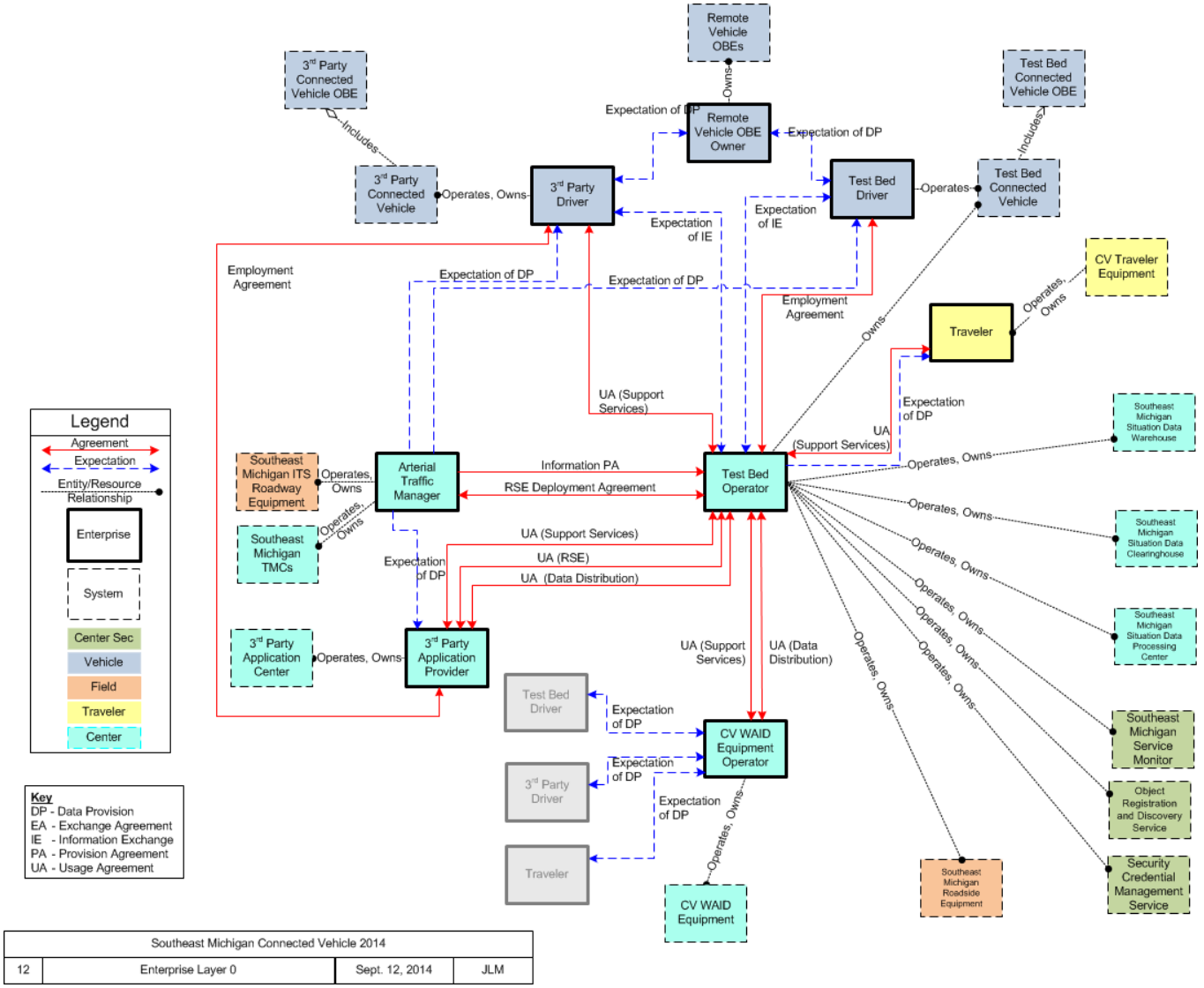

Figure 8 – Enterprise View – Layer 0

6.2.1.2.2 Enterprise – Layer 0 – Objects

The table below describes each of the Enterprise Objects illustrated in the diagram above. The entries in the table below are based on the descriptions listed in the CVRIA Enterprise Objects repository.

Object	Description
Arterial Traffic Manager	An entity responsible for the management of arterial traffic in the Southeast Michigan Test Bed geographic region.
Connected Vehicle Wide Area Information Distribution Operator	The Wide Area Information Distribution Operator provides operational and technical support for Wide Area Information Distribution Operator systems and components. Owns and operates the Wide Area Information Distributor. The Operator facilitates and maintains multiple agreements with other Test Bed Entities.
Remote Vehicle OBE Owner	Remote Vehicle Drivers (or Remote Mobile Device Operators) include the operators of any **other** vehicle or mobile device equipped with the enabling technologies and possessing valid security credentials which allow connected vehicle operations within the Southeast Michigan Test Bed. This is an essentially artificial distinction created to better illustrate the relationship between CV equipped vehicles.
Test Bed Driver	Drivers include the operators of any vehicle or mobile device equipped with the enabling technologies and possessing valid security credentials which allow connected vehicle operations within the Southeast Michigan Test Bed. Non-motorized mobile device operators (pedestrians and cyclists) have different operating characteristics and needs than motorized mobile device operators. Test Bed drivers operate Tess Bed Connected vehicles and have an employment agreement with the Test Bed Operator.
Test Bed Operator	The Test Bed Operator provides operational and technical support for the Southeast Michigan Test Bed systems and components. This includes operational, technical and management of deployed Roadside Equipment (RSE) units, Test Bed vehicles, Data Warehouses and other infrastructure services and platforms, the supporting communications, security and management services and infrastructure. • Owns and operates the Object Registration and Discovery Service. Facilitates and maintains an Expectation of information exchange with other Test Bed Entities. • Owns and operates the Security Credential Management Service. Facilitates and maintains an associated Security Information Exchange Agreement with other Test Bed Entities. • Owns and operates the Southeast Michigan Situation Data Clearinghouse. Facilitates and maintains an Information Provision Agreement with other Test Bed Entities. • Owns and operates the Southeast Michigan Situation Data Warehouse. Facilitates and maintains an Information Provision Agreement with other Test Bed Entities.
Third Party Application Provider	Third Party Application Providers are specified more by role than by function. They are responsible for the development of the third party applications on either mobile, field or center-based System Elements. This includes initial creation, enhancements, operational support and maintenance. For those System Elements that they host, they are also responsible for the establishment, maintenance and secure operations of the supporting computing infrastructure and facilities.

Object	Description
Third Party Driver	Third Party Drivers include the operators of any vehicle or mobile device equipped with the enabling technologies and possessing valid security credentials which allow connected vehicle operations within the Southeast Michigan Test Bed. Non-motorized mobile device operators (pedestrians and cyclists) have different operating characteristics and needs than motorized mobile device operators.
Traveler	The "Traveler" represents any individual (other than a “Test Bed Driver” or “Third Party Driver”) who uses transportation services. The interfaces to the traveler provide general pre-trip and en-route information supporting trip planning, personal guidance, and requests for assistance in an emergency that are relevant to all transportation system users. It also represents users of a public transportation system and addresses interfaces these users have within a transit vehicle or at transit facilities such as roadside stops and transit centers. Travelers include the operators of any mobile device equipped with the enabling technologies and possessing valid security credentials which allow connected vehicle operations within the Southeast Michigan Test Bed.

6.2.1.2.3 Enterprise – Layer 0 – Roles

The table below lists and defines the roles between the Enterprise Objects specified in the previous section. They are based on the CVRIA Enterprise Roles defined in the CVRIA website.

Role Name	Description
Operates	An Enterprise controls the functionality and state of the target object.
Owns	An Enterprise has financial ownership and control over the target object.

6.2.1.2.4 Enterprise – Layer 0 – Relationships

The table below lists and defines the roles between the CVRIA Enterprise Relationships specified in the Section 6.1.1.5 above. They are based on the CVRIA Enterprise Relationships defined in the CVRIA website.

Object 1	Object 2	Relationship Type	Description
Arterial Traffic Manager	Test Bed Driver	Expectation of Data Provision	An expectation by the Test Bed Driver that the Arterial Traffic Manager will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Test Bed Driver in the context of the Test Bed Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Arterial Traffic Manager	Test Bed Operator	Information Provision Agreement	An agreement where the Arterial Traffic Manager will provide the Test Bed Operator the agreed upon information whenever such information is likely relevant to the recipient. Typically this information will consist of signal, phase and timing information from traffic signal controllers and it includes a clear expectation of the content, timeliness, quality, precision and similar qualities of the information.
Arterial Traffic Manager	Test Bed Operator	RSE Deployment Agreement	Agreement to install, configure and make operational roadside equipment, between Test Bed Operator (which owns and operates the RSEs) and the Arterial Traffic Manager (which controls access to the roadside). It may define locations, expectation of power provision, backhaul responsibility and installation restrictions.
Arterial Traffic Manager	Third Party Application Provider	Expectation of Data Provision	An expectation by the Third Party Application Provider that the Arterial Traffic Manager will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Third Party Application Provider in the context of the Third Party Application Provider's applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Arterial Traffic Manager	Third Party Driver	Expectation of Data Provision	An expectation by the Third Party Driver that the Arterial Traffic Manager will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Third Party Driver in the context of the Third Party Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Remote Vehicle OBE Owner	Test Bed Driver	Expectation of Data Provision	An expectation by the Test Bed Driver that the Remote Vehicle OBE Owner will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Test Bed Driver in the context of the Test Bed Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Remote Vehicle OBE Owner	Third Party Driver	Expectation of Data Provision	An expectation by the Third Party Driver that the Remote Vehicle OBE Owner will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Third Party Driver in the context of the Third Party Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.

Object 1	Object 2	Relationship Type	Description
Test Bed Driver	Test Bed Operator	Employment Agreement	An agreement between a Test Bed Driver and the Test Bed Operator, whereupon the Test Bed Driver agrees to provide labor to the Test Bed Operator, which in turn will compensate the Test Bed Driver. It stipulates the level of compensation, working conditions, necessary equipment and training and expectations of employee performance
Test Bed Driver	Test Bed Operator	Expectation of Information Exchange	An expectation, held by both the Test Bed Operator and the Test Bed Driver, where each party believes and anticipates that the reciprocal party will provide it information whenever such information is likely relevant to the recipient.
Test Bed Driver	Wide Area Information Distribution Operator	Expectation of Data Provision	An expectation by the Test Bed Driver that the Wide Area Information Distribution Operator will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Test Bed Driver in the context of the Test Bed Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Test Bed Operator	Third Party Driver	Expectation of Information Exchange	An expectation, held by both the Test Bed Operator and the Third Party Driver, where each party believes and anticipates that the reciprocal party will provide it information whenever such information is likely relevant to the recipient.
Test Bed Operator	Third Party Driver	Usage Agreement (Support Services)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Object Registration and Discovery Service and the Security Credential Management Service objects gives the Third Party Driver the necessary tools and permission to interact with these Test Bed objects.
Test Bed Operator	Third Party Application Provider	Usage Agreement (Support Services)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Object Registration and Discovery Service and the Security Credential Management Service objects gives the Third Party Application Provider the necessary tools and permission to interact with these Test Bed objects.
Test Bed Operator	Third Party Application Provider	Usage Agreement (Data Distribution)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Text Bed Situation Data Warehouse and Situation Data Clearinghouse objects gives the Third Party Application Provider the necessary tools and permission to interact with these Test Bed objects.
Test Bed Operator	Third Party Application Provider	Usage Agreement (RSE)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Text Bed RSE objects gives the Third Party Application Provider the necessary tools and permission to operate their application object(s) on one or more Southeast Michigan Test Bed RSEs.
Test Bed Operator	Traveler	Expectation of Data Provision	An expectation by the Traveler that the Test Bed Operator will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Traveler in the context of the Traveler's mobile applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Test Bed Operator	Traveler	Usage Agreement (Support Services)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Object Registration and Discovery Service and the Security Credential Management Service objects gives the Traveler the necessary tools and permission to interact with these Test Bed objects.

Object 1	Object 2	Relationship Type	Description
Test Bed Operator	Wide Area Information Distribution Operator	Usage Agreement (Support Services)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Object Registration and Discovery Service and the Security Credential Management Service objects gives the Wide Area Information Distribution Operator the necessary tools and permission to interact with these Test Bed objects.
Test Bed Operator	Wide Area Information Distribution Operator	Usage Agreement (Data Distribution)	An agreement in which the Southeast Michigan Test Bed Operator that operates and controls the Southeast Michigan Text Bed Situation Data Warehouse and Situation Data Clearinghouse objects gives the Wide Area Information Distribution Operator the necessary tools and permission to interact with these Test Bed objects.
Third (3rd) Party Application Provider	Third (3rd) Party Driver	Employment Agreement	An agreement between a Third (3rd) Party Driver and the Third (3rd) Party Application Provider, whereupon the Third (3rd) Party Driver agrees to provide labor to the Third (3rd) Party Application Provider, which in turn compensates the Third (3rd) Party Driver. Stipulates level of compensation, working conditions, necessary equipment and training and expectations of employee performance
Third (3rd) Party Driver	Wide Area Information Distribution Operator	Expectation of Data Provision	An expectation by the Third Party Driver that the Wide Area Information Distribution Operator will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Third Party Driver in the context of the Third Party Driver's vehicle applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.
Traveler	Wide Area Information Distribution Operator	Expectation of Data Provision	An expectation by the Traveler that the Wide Area Information Distribution Operator will provide data on a regular and recurring basis, and that that provisioned data will be useful to the Traveler in the context of the Traveler's mobile applications, and includes some expectation of the content, timeliness, quality, precision and similar qualities of the data.

6.3 Object Requirements

This following section describes the physical objects and selected application objects identified in Figure 3 depicted in Section 6.2.2 above. Only the non-legacy (light or dark grey colored boxes) application objects in the architecture diagrams presented above will be described. Specifically, the description will be in the form of lists of high-level requirements for each application object. Traditionally, requirements are generated from the user needs defined in the Concept of Operations, and are specified in a separate document. However, due to the time constraints of the 2014 Southeast Michigan Test Bed project, this process was compressed and a single combined document was developed.

6.3.1 Connected Vehicle Onboard Equipment (OBE)

The Connected Vehicle Onboard Equipment (OBE) will fall into either of the following two categories

1. OBEs installed in Southeast Michigan Test Bed owned and operated vehicles. These OBEs will only have the first three applications objects described below.
2. OBEs installed in Third Party owned and operated vehicles. These OBEs will have all four application objects described below.

6.3.1.1 OBE Support Services

OBE Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.

OBE Support Services – Security Credential Services

This assumes that the OBE Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS or the WAID, the latest CRL. Ensure that any expired CRLs are discarded.

6.3.1.2 OBE Situation Data Reception

The OBE Situation Data Reception application object will periodically query the Southeast Michigan Situation Data Warehouse for Situation Data Bundles of interest. Relevance, and therefore the query

itself, will be determined by the OBE Situation Data Reception application object based on the vehicle's current geographic position, etc. These bundles will be deconstructed as needed and processed accordingly for potential presentation (audio, visual, haptic, etc.) to the Driver.

OBE Situation Data Reception – Query Generation

1. If needed, discover the address of the Situation Data Warehouse.
2. Reach out to the Situation Data Warehouse to confirm its address and subsequently establish trust, effectively registering as a "data consumer". Store any authorizations or information received.
3. Construct and transmit to the Situation Data Warehouse, a properly structured and formatted query with the following elements:
    a. Type of data requested
    b. Geographic boundary of data requested
4. As needed, or after configurable intervals, regenerate (using updated element values) and retransmit an updated query.

OBE Situation Data Reception – Query Response Processing

1. Validate the structure and contents of the bundles delivered in the in the query response from the Situation Data Warehouse
2. Process each bundle into an internal data store, ensuring that there are no duplicate messages.

OBE Situation Data Reception –Situation Data Message Processing

1. Based on vehicle kinematics and Driver preferences, determine which Intersection Situation Messages or Traveler Situation Messages currently in the internal data store are relevant and urgent.
2. Process each exigent message accordingly. The algorithms and procedures for this are outside the scope of this specification.
3. Monitor and manage the internal data store, discarding expired messages or messages that are irrelevant.

6.3.1.3 OBE Situation Data Generation

The OBE Situation Data Generator application object will generate Enhanced Vehicle Situation Messages which will be bundled and deposited with the Situation Data Clearinghouse. Connectivity between the OBE Situation Data Generator and the Situation Data Clearinghouse will be IP-based and may use any communications medium that supports IP connectivity. The OBE Situation Data Generator will perform the following operational steps:

OBE Situation Data Generator – Create Bundles

Although BSMs may not be transmitted at a 10 Hz rate if certain congestion mitigation algorithms are in place. It is assumed that Enhanced Vehicle Situation Data Message will be created at a 10 Hz rate.

1. Do nothing until the configurable "Trip Start Obfuscation Delay" time threshold has passed.
2. Generate Enhanced Vehicle Situation Data Messages at the configured rate.

3. After generating a configurable number (default is 8) of Enhanced Vehicle Situation Messages, package these Enhanced Vehicle Situation Messages into an Enhanced Vehicle Situation Message Bundle.
4. Correctly populate the data fields in the Enhanced Vehicle Situation Message Bundle Header Segment.
5. Store the Enhanced Vehicle Situation Message Bundle
6. Discard any bundle with a Bundle Generation Time value indicating that it is older than the time interval defined by the "Max Bundle Lifespan" (default to 30 minutes).

OBE Situation Data Generator – Deposit Bundles

1. When appropriate (based on volume of generated bundles, connection status to the Situation Data Clearinghouse, etc.) prepare to deposit bundles.
2. Select all generated bundles with Bundle Generation Time values indicating that they were generated before time interval defined by the "Trip End Obfuscation Delay" threshold.
3. Attempt to deposit, using LIFO ordering, all secured Enhanced Vehicle Situation Data Message Bundle with the Situation Data Clearinghouse using the selected communications path.
4. Discard each Enhanced Vehicle Situation Message Bundle and associated Enhanced Vehicle Situation Messages after the deposit attempt.

6.3.1.4 OBE 3P P2P Application

It is anticipated and strongly encouraged that these Third Party applications will be developed using the "Peer to Peer" Data Exchange Pattern described in Section 6.2.1 above. Their specific usage and functionality is outside the scope of this document.

6.3.2 Connected Vehicle Traveler Equipment

These are third party portable devices which when operated within a third party vehicle provide a subset of the functionality of an OBE. These "mobile device" Traveler Equipment Objects will have three application objects described below.

6.3.2.1 TE Support Services

TE Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.

TE Support Services – Security Credential Services

This assumes that the TE Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS or the WAID, the latest CRL. Ensure that any expired CRLs are discarded.

6.3.2.2 TE Situation Data Reception

The TE Situation Data Reception application object will periodically query the Southeast Michigan Situation Data Warehouse for all Traveler Situation Data Bundles in their geographic region. Relevance, and therefore the query itself, will be determined by the TE Traveler Data Reception application object based on the vehicle's current geographic position, etc. These bundles will be deconstructed as needed and processed accordingly for potential presentation (audio, visual, haptic, etc.) to the Traveler.

TE Situation Data Reception – Query Generation

1. If needed, discover the address of the Situation Data Warehouse.
2. Reach out to the Situation Data Warehouse to confirm its address and subsequently establish trust, effectively registering as a "data consumer". Store any authorizations or information received.
3. Construct and transmit to the Situation Data Warehouse, a properly structured and formatted query with the following elements:
    a. Type of data requested
    b. Geographic boundary of data requested
4. As needed, or after configurable intervals, regenerate (using updated element values) and retransmit an updated query.

TE Situation Data Reception – Query Response Processing

1. Validate the structure and contents of the bundles delivered in the in the query response from the Southeast Michigan Warehouse
2. Process each bundle into an internal data store, ensuring that there are no duplicate messages.

TE Situation Data Reception – Situation Data Message Processing

1. Based on vehicle kinematics and Driver preferences, determine which Intersection Situation Messages or Traveler Situation Messages currently in the internal data store are relevant and urgent.
2. Process each exigent message accordingly. The algorithms and procedures for this are outside the scope of this specification.
3. Monitor and manage the internal data store, discarding expired messages or messages that are irrelevant.

6.3.2.3 TE 3P P2P Application

It is anticipated and strongly encouraged that these Third Party applications will be developed using the "Peer to Peer" Data Exchange Pattern described in Section 6.2.1 above. Their specific usage and functionality is outside the scope of this document.

6.3.3 Object Registration & Discovery Service (ORDS)

Many of the services offered by roadside or center-based service providers operating within the Southeast Michigan Test Bed geographic boundary will require an advertisement of their existence and cyber location to potential users; which consist primarily of Test Bed vehicles, but could include roadside or other center based services. This support service will facilitate the registration of services by the respective service providers and the subsequent query-based discovery of these registered services. Please note that center based services operating outside of Southeast Michigan Test Bed geographic boundary will not be allowed to register.

6.3.4 Security Credential Management Services (SCMS)

Security Credential Management Service (SCMS), one of the support services of the Southeast Michigan Test Bed has been developed using on the Security Credential Management System Design[1] for the Safety Pilot Model Deployment (SPMD) without substantial changes. Newly added information flows are for transactions in the trust establishment and non-repudiation stages. It is assumed that the Test Bed object that is interested in requesting SCMS service has completed bootstrapping and possessed required key pairs and certificates for the transactions described below.

6.3.4.1 Credential Retrieval

The SCMS will support the secure provisioning of a given Southeast Michigan Test Bed object's certificates in response to an authorized request from that Object. The retrieved credentials will be used by the receiving Test Bed Object to enable secure communications with other Test Bed Objects and to enable it to conduct authorized transactions and operations with other Test Bed Objects. The batches of encrypted certificates will be infrequently retrieved and stored locally by the Test Bed Object, to be accessed as needed in a specific order.

6.3.4.2 Decryption Key Retrieval

The SCMS will support the secure provisioning of a given Southeast Michigan Test Bed object's Decryption Key in response to an authorized request from that Object. The retrieved Decryption Key will be used by the receiving Test Bed Object to decrypt the "next valid" batch within the set of previously retrieved Security Credential batches.

6.3.4.3 CRL Retrieval

The Security Credential Management Service (SCMS) will support the secure transmission of the indicated Certificate Revocation List (CRL) to a given a Southeast Michigan Test Bed object's Decryption Key in response to an authorized request from that Object. The CRL will be used by the receiving Test

[1] *Security Credential Management System Design, Draft Report, USDOT, April 13, 2013*

Bed object to identify revoked credentials thus allowing the Object to take appropriate actions, such as misbehavior reporting.

6.3.5 Southeast Michigan Roadside Equipment (RSE)

The Southeast Michigan Roadside Equipment (RSE) is a field-based object built and operated by the Southeast Michigan Test Bed. The RSEs are Connected Vehicle enabled devices that are used to send messages to, and receive messages from, nearby CV-equipped vehicles using the Dedicated Short Range Communications (DSRC) 5.9GHz spectrum and IEEE 1609 based communications protocols. It is possible that an RSE could have support additional communications mechanism and protocols.

The four main functions of the Southeast Michigan Roadside Equipment are:

1) **RSE Situation Data Communications** which facilitates the RSE interacting with the Situation Data Warehouse to request and accept Traveler Situation Data Messages for dispatch to passing Connected Vehicle OBEs.
2) **RSE Basic Intersection Management** which facilitates the RSE receiving Signal Phase and Timing (SPaT) information from locally connected ITS Roadway equipment (traffic signal controller) and encapsulating into Intersection Situation Data (ISD) messages for dispatch to passing Connected Vehicle OBEs. These ISD messages are collected and transmitted in bundles to the Situation Data Warehouse for subsequent delivery to requesting Connected Vehicle OBEs.
3) **RSE Support Services** to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; discover the location and credentialing information of other Test Bed Objects; and to obtain and manage security credentials with the SCMS.
4) **RSE 2P P2P Application** provided by an authorized Third Party Application Provider, this application will support private "Peer-to-Peer" communications with other partnered applications located on mobile and/or center based platforms to provide a Connected Vehicle service.

The RSE will interact with the following Test Bed objects

1. **Connected Vehicle OBEs** to broadcast Traveler Situation Data messages, Intersection Situation Data messages.
2. **Connected Vehicle TEs** to broadcast Traveler Situation Data messages.
3. **Situation Data Clearinghouse** to deposit Intersection Situation Data Message bundles for eventual distribution to CV equipped vehicles.
4. **Situation Data Warehouse** to retrieve Traveler Situation Data Messages for eventual distribution to CV equipped vehicles.
5. **ITS Roadway Equipment** to receive and/or exchange information such as signal, phase and timing information.
6. **Support Services** to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; and to obtain and manage security credentials with the SCMS.

6.3.5.1 RSE Support Services

RSE Support Services – Object Registration

1. Reach out to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to register its current cyber location and active public credentialing information.
2. Update its registration information with the Object Registration and Discovery Service upon any change in cyber location information.
3. Update its registration information with the Object Registration and Discovery Service upon any change in public credentialing information.

RSE Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.
5. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, reach out to the Object Registration and Discovery Service to "rediscover" the object and obtain its updated information.

RSE Support Services – Security Credential Services

This assumes that the RSE Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS or the WAID, the latest CRL. Ensure that any expired CRLs are discarded.

RSE Support Services – Service Monitoring

The Service Monitor Object has not been defined yet. This section will be added in a future version of this specification.

6.3.5.2 RSE Basic Intersection Management

1) Place the latest Geometric Intersection Definition (GID) or "MAP" message along with its respective dispatch instructions into the managed broadcast playlist, replacing any previously entered MAP message.

2) Access the Southeast Michigan ITS Roadway Equipment to receive signal, phase and timing information.
3) Using the received signal, phase and timing information, periodically generate a "snapshot" ISD message in a format suitable for broadcast.
4) Buffer a copy of each snapshot ISD message until subsequent bundling for transfer to the Southeast Michigan Situation Data Clearinghouse.
5) Place the latest "snapshot" ISD message, along with the currently configured standard (for SPaT) dispatch instructions, into the managed broadcast playlist, replacing any previously entered "snapshot" ISD message.
6) Bundle the latest MAP message and an optimal (for efficient transmission) number of stored ISD messages together into a single ISD Bundle.
7) Access the Situation Data Clearinghouse to "deposit" the ISD Bundle.
8) Discard the "deposited" bundle and any buffered message that it contained.

6.3.5.3 RSE Situation Data Communications

1) Using the configured geographic area of interest for the RSE, request and accept Traveler Situation Data Bundles from the Situation Data Warehouse,
2) Process the retrieved bundles of Traveler Situation Data Messages ensuring that each TSD message is entered along with its respective dispatch instructions into a managed TSD message list.
3) Access the managed TSD message list as required ensuring that each "active" TSD Message is inserted into the managed broadcast playlist, based on the associated dispatch instructions.
4) Process the managed TSD message list playlist to remove (archiving or deleting as necessary) any expired TSD messages.
5) Broadcast all messages in the managed broadcast playlist according to their respective dispatch instructions.
6) Maintain the managed broadcast playlist.

6.3.5.4 RSE 3P P2P Application

It is anticipated and strongly encouraged that these Third Party applications will be developed using the "Peer to Peer" Data Exchange Pattern described in Section 6.2.1 above. Their specific usage and functionality is outside the scope of this document.

6.3.6 Southeast Michigan Service Monitor

The Southeast Michigan Service Monitor Object has not been defined yet. This section will be added in a future version of this specification

6.3.6.1 Service Monitor

The Service Monitor application object has not been defined yet. This section will be added in a future version of this specification

6.3.7 Southeast Michigan Situation Data Clearinghouse (SDC)

The Situation Data Clearinghouse is a Center-based object built and operated by the Southeast Michigan Test Bed Operator. It will provide warehouse functions enabling the collection and distribution of two inventory items: bundles of enhanced vehicle situation data and bundles of intersection situation data. As with any warehouse, the suppliers and consumers of these bundles will not need to have an established agreement with each other, nor will they need to have "a priori" knowledge of each other.

Again, as with many warehouse based distribution systems, each Situation Data Clearinghouse will have an exclusive (non-overlapping) geographic region for which it will accept or provide goods (e.g. Enhanced Vehicle Situation Data Bundles). These geographic regions will be defined and bounded in units of degrees. Given that, the initial Situation Data Clearinghouse will be the located in the Southeast Michigan 2014 Test Bed and will have the geographic region shown above (See 4.2.1.1). As more providers come on line, the service area will be divided into 10 millidegree rectangles to support the greater granularity needed for the increased data volumes. As other Affiliated Test Beds come online, additional Situation Data Clearinghouses could be created with respective defined geographic regions.

There are two inventory item processed by the Situation Data Clearinghouse:

1. The Enhanced Vehicle Situation Data Bundle. Its data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735. Enhanced Vehicle Situation Data Bundles will be tagged/encoded according to the rules defined in SAE J2735 (XML or ASN.1)
2. The Intersection Situation Data Bundle. Its data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735.

The Situation Data Clearinghouse will interact with the following Test Bed objects

1. Connected Vehicle Onboard Equipment to accept deposits of Enhanced Vehicle Situation Data Bundles.
2. Southeast Michigan Roadside Equipment to accept inbound deposits of Intersection Situation Data Bundles
3. Southeast Michigan Situation Data Processing Center to deliver Enhanced Vehicle Situation Data bundles or Intersection Situation Data bundles based on delivery instructions provided by the Southeast Michigan Situation Data Processing Center.
4. Southeast Michigan Situation Data Warehouse to deliver a copy of all deposited Enhanced Vehicle Situation Data Bundles
5. Southeast Michigan Support Services to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; and to obtain and manage security credentials with the SCMS.
6. Third Party Application Center to deliver Enhanced Vehicle Situation Data bundles or Intersection Situation Data bundles based on delivery instructions provided by the Third Party Application Center.

6.3.7.1 SDC Support Services

SDC Support Services – Object Registration

1. Reach out to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to register its current cyber location and active public credentialing information.
2. Update its registration information with the Object Registration and Discovery Service upon any change in cyber location information.
3. Update its registration information with the Object Registration and Discovery Service upon any change in public credentialing information.

SDC Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.
5. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, reach out to the Object Registration and Discovery Service to "rediscover" the object and obtain its updated information.

SDC Support Services – Security Credential Services

This assumes that the SDC Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS or the WAID, the latest CRL. Ensure that any expired CRLs are discarded.

SDC Support Services – Service Monitoring

The Service Monitor Object has not been defined yet. This section will be added in a future version of this specification.

6.3.7.2 SDC Data Access Management

Data Access Management is handled separately for data providers and data consumers. The different exchanges of information between Data Producers/Consumers and the Situation Data Clearinghouse

will be derived from the Peer-to-Peer Data Exchange Message Sequence pattern described in Section 5.3.2 above and each will, in turn, be described in specific detail in Section 6.4 below.

6.3.7.3 SDC Data Collection and Aggregation

The fundamental data processing paradigm of the Situation Data Clearinghouse can best be characterized as "publish and subscribe". The characteristics (e.g. generation location) of any data that is deposited will be immediately matched against the characteristics of interest for each registered consumer to determine which user(s) are interested in the deposited data. A single attempt will be made to send the data to each "matched" consumer. After all matches are processed, the data is discarded.

The Situation Data Clearinghouse will handle data collection and aggregation from producers (Deposits) and consumers (deliveries) as described below.

Situation Data Clearinghouse - Deposit Processing

The Situation Data Clearinghouse will perform the following functions for each deposited situation data bundle.

1. Authenticate, as necessary, the credential of the Depositor of the inbound bundle
2. Validate the authenticated bundle structure and format.
3. Store the validated bundle in internal data stores for subsequent retrieval in support outbound (delivery) data collection and aggregation functions.
4. The Situation Data Clearinghouse will generate and log required (metadata) attributes of incoming deposit bundles.
5. All logging function parameters will be configurable.
6. All log storage will be bounded by configurable size thresholds and/or configurable lifespans.

Situation Data Clearinghouse - Delivery Establishment

The Situation Data Clearinghouse will perform the following functions to register a given consumer and prepare for subsequent delivery of bundles to that registered consumer.

1. The Situation Data Clearinghouse will authenticate the delivery request
2. The Situation Data Clearinghouse will validate the supplied delivery criteria (e.g. bundle type, location boundary, network address).
3. The Situation Data Clearinghouse will log and discard any unauthenticated or invalid delivery request.
4. The Situation Data Clearinghouse will store a record of the identity and associated criteria of the validated delivery request.

Situation Data Clearinghouse - Delivery Processing

The Situation Data Clearinghouse will perform the following functions to process bundles for delivery to registered consumers.

1. The Situation Data Clearinghouse will access the delivery data store to match the characteristics of each constituent delivery request with the characteristics of the deposited bundles.

   a. Only bundles will the matching Bundle Type will be aggregated
   b. Only bundles with a Bundle Generation Location that fall within the Geographic Boundary of Request will be aggregated.
   c. Only bundles with a Bundle Generation Time that fall within the Time Boundary of the delivery criteria will be aggregated.
2. The Situation Data Clearinghouse will aggregate the collected bundles into a "bundle of bundles" in preparation for delivery to the registered consumer.
3. The Situation Data Clearinghouse will purge data bundles once all matching records in the delivery data store have been processed.
4. The Situation Data Clearinghouse will log attributes (metadata) of outgoing delivery bundles, and maintain transaction summaries and statistics.
5. All logging function parameters will be configurable.
6. All log storage will be bounded by configurable size thresholds and/or configurable lifespans.

6.3.8 Southeast Michigan Situation Data Processing Center

The Southeast Michigan Situation Data Processing Center is a center based object built and operated by the Southeast Michigan Test Bed. It is intended to provide operational support for the management and control of the Southeast Michigan Test Bed, as well as provide operational support for third party research and development activities. The SDPC will interact with the following Test Bed objects

- **Situation Data Clearinghouse** to place subscriptions and subsequently accept deliveries of Enhanced Vehicle Situation Data Bundles or Intersection Situation Data Bundles.
- **Situation Data Warehouse** to generate and deposit Traveler Situation Data Messages for eventual distribution to CV equipped vehicles; and retrieve Enhanced Vehicle Situation Data Bundles or Intersection Situation Data Bundles of interest.
- **Support Services** to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; discover the location and credentialing information of other Test Bed Objects; and to obtain and manage security credentials with the SCMS.

6.3.8.1 SPDC Support Services

SDPC Support Services – Object Registration

1. Reach out to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to register its current cyber location and active public credentialing information.
2. Update its registration information with the Object Registration and Discovery Service upon any change in cyber location information.
3. Update its registration information with the Object Registration and Discovery Service upon any change in public credentialing information.

SDPC Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.
5. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, reach out to the Object Registration and Discovery Service to "rediscover" the object and obtain its updated information.

SDPC Support Services – Security Credential Services

This assumes that the SDPC Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS, the latest CRL. Ensure that any expired CRLs are discarded.

SDPC Support Services – Service Monitoring

The Service Monitor Object has not been defined yet. This section will be added in a future version of this specification.

6.3.8.2 SPDC Information Dissemination

The SDPC Information Dissemination application object facilitates the SDPC interacting with the Situation Data Clearinghouse and Situation Data Warehouse.

Situation Data Processing Center – Subscription Management

The Situation Data Processing Center will perform the following functions for subscriptions that will be sent to the Situation Data Clearinghouse.

1. Generate subscription messages with valid structure, content and format for Enhanced Vehicle Situation Data subscriptions; and subsequently initiate and manage the Enhanced Vehicle Situation Data Delivery information flow the Situation Data Clearinghouse.
2. Generate subscription messages with valid structure, content and format for Intersection Situation Data subscriptions; and subsequently initiate and manage the Intersection Situation Data Delivery information flow the Situation Data Clearinghouse.
3. Track and manage all active subscriptions, using refreshed security credentials
4. Generate and log required (metadata) attributes of each subscription.

Situation Data Processing Center – Subscribed Content Processing

The Situation Data Processing Center will perform the following functions for each "subscribed" situation data bundle that it receives.

1. Authenticate, as necessary, the credential of the Situation Data Clearinghouse
2. Validate the authenticated bundle structure and format.
3. Validate the structure and format of messages within the bundle
4. Store the validated bundle and/or messages in internal data stores for subsequent access.
5. Generate and log required (metadata) attributes of incoming deposit bundles.

Situation Data Processing Center – Query Management

The Situation Data Processing Center will perform the following functions for queries that will be sent to the Situation Data Warehouse/

1. Generate queries with valid structure, content and format for Enhanced Vehicle Situation Data Bundles; and subsequently initiate and manage the Enhanced Vehicle Situation Data Delivery information flow to the Situation Data Warehouse.
2. Generate queries with valid structure, content and format for Intersection Situation Data bundles; and subsequently initiate and manage the Intersection Situation Data Delivery information flow to the Situation Data Warehouse.
3. Track and manage all active subscriptions, using refreshed security credentials
4. Generate and log required (metadata) attributes of each subscription.

Situation Data Processing Center – Query Response Processing

The Situation Data Processing Center will perform the following functions for each retrieved situation data bundle.

1. Authenticate, as necessary, the credential of the of the Situation Data Warehouse
2. Validate the authenticated bundle structure and format.
3. Validate the structure and format of messages within the bundle
4. Store the validated bundle and/or messages in internal data stores for subsequent access.
5. Generate and log required (metadata) attributes of incoming deposit bundles.

Situation Data Processing Center – TSDM Depositing

The Situation Data Processing Center will perform the following functions for each Traveler Situation Data Message that is wishes to have disseminated.

1. Generate a Traveler Situation Data Message and its associated delivery/dispatch instructions with valid structure, content and format. The Traveler Situation Data Message data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735.
2. Subsequently initiate and manage the Traveler Situation Data Deposit information flow to the Situation Data Warehouse.

3. Track and manage all Traveler Situation Data messages that it deposited, using refreshed security credentials as necessary.
4. Generate and log required (metadata) attributes of each subscription.

6.3.9 Southeast Michigan Situation Data Warehouse (SDW)

The Situation Data Warehouse (SDW) is a Center based service built and operated by the Southeast Michigan Test Bed. It will provide data warehouse functions enabling the collection and distribution of a single inventory item, one or multiple (bundle) of regional historic situation data messages. As with any warehouse, the suppliers and consumers of transferred information will not need to have an established agreement with each other, nor will they need to have "a priori" knowledge of each other.

The two items processed by the Situation Data Warehouse are

1. The Traveler Situation Data Messages and the derivative Bundles. The Traveler Situation Data Message data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735. Traveler Situation Data Bundles will be tagged/encoded according to the rules defined in SAE J2735 (XML or ASN.1)
2. The Intersection Situation Data Bundle. Its data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735.

The three main functions of the Situation Data Warehouse, described below, are:

1. **Data Access Management** which defines the access mechanisms, structures and restrictions for inbound (from providers) and outbound (to requestors) data flows.
2. **Data Aggregation and Management** which defines the data storage, processing and management of the data within the warehouse.
3. **Support Services** to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; discover the location and credentialing information of other Test Bed Objects; and to obtain and manage security credentials with the SCMS.

The exchange of delivery information between the Provider and the Situation Data Clearinghouse will be derived from the Peer-to-Peer Data Exchange Message Sequence pattern described in Section X above, and in urn described in more detail in Section 6.3.3 below.

The Situation Data Clearinghouse will interact with the following Test Bed objects

1. Southeast Michigan Situation Data Processing Center which will deposit Traveler Situation Data Messages to the Warehouse. These messages will be assessed, categorized and aggregated into "bundles" based on the message's geo-boundary
2. Third Party Application Center which will deposit Traveler Situation Data Messages to the Warehouse. These messages will be assessed, categorized and aggregated into "bundles" based on the message's geo-boundary
3. Connected Vehicle OBE to accept inbound delivery requests and subsequently deliver requested Intersection Situation Data Bundles and/or Traveler Situation Data Message Bundles.

4. Test Bed Roadside Equipment to accept inbound deposits of Intersection Situation Data Bundles and to deliver Traveler Situation Data Messages Bundles when a valid request is received.
5. Support Services to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; and to obtain and manage security credentials with the SCMS.

6.3.9.1 SDW Support Services

SDW Support Services – Object Registration

1. Reach out to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to register its current cyber location and active public credentialing information.
2. Update its registration information with the Object Registration and Discovery Service upon any change in cyber location information.
3. Update its registration information with the Object Registration and Discovery Service upon any change in public credentialing information.

SDW Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.
5. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, reach out to the Object Registration and Discovery Service to "rediscover" the object and obtain its updated information.

SDW Support Services – Security Credential Services

This assumes that the SDW Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS or the WAID, the latest CRL. Ensure that any expired CRLs are discarded.

SDW Support Services – Service Monitoring

The Service Monitor Object has not been defined yet. This section will be added in a future version of this specification.

6.3.9.2 SDW Data Access Management

Data Access Management is handled separately for data providers and data consumers. Again, as with many warehouse based distribution systems, each Situation Data Warehouse will have an exclusive (non-overlapping) geographic region for which it will accept or provide goods (Traveler Situation Data Messages/Bundles, Intersection Situation Data Bundles, etc.). These geographic regions will be defined and bounded in units of degrees. Given that, the initial Situation Data Warehouse will be the located in the Southeast Michigan 2014 Test Bed and will have the geographic region shown above (See 4.2.1.1). As more providers come on line, the service area will be divided into 10 millidegree rectangles to support the greater granularity needed for the increased data volumes. As other Affiliated Test Beds come online, additional Situation Data Warehouses could be created with respective defined geographic regions.

6.3.9.3 SDW Data Collection and Aggregation

The Situation Data Warehouse will handle data collection and aggregation from providers (deposits) and consumers (deliveries) as described below.

Situation Data Warehouse – TSD Deposit Processing

The Situation Data Warehouse will perform the following functions for each deposited Traveler Situation Data Message.

1. Validate the structure and format of the TSD Deposit
2. Validate the structure, format and contents of the dissemination instructions.
3. Store the TSD message and associated dissemination instructions in internal data stores.
4. Discard any message with an End Time value that has been exceeded
5. Discard any message when its security credential expires.
6. Generate and log required (metadata) attributes of accepted messages.

Situation Data Warehouse – ISD Subscription Management

The Situation Data Warehouse will perform the following functions for its subscription that will be sent to the Situation Data Clearinghouse.

1. Generate subscription messages with valid structure, content and format for Intersection Situation Data subscriptions
2. Subsequently initiate and manage the Intersection Situation Data Delivery information flow the Situation Data Clearinghouse.
3. Track and manage the active subscription, using refreshed security credentials
4. Generate and log required (metadata) attributes of the subscription.

Situation Data Processing Center – Subscribed ISD Processing

The Situation Data Warehouse will perform the following functions for each “subscribed” situation data bundle that it receives.

1. Authenticate, as necessary, the credential of the Situation Data Clearinghouse
2. Validate the authenticated bundle structure and format.

3. Validate the structure and format of messages within the bundle
4. Store the validated bundle and/or messages in internal data stores for subsequent access.
5. Generate and log required (metadata) attributes of incoming deposit bundles.
6. Discard any ISD bundle with a Bundle Generation Time value indicating that it is older than the time interval defined by the "Max Bundle Lifespan" (default to 30 minutes)

Situation Data Warehouse – Query Response (Delivery) Processing

The Situation Data Clearinghouse will perform the following functions to process and prepare bundles for query-based delivery to registered consumers.

1. The Situation Data Warehouse will authenticate the delivery request and validate the supplied delivery criteria (bundle type, location boundary, etc.).
2. It will log and discard any unauthenticated or invalid delivery request.
3. The Situation Data Warehouse will access the internal data stores to extract a copy of each message or bundle that matches all provided delivery request criteria.
    - Only messages or bundles will the matching Message Type will be gathered
    - Only messages or bundles with a Bundle Location that fall within the Geographic Boundary of Request will be collected.
    - Messages will be bundled into the corresponding bundle type.
4. The Situation Data Warehouse will aggregate the collected bundles in preparation for delivery to the registered requestor.

Situation Data Warehouse - Housekeeping

1. The Situation Data Warehouse will log attributes of incoming deposit messages and bundles and outgoing delivery bundles,
2. The Situation Data Warehouse will prepare transaction summaries and statistics.
3. The Situation Data Warehouse will purge expired data messages and/or bundles.
4. A log record of each bundle purge along with associated metadata will be generated and captured. All logging functions will be configurable to be turned on or off.
5. All log storage will be bounded by configurable size thresholds and/or configurable lifespans.

6.3.10 Third Party Application Center

The Third Party Application Center (TPAC) represents the private infrastructure (deployed off roadways) which is used to develop, maintain and or host third party software processes or applications which will interact with other Test Bed objects. It is anticipated that there will be multiple Third Party Application Centers owned and operated by different Enterprises. It is anticipated that, for the most part, each of these Enterprises will also own and operate "peer" applications running on their Third Party Connected Vehicle OBEs.

The TPAC will interact with the following Test Bed objects

- **Situation Data Clearinghouse** to accept deliveries of Enhanced Vehicle Situation Data Bundles deposited by vehicles. This will support the TPAC's ability to execute algorithms necessary to evaluate current traffic and conditions.

- **Situation Data Warehouse** to generate and deposit Traveler Situation Data Messages for eventual distribution to CV equipped vehicles.
- **Support Services** to register its location (geo-fence and cyber address) with the Object Registration & Discovery Service; and to obtain and manage security credentials with the SCMS.

6.3.10.1 Third Party (3P) Center Support Services

TPAC Support Services – Object Registration

1. Reach out to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to register its current cyber location and active public credentialing information.
2. Update its registration information with the Object Registration and Discovery Service upon any change in cyber location information.
3. Update its registration information with the Object Registration and Discovery Service upon any change in public credentialing information.

TPAC Support Services – Object Discovery

1. Reach out, as needed, to the Object Registration and Discovery Service using its preconfigured (e.g. hardcoded, manually configured, or obtained via bootstrap) cyber location to requires the cyber location of other Southeast Michigan Test Bed objects.
2. Store any information and security credentials retrieved from the ORDS for subsequent access.
3. Monitor the list of retrieved information for other Test Bed objects for the expiration of either the cyber location or the associated credentialing information.
4. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, take appropriate actions to terminate active dialogs with the specific object.
5. Upon expiration of either cyber location or the associated credentialing information for any "discovered" object, reach out to the Object Registration and Discovery Service to "rediscover" the object and obtain its updated information.

TPAC Support Services – Security Credential Services

This assumes that the TPAC Support Services application object will already have the cyber location of the SCMS, either as preconfigured information or as obtained from the ORDS.

1. Retrieve, as required, from the SCMS all necessary security credentials. Store any credentials or authorizations received. Ensure that any expired credentials are discarded.
2. Retrieve, as required, from the SCMS all necessary decryption keys. Store any credentialing information received from the SCMS. Ensure that any expired keys are discarded.
3. Retrieve, as required, from the SCMS, the latest CRL. Ensure that any expired CRLs are discarded.

6.3.10.2 Third Party (3P) Information Dissemination

The Third Party (3P) Information Dissemination which facilitates the TPAC interacting with the Situation Data Warehouse to deposit Traveler Situation Data Messages for eventual dispatch to CV equipped

vehicles. It also facilitates the TPAC interacting with the Situation Data Clearinghouse to subscribe for and to accept and process deliveries of Enhanced Vehicle Situation Data bundles.

Third Party Information Dissemination – Subscription Management

The Third Party Information Dissemination will perform the following functions for subscriptions that will be sent to the Situation Data Clearinghouse.

1. Generate subscription messages with valid structure, content and format for Enhanced Vehicle Situation Data subscriptions; and subsequently initiate and manage the Enhanced Vehicle Situation Data Delivery information flow the Situation Data Clearinghouse.
2. Generate subscription messages with valid structure, content and format for Intersection Situation Data subscriptions; and subsequently initiate and manage the Intersection Situation Data Delivery information flow the Situation Data Clearinghouse.
3. Track and manage all active subscriptions, using refreshed security credentials
4. Generate and log required (metadata) attributes of each subscription.

Third Party Information Dissemination – Subscribed Content Processing

The Third Party Information Dissemination will perform the following functions for each "subscribed" situation data bundle that it receives.

1. Authenticate, as necessary, the credential of the Situation Data Clearinghouse
2. Validate the authenticated bundle structure and format.
3. Validate the structure and format of messages within the bundle
4. Store the validated bundle and/or messages in internal data stores for subsequent access.
5. Generate and log required (metadata) attributes of incoming deposit bundles.

Third Party Information Dissemination – Query Management

The Third Party Information Dissemination will perform the following functions for queries that will be sent to the Situation Data Warehouse/

1. Generate queries with valid structure, content and format for Enhanced Vehicle Situation Data Bundles; and subsequently initiate and manage the Enhanced Vehicle Situation Data Delivery information flow to the Situation Data Warehouse.
2. Generate queries with valid structure, content and format for Intersection Situation Data bundles; and subsequently initiate and manage the Intersection Situation Data Delivery information flow to the Situation Data Warehouse.
3. Track and manage all active subscriptions, using refreshed security credentials
4. Generate and log required (metadata) attributes of each subscription.

Third Party Information Dissemination – Query Response Processing

The Third Party Information Dissemination will perform the following functions for each retrieved situation data bundle.

1. Authenticate, as necessary, the credential of the of the Situation Data Warehouse
2. Validate the authenticated bundle structure and format.

3. Validate the structure and format of messages within the bundle
4. Store the validated bundle and/or messages in internal data stores for subsequent access.
5. Generate and log required (metadata) attributes of incoming deposit bundles.

Third Party Information Dissemination – TSDM Depositing

The Third Party Information Dissemination will perform the following functions for each Traveler Situation Data Message that is wishes to have disseminated.

1. Generate a Traveler Situation Data Message and its associated delivery/dispatch instructions with valid structure, content and format. The Traveler Situation Data Message data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735.
2. Subsequently initiate and manage the Traveler Situation Data Deposit information flow to the Situation Data Warehouse.
3. Track and manage all Traveler Situation Data messages that it deposited, using refreshed security credentials as necessary.

Third Party Information Dissemination – ISD Bundle Depositing

The Third Party Information Dissemination will perform the following functions for each Intersection Situation Data Bundle that is wishes to deposit.

1. Generate one or more Intersection Situation Data Bundle with valid structure, content and format. The Intersection Situation Data Message data elements will be selected from the data elements identified in the published Society of Automotive Engineers (SAE) J2735 standard, or created according to the rules given in SAE J2735. The sourcing of the data and translation into the SAE structure is outside the scope of this project.
2. Subsequently initiate and manage the Intersection Situation Data Deposit information flow to the Situation Data Warehouse.

6.3.10.3 Third Party (3P) Center P2P Application

The Third Party (3P) Center P2P Application hosts one or more third party applications which will communicate with "peer" applications deployed onboard connected vehicles. It is anticipated and strongly encouraged that these Third Party applications will be developed using the "Peer to Peer" Data Exchange Pattern described in Section 6.2.1 above. Their specific usage and functionality is outside the scope of this document.

6.3.11 Wide Area Information Distributor

Section is under development.

6.3.11.1 WAID Support Services

Section is under development.

6.3.11.2 WAID Situation Data Communications

Section is under development.

7 Operational Scenarios

This section is intended to provide an overview of the major operational uses for the Southeast Michigan 2014 Test Bed.

7.1 Enhanced Vehicle Situation Data Distribution

This scenario illustrates how enhanced vehicle situation data will be collected from the various Connected Vehicle OBEs and consolidated into a Data Distribution System (Situation Data Clearinghouse) for subsequent distribution to interested parties.

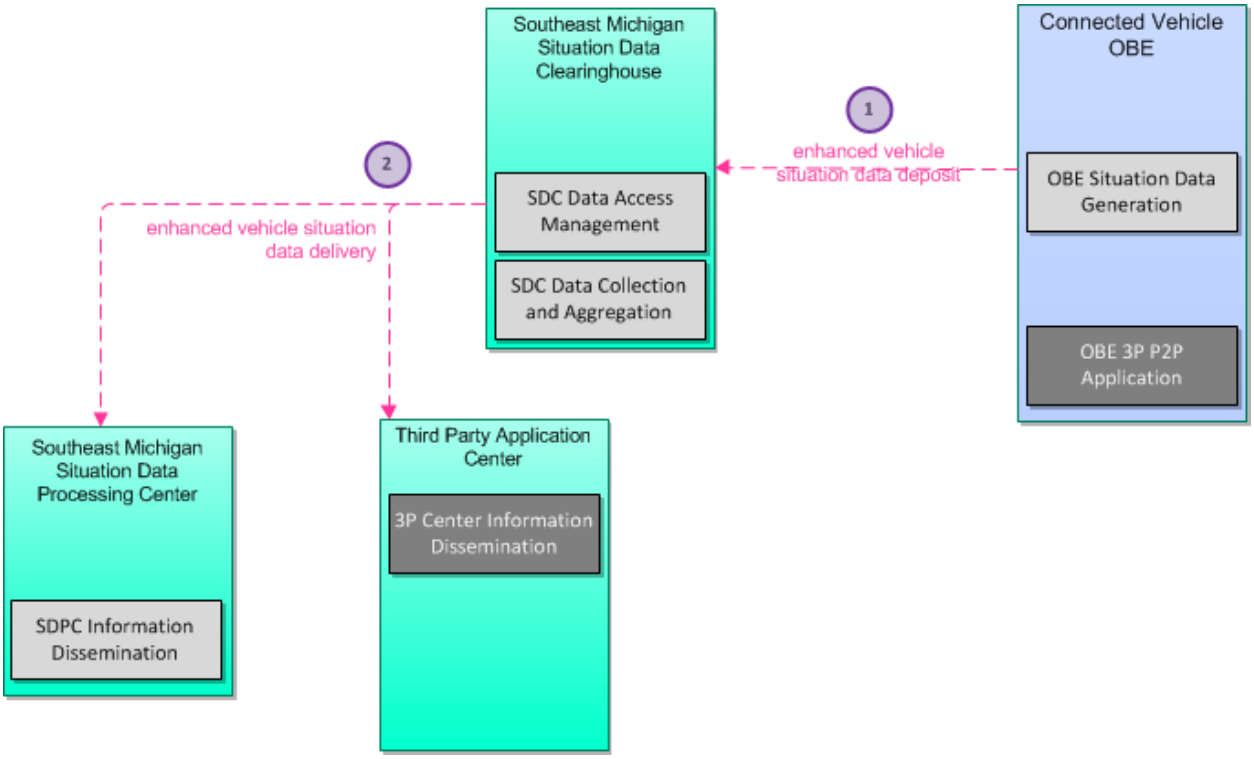

Figure 9 – Enhanced Vehicle Situation Data Dissemination

Operational Steps

1. Enhanced Situation Data Messages will be periodically generated by Connected Vehicle OBEs, and bundled for subsequent deposit into the Situation Data Clearinghouse.
2. The Situation Data Clearinghouse will "immediately forward" a copy of any deposited EVSD Bundle to any Test Bed Object which has subscribed to receive EVSD bundles with matching characteristics.

7.2 Intersection Situation Data Dissemination

This scenario illustrates how intersection situation data is generated and distributed throughout the Southeast Michigan 2014 Test Bed.

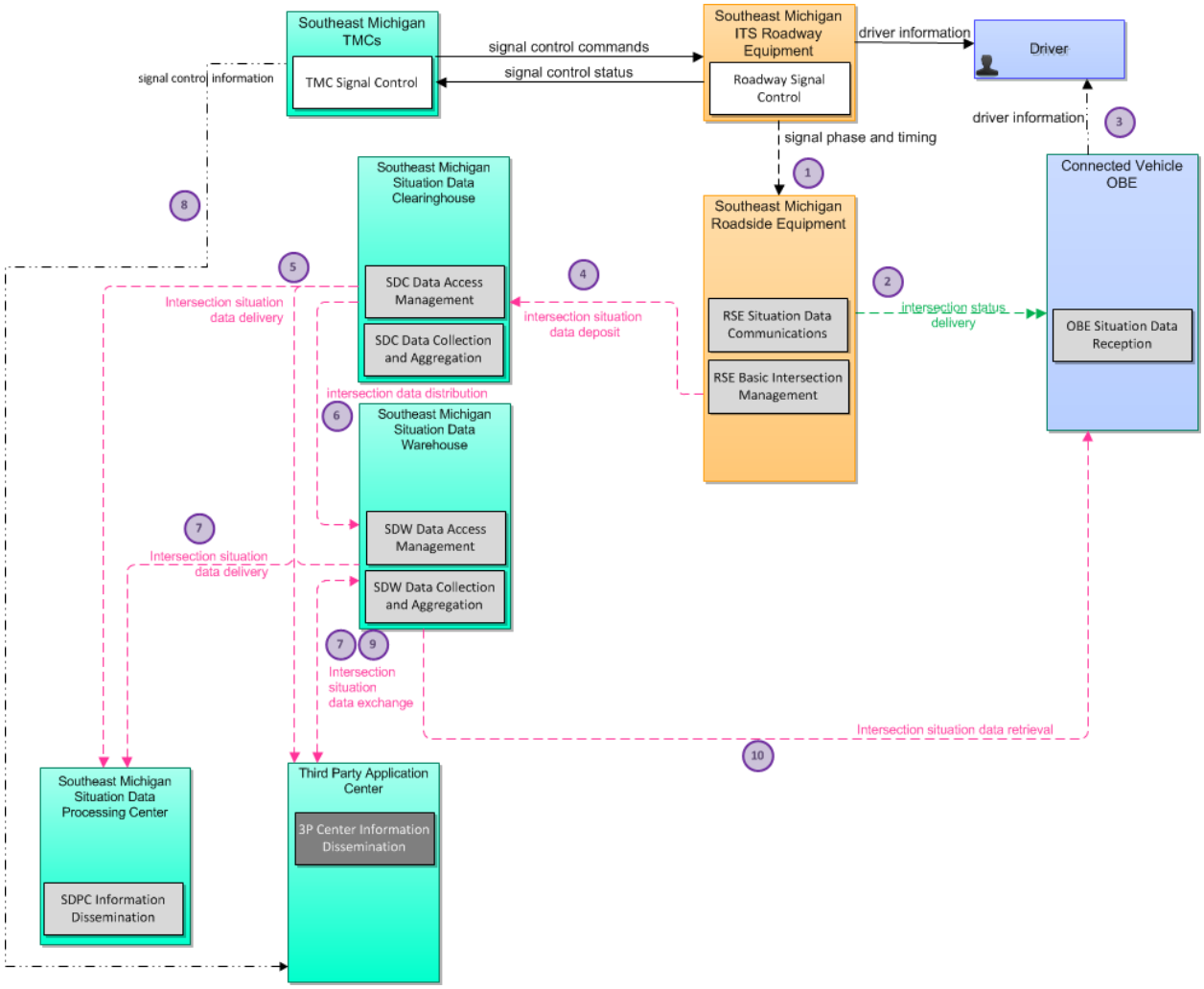

Figure 10 – Intersection Situation Data Dissemination

Operational Steps

1. ITS Roadway Equipment will send the signal, phase and timing information it generates to the RSE.
2. The RSE will generate periodic snapshots of this information into Signal Phase & Timing (SPaT) messages and will broadcast them to passing Connected Vehicles OBEs.
3. Each Connected Vehicle which receives the SPaT message may present part or all of the signal, phase and timing information received in the SPaT message to its Driver.
4. Some or all of the SPaT Messages will be bundled by the RSE, along with the current MAP into ISD Bundles, and deposited at the Situation Data Clearinghouse.

5. The Situation Data Clearinghouse will "immediately forward" a copy of any deposited ISD Bundle to any Test Bed Object which has subscribed to receive ISD bundles with matching characteristics.
6. The Situation Data Clearinghouse will "immediately forward" a copy of **all** deposited ISD Bundles to the Situation Data Warehouse for subsequent retrieval by other Test Bed Objects.
7. The Situation Data Processing Center and any Third Party Application Center may query and retrieve stored ISD bundles from the Situation Data Warehouse, prior to the expiration of these bundles.
8. Selected Third Party Application Centers may directly receive signal, phase and timing information and GID information, via Southeast Michigan TMCs, for intersections that are not collocated with RSEs.
9. The Third Party Application Centers will generate SPaT Messages for these intersections and bundle them, along with corresponding MAP message into ISD bundles which will be deposited into the Situation Data Warehouse. Additionally, the Third Party Application Centers could generate SPaT Messages for targeted non-signalized intersections, and bundle them, along with corresponding MAP message into ISD bundles which will also be deposited into the Situation Data Warehouse.
10. Connected Vehicle OBEs may periodically query the Situation Data Warehouse for retrieval of ISD bundles within a geographic boundary. The Situation Data Warehouse will deliver these bundles to the requesting Connected Vehicle OBE; which will use them for various onboard applications.

7.3 Traveler Situation Data Dissemination

This scenario illustrates how traveler situation data is generated and distributed throughout the Southeast Michigan 2014 Test Bed.

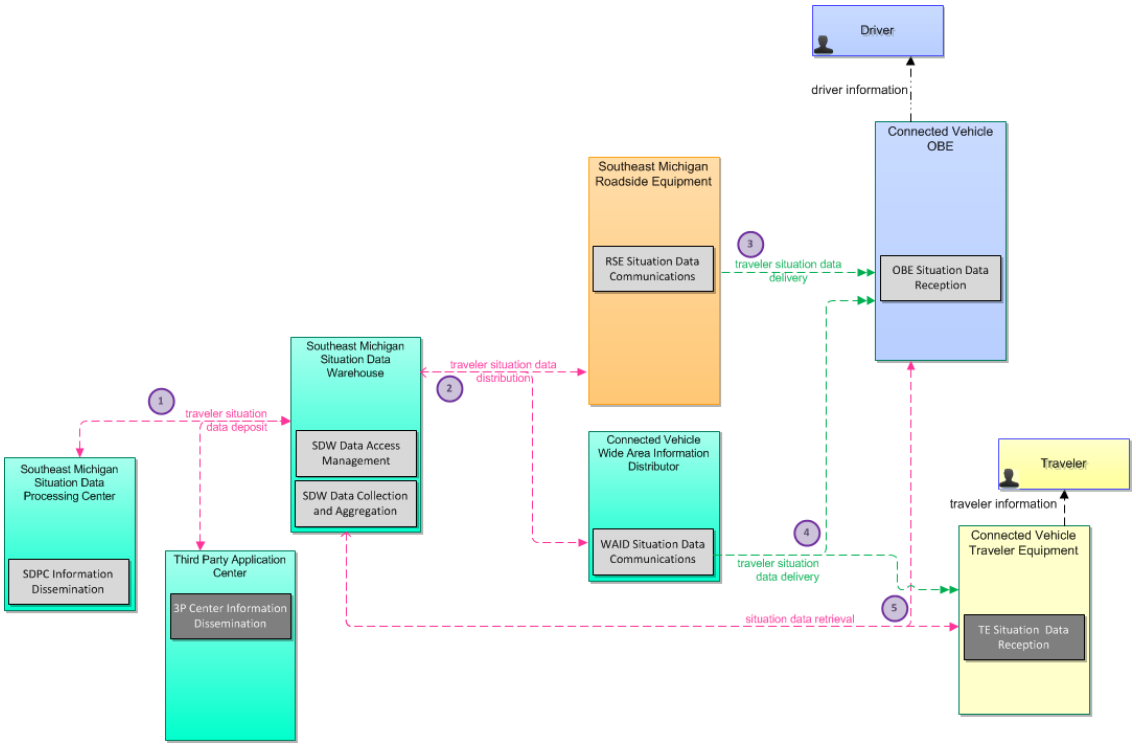

Figure 11 – Traveler Situation Data Dissemination

1. The Situation Data Processing Center or an authorized Third Party Application Center, generate and send an traveler (advisory) situation data message and its associated dispatch instructions to the to the Situation Data Warehouse.
2. The Situation Data Warehouse validates, sorts and bundles these messages into data stores based on the geographic area associated with the advisory message.
3. The WAID and each RSE periodically requests all traveler situation data bundles within their respective geographic boundary and respectively construct their radio “playlist” based on the dispatch instructions associated with the constituent messages within the retrieved bundles.
4. A traveler (advisory) message and its associated delivery instructions are generated by the Situation Data Processing Center or a Third Party Application Center and send to the Regional Historic Situation Data Warehouse. The Warehouse validates and sorts these messages into data stores based on the geographic boundary associated with the advisory message. Connected Vehicles may periodically requests advisory messages within a geographic boundary. The Warehouse will bundle and deliver these messages to the requesting vehicle.