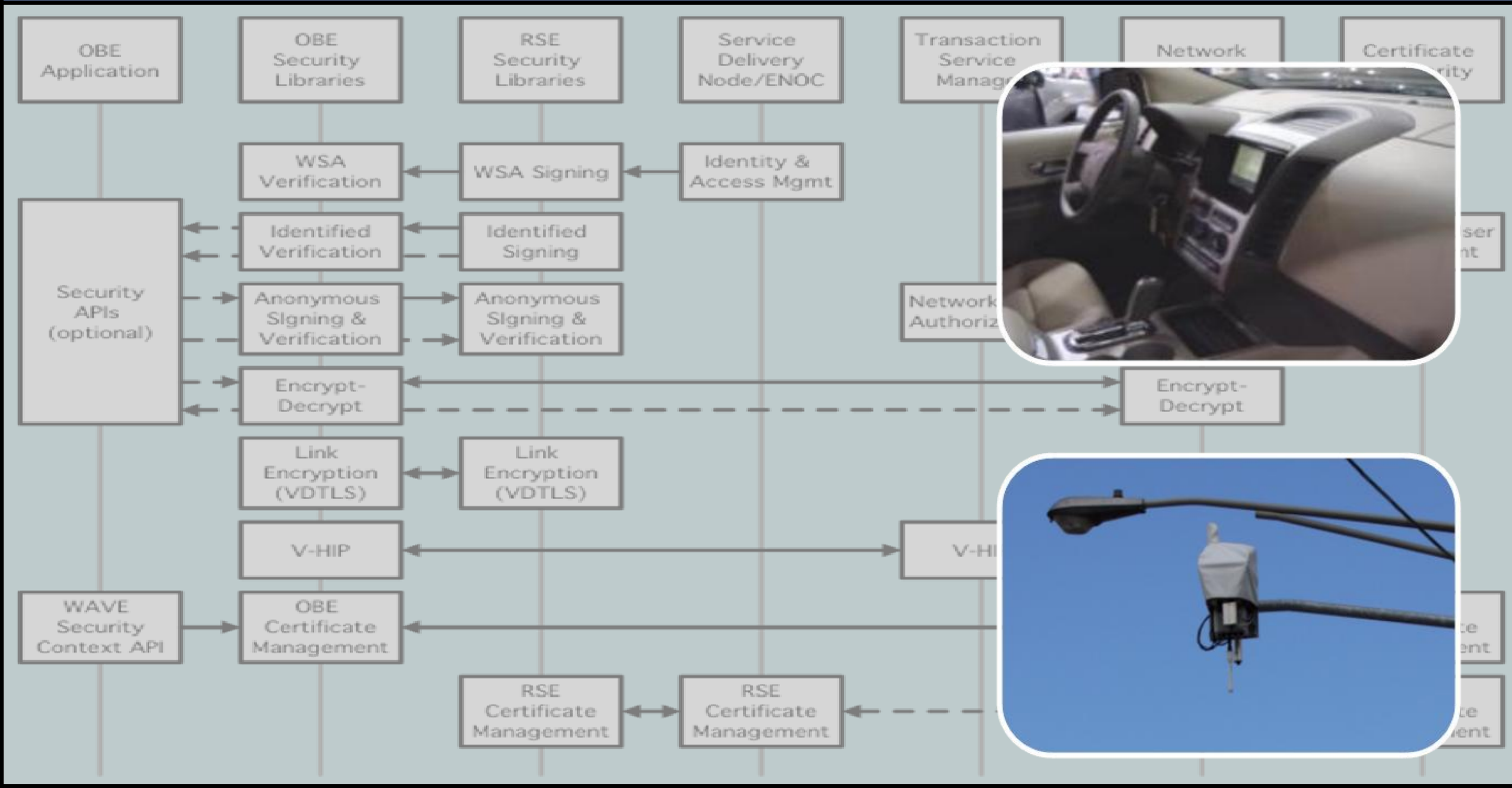
Final Report:

Vehicle Infrastructure Integration Proof of Concept Executive Summary – Vehicle



Submitted to the
Research and Innovative
Technology Administration,
US Department of Transportation
by
The VII Consortium
May 19, 2009

Notice 1

This material is based upon work supported by the United States Department of Transportation under Cooperative Agreement # DTFH61-05-H-00003.

Notice 2

This report includes references to “Vehicle Infrastructure Integration” (VII). This program name was in official use at the inception of and during the execution of the work described in this report. The United States Department of Transportation has initiated a new program entitled “IntelliDrive^{SM}” which now encompasses all activities that were previously part of VII.

Notice 3

This publication is distributed by the United States Department of Transportation in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation. The United States Government assumes no liability for its contents or use thereof.

If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Technical Report Documentation Page

1. Report Number
FHWA-JPO-09-003

2. Government Accession No.

3. Recipient's Catalog No.
EDL 14443

4. Title and Subtitle
Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary - Vehicle

5. Report Date
May 19, 2009

6. Performing Organization Code

7. Author(s)
Scott Andrews, Michael Cops

8. Performing Organization Report No.

9. Performing Organization Name and Address
VII Consortium, Suite 600,
39555 Orchard Hill Place,
Novi, MI 48375

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFH61-05-H-00003

12. Sponsoring Agency Name and Address
U.S. Department Of Transportation
Research and Innovative Technology Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

13. Type of Report and Period Covered
Executive summary of completed program.
Oct 2005 to Dec 2008

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract
This report summarizes a program of work resulting from a Cooperative Agreement between USDOT and the VII Consortium to develop and test a Proof of Concept VII system based on DSRC wireless communication between an infrastructure and mobile terminals. It supports applications for improvement in safety, mobility and enables other commercial applications. Key findings and recommendations for further work are presented.

17. Key Words
ITS Architecture, IA, Intelligent Transportation Systems, ITS, Vehicle Infrastructure Integration, VII, Architecture, Transportation, Transportation Systems, Infrastructure, Integration, Intellidrive^{SM}

18. Distribution Statement
No restrictions.
This document is available to the public.

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
27

22. Price

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

GLOSSARY OF TERMS AND ACRONYMS

3G	Third Generation Cellular (Wireless Data System)
AASHTO	American Association of State Highway and Transportation Officials
AOCA	Anonymous OBE Certifying Authority
AMDS	Advisory Message Delivery Service
API	Application Programming Interface
BAH	Booz Allen Hamilton
BER	Burst Error Rate
BMW	BMW of North America, LLC
BSP	Board Support Package
CA	Certificate Authority
CAN	Controller Area Network
CCL	Channel Coordination Layer
CCH	Control Channel
CEP	Circular Error Probable
CM	Certificate Manager
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
CRL	Certificate Revocation List
DGPS	Differential Global Positioning System
DSRC	Dedicated Short Range Communications
DTE	Development Test Environment
ECC	Elliptic Curve Cryptography
ENOC	Enterprise Network Operations Center
ESB	Enterprise Service Bus
XML	Extensible Markup Language
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FPGA	Field Programmable Gate Array
Gbps	Gigabit Per Second
GHz	Giga-Hertz
GID	Geographic Intersection Description
GM	General Motors Corporation
GPS	Global Positioning System
HANDGPS	High Accuracy National Differential GPS
HB	Heartbeat
HIP	Host Identity Protocol
HMI	Human Machine Interface
HPSAM	High Performance Security Accelerating Module
HTTP	Hypertext Transfer Protocol
ILS	Information Lookup Service
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISO	International Standards Organization
IVI	Intelligent Vehicle Initiative
I2V	Infrastructure to Vehicle

IVPS	In-Vehicle Payment Service
IVTP	In-Vehicle Toll Processing
ITS	Intelligent Transportation Systems
JMS	Java Message Service
JVM	Java Virtual Machine
LIN	Local Interconnect Network
LLCF	Low Level CAN Framework
LTP	Local Transaction Processor
LTTP	LTP Toll Processing
MAC	Medium Access Control
MDOT	Michigan Department of Transportation
MEDS	Map Element Distribution System
MEG	Map Element Generator
MHz	Mega-Hertz
MINAP	Michigan Network Access Point
MTU	Maximum Transmission Unit
NTPDA	Network Trip Path Data Accumulator
NUC	Network User Component
NUG	Network User Gateway
NUPS	Network Users Payment Service
OAA	OBE Authorizing Authority
OBE	On-Board Equipment
OCM	OBE Communications Manager
OEM	Original Equipment Manufacturer
OBNA	Off-Board Navigation Application
OS	Operating System
OSGi	Open Services Gateway Initiative
PC	Personal Computer
PCI	Peripheral Component Interconnect
PDC	Probe Data Collection
PDCS	Probe Data Collection Service
PDDS	Probe Data Distribution Service
PDSS	Probe Data Subscription Service
PDM	Probe Data Management
PDU	Protocol Data Units
PDS	Probe Data Service
PDVC	Probe Data Vehicle Component
PER	Packer Error Rate
PKI	Public Key Infrastructure
POC	Proof of Concept
PSC	Provider Service Context
PSID	Provider Service Identifier
PSN	Probe Sequence Number
RCOC	Road Commission for Oakland County
RF	Radio Frequency
RITA	Research and Innovative Technology Administration
RSE	Roadside Equipment
SAE	Society of Automotive Engineers
SCH	Service Channel

SDN	Service Delivery Node
SDRAM	Synchronous Dynamic Random Access Memory
SIT (Tunnel)	Simple Internet Transition (Tunnel)
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPAT	Signal Phase and Timing
SRS	Software Requirement Specification
TCP/IP	Transmission Control Protocol/ Internet Protocol
TMT	Technical Management Team
TPGA	Trip-Path General Application
TPT	Trip-Path Transmission
TSM	Transaction Service Manager
UDP	Universal Datagram Protocol
URL	Uniform Resource Locator
USDOT	United States Department of Transportation
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VAPI	Virus Application Programming Interface
V-DTLS	VII-Datagram Transport Layer Security
VEG	Vehicle Expert Group
V-HIP	VII-Host Identity Protocol
VGA	Video Graphics Array
VIDMT	Vehicle Interface Device Management Tree
VII	Vehicle Infrastructure Integration
VIIC	Vehicle Infrastructure Integration Consortium
VIN	Vehicle Identification Number
VIS	Vehicle Interface Service
VPN	Virtual Private Network
VSC	Vehicle Signage Component
VW	Volkswagen of America, Inc.
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environments
WME	Wave Management Entity
WO	Work Order
WSA	WAVE Service Advertisement
WSC	WAVE Security Context
WSMP	WAVE Short Message Protocol

1 Abstract

This report summarizes a program of work resulting from a Cooperative Agreement # DTFH61-05-H-00003 between the United States Department of Transportation (USDOT) and the Vehicle Infrastructure Integration Consortium (VIIC) to develop and test a Proof of Concept (POC) Vehicle Infrastructure Integration (VII) system, based on Dedicated Short Range Communications (DSRC), a wireless communication between an infrastructure and mobile terminals. It supports applications for improvement in safety, mobility and enables other commercial applications. Key findings and recommendations for further work are presented.

2 Organization of the Final Report

The VIIC's Final Report is organized into five volumes. Volume 1a is **Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary – Vehicle**, which provides an overview of the program goals and objectives, program organization, program technical direction and key findings and recommendations. It does not detail test results (See Volumes 3a, 4a and 5a for test result details) and is recommended for executives and managers of organizations concerned with the deployment of VII systems.

The remaining four volumes are:

Volume 2a -- Final Report: VII Proof of Concept Technical Description - Vehicle
This volume describes the technical approach of the program and specifically describes the system architecture, the system component design and the sample applications designed to enable some of the system testing. In addition, the deployment of the system to the test track and Development Test Environment (DTE) is described. This report is recommended for engineering managers and practicing engineers concerned with the deployment of VII systems.

Volume 3a -- Final Report: VII Proof of Concept Results and Findings Summary - Vehicle
This volume describes the test objectives and approach and presents a summary of results and findings for both the system and application testing. Detailed results are not presented. This report is recommended for engineering managers and engineers concerned with the deployment of VII systems. It assumes the reader has knowledge of the system architecture as described in Volume 2a.

Volume 4a -- Final Report: VII Proof of Concept System Detailed Test Results – Vehicle
This volume describes the system test objectives, the system test approach and details the results of the individual components and the end-to-end system tests. This report is recommended for engineers concerned with the deployment of VII systems. It assumes the reader has knowledge of the system architecture and components as described in Volume 2a.

Volume 5a -- Final Report: VII Proof of Concept Applications Detailed Test Results - Vehicle
This volume describes application test objectives, the application test approach and details the results of the individual application tests. This report is recommended for engineers concerned with the deployment of VII systems and the design of VII applications. It assumes the reader has knowledge of the system architecture and applications as described in Volume 2a.

Volumes 1a, 2a and 3a have complimentary reports: Volumes 1b, 2b and 3b, which describe the development and testing of the POC infrastructure written by Booz Allen Hamilton (BAH).

3 VII POC Program Overview

3.1 Background

During the 10th World Congress held in Madrid, Spain (November 2003), the USDOT announced a new initiative, namely, Vehicle Infrastructure Integration (VII). This initiative represents the confluence of three areas of high interest to transportation policy managers: the Intelligent Vehicle Initiative (IVI), an emphasis on improved traffic operations, and the continuing evolution in telecommunication technology.

Regarding the latter item, the Federal Communications Commission (FCC) has allocated 75 MHz at 5.9 GHz for the primary purpose of improving transportation safety. In addition to safety of life and public safety applications, the FCC's Final Report and Order also allows private and non-safety applications to make use of the spectrum on a lower priority basis. DSRC, the wireless medium, will allow vehicles to communicate with a low-cost roadside infrastructure, as well as with each other, in real time. This communications capability, in combination with a nationwide data collection and processing network, will facilitate improvements to safety, mobility and productivity/convenience.

Reducing the number and severity of roadway transportation incidents is a top priority of the USDOT. Development of a system supporting communication between vehicles and between vehicles and a roadway infrastructure has the potential for positively contributing to the government's goal of improving transportation safety. Such real-time communications would enable a range of crash avoidance and crash mitigation applications with the potential to reduce traffic deaths and injuries, while simultaneously enabling a host of additional applications with secondary benefits, such as optimized traffic and incident management systems.

To enable this vision, it was proposed to undertake a project to specify, design, build and test a small-scale instantiation of the envisioned national system to determine if the concept was sound and could support the intended use. Pending the anticipated results of the system's testing, a nationwide system would be deployed. It was understood that the success of the project required close collaboration between the USDOT, the State Departments of Transportation through the American Association of State Highway and Transportation Officials (AASHTO) and light-duty vehicle manufacturers. These primary stakeholders were brought together by the USDOT in the National Vehicle Infrastructure Integration Coalition.

3.2 Program Goals and Objectives

The original program goals included development and testing of a concept system that could be nationally deployed beginning some time around 2010, to provide a mechanism for wirelessly sending and receiving roadway information to and from vehicles, and between vehicles to satisfy the following viability criteria*:

Safety

- Provides for infrastructure-initiated safety applications.
- Supports vehicle-initiated safety applications.

Mobility

- Provides for collection of various mobility data from vehicles.
- Provides for use of collected mobility data by state and local authorities.
- Exhibits sufficient benefit in terms of road and traffic management and transportation efficiency.

Private Services

- Vehicles can access private services through system.
- Private services can access vehicles through system.
- Co-existence of private services with safety and mobility services is economically viable.
- Private services can be implemented in a manner that does not interfere with safety and mobility Applications.

Security

- System is resistant to denial of service, replay and intrusion attacks.
- Security compromises can be identified and mitigated.
- Security credentials can be properly distributed and managed at all levels of deployment.

Maintainability

- Roadside Equipment (RSE) software can be remotely managed through the network.
- VII-related vehicle software can be securely maintained over the vehicle life cycle.

Privacy

- Cannot track an individual vehicle over any road segment longer than 2 km.
- Cannot identify any individual vehicle as violating a traffic law through publicly collected data.
- Cannot identify a vehicle or a vehicle occupant or owner from messages sent to, or through, the infrastructure.

* Note: These criteria were developed by the VIIC at the start of the program. They were agreed upon between the VIIC members and the USDOT. Other criteria have been proposed, but as of this date, none have been fully agreed upon by all of the VII stakeholders. The other criteria are generally a simplified and less comprehensive set, relative to the criteria presented here. These criteria are used for completeness, and in general, any differences between this set and the others discussed are minor.

3.3 Project Roles and Responsibilities

The system concept was understood to consist of a roadside network component and on-board vehicle equipment component. The responsibility for the network and RSE was assigned to Booz Allen Hamilton (BAH), a USDOT contractor, and the On-Board Equipment (OBE) to light-duty vehicle manufacturers, represented by the VIIC. Additionally, it was anticipated that typical applications would be designed and tested as part of the project. The responsibility for public applications, i.e. those to be used by the Federal and state governments, was assigned to BAH and those likely to be used by the vehicle manufacturers and providers of the commercial services, were assigned to the VIIC and their suppliers for development.

The USDOT's Intelligent Transportation Systems (ITS) Joint Program Office provided oversight and program management. Funding for the program was shared between USDOT and the VIIC, with the USDOT providing the majority share.

3.4 VII Consortium Formation

The VIIC was formed in February 2005 by three manufacturers of light-duty vehicles for the specific purpose of actively engaging in the design, testing and evaluation of a deployable VII system for the United States. The Consortium was also formed to provide a contracting mechanism for the Cooperative Agreement that was later established with the USDOT Federal Highway Administration (FHWA). Initial membership included Daimler-Chrysler, Ford Motor Company and Nissan Technical Center North America, Inc. Subsequently, the membership increased to include BMW of North America, LLC, General Motors Corporation, Honda R&D Americas, Inc, Toyota Motor Engineering and Manufacturing North America, Inc. and Volkswagen of America, Inc. Since the split of the Daimler-Chrysler organization, both Mercedes-Benz Research and Development North America, Inc. and Chrysler LLC have retained memberships resulting in the VIIC membership totaling nine light-duty vehicle manufacturers at the time of this report publication. The Consortium is a Michigan 501(c)(6) non-profit organization.

3.5 Cooperative Agreement between VIIC and USDOT

A Cooperative Agreement between the USDOT FHWA and the VIIC was executed on December 7, 2005. The objectives of this agreement are:

- Analysis of the requirements to permit the auto industry to provide a coordinated input to the Vehicle Infrastructure Integration Coalition
- Analysis of the requirements and definition of specific design elements of the VII architecture
- Design of specific hardware to facilitate the implementation of VII system
- Develop software that could be employed either on the vehicle or in the infrastructure
- Fabrication or procurement of equipment to be used in the test and evaluation of the VII program
- Test specific elements and/or combinations of elements of the VII architecture
- Integration of elements of the VII architecture to permit evaluation of the design
- Evaluation of the effectiveness of specific designs with respect to the stated objectives of VII
- Analysis of data and results of the VII program.

The period of performance of the Cooperative Agreement is 60 months.

3.6 VIIC Organization

The VIIC organization is detailed in Figure 3-1.

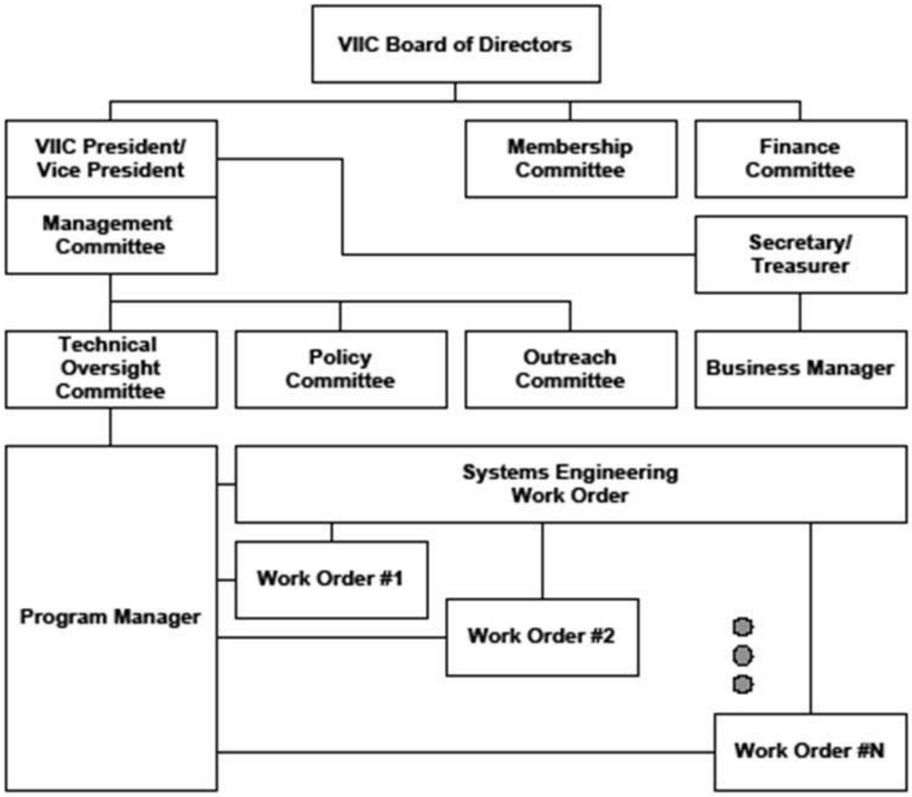


Figure 3-1 VIIC Program Organization

The VIIC Management Committee consisting of members from each of the VIIC participating vehicle manufacturers report to the VIIC Board of Directors, which is responsible for carrying out the charter outlined in the Articles of Incorporation. The Management Committee manages the daily operations of the VIIC through three committees: the Technical Oversight Committee, the Policy Committee and the Outreach Committee. The program is subdivided into a series of twelve (12) Work Orders detailed in Table 1 for executing the technical work policy and outreach programs.

The Policy and Outreach Committees have jurisdiction over the Policy Work Order (WO) and the Technical Oversight Committee has jurisdiction over the remaining WOs dealing with technical content of the program through the office of the Program Manager. Each WO is managed by a Technical Management Team (TMT) leader who is responsible for its technical direction, delivering the work products and maintaining the schedule for the deliverables.

Work Order #	***Work Order Title***	***Work Order #***	***Work Order Title***
1	Program Management	7	Positioning
2	Systems Engineering	8	Security Framework
3	Radio	9	Testing Lab and Facilities
4	Policy Support	10	Field Operational Test*
5	OBE Subsystem	11	Alternative Analyses*
6	Application Development	12	Private Service Enablers

*****not initiated

Table 1 Cooperative Agreement Work Orders

3.7 VIIC Supplier Selection

The design of a complex system required the expertise of companies with a wide range of diverse skills ranging from automotive electronics to networking systems. It was also recognized that the inclusion of a significant number of suppliers in the program would involve related industries and help to accelerate industry involvement. Invitations to submit proposals were sent to approximately 100 suppliers known to have an interest and the capabilities to develop the VII system. Proposals were reviewed and selections of the final supplier candidates were made by the program team including the VIIC membership. This activity is detailed in Volume 2a.

3.8 Collaboration Agreement between VIIC and Suppliers

The Collaboration Agreement was developed to protect the intellectual property right of the WO participants. The Collaboration Agreement was used in WOs where intellectual property was likely to be used or developed. Each WO was supported by a number of suppliers as detailed in Volume 2a. As a result of the Collaboration Agreement, these teams of suppliers were able to work collaboratively in a pre-competitive environment.

3.9 Combined Program Management Process

Formal program management processes were applied as appropriate for the size and complexity of the program. The need for this was accentuated by the number of WOs, (the relatively large number of suppliers spread across two continents) and the assignment of responsibilities between VIIC and BAH as described in Section 3.3. To achieve this goal, the program was broken down into the following tasks:

1. Collect stakeholder requirements.
2. Develop a concept of operations for the system, based on stakeholder requirements.
3. Develop requirements for the system concept and its components.
4. Develop or procure the components according to the requirements.
5. Assemble and deploy a small scale version of the system.
6. Perform integration testing.
7. Perform system testing against performance specifications.
8. Analyze results and determine if the viability criteria for the system had been met.
9. Report on the findings of the program.

4 VII POC Technical Overview

4.1 POC System Architecture Description

The POC system includes mobile terminals that were typically installed in vehicles. In the POC these units are known as On-Board Equipment (OBE). OBEs exchange messages with each other for Vehicle-to-Vehicle (V2V) applications and with stationary roadside terminals known as Roadside Equipment (RSE) for Vehicle to Infrastructure (V2I) applications. The link between OBEs and between OBE and RSE is the DSRC Radio system. The RSEs are connected to, and are remotely managed by a Service Delivery Node (SDN) and an Enterprise Network Operations Center (ENOC). The SDN provides a variety of services that are described in more detail in subsequent sections.

A critical aspect of the VII architecture is the management of scale. The system needs to be designed to support 100% vehicle deployment, which translates to just over 200 million vehicles. In operation, this means that applications such as Probe Data Collection (PDC) may be handling tens of millions of messages per second, across the entire network. The system must allow a single user to post, for example, a warning sign in the vicinity of a particular hazard. To manage these large-scale extremes, the system uses a tiered tree-like architecture. Each RSE is connected to a regional SDN via a backhaul link, and each SDN is connected to all other SDNs via a wide-band backbone network. Using this architecture, any RSE is accessible from any SDN, and this is a key feature of the scalability of the system, since any user connecting to the local SDN can interact with any RSE.

A typical SDN is expected to support about 1000 to 2000 RSEs, so, for a nationwide deployment there would be between 100 and 200 SDNs. The POC implementation of the system included 55 RSEs placed at various locations in the northwestern Detroit suburbs. These RSEs were linked to two different SDNs using a variety of different backhaul technologies. One SDN was located in Novi, Michigan, and the other was located in Herndon, Virginia. The Herndon facility also included an ENOC and the Certificate Authority (CA) required to support security functions. The POC implementation was thus a minimalist version of the national system architecture allowing the program to assess the operational behavior of the system as if it were a full-scaled deployment.

4.2 Concept of Operations

Conceptually, the system provides several core functions from which a suite of applications may be created. The POC system:

- Delivers broadcast messages from network providers to OBEs at specified geographic locations
- Delivers broadcast messages from local systems such as traffic signals or toll stations to OBEs at specified geographic locations
- Delivers broadcast messages between OBEs
- Collects data from OBEs and distributes topical information extracted from the data to network subscribers
- Provides OBEs access to remote private service providers, and this access can be carried over from one RSE to the next without disrupting the service
- Provides security functions to protect against attacks and to protect the privacy of the individual users.

As part of the overall VII program a set of approximately 100 use cases or applications were developed by various stakeholder groups. In general, these descriptions did not fully articulate the use cases in the context of the system, but they did provide insight into the needs and priorities of the various stakeholders. From this initial set, 20 use cases were expected to be available at the system's initial deployment and were identified and articulated in more detail. This group is known as the "Day-1 Use Cases."

Because developing and testing all 20 Day-1 Use Cases would have been impracticable, the POC program identified a subset of use cases that exercised the core functions, described previously. These were then implemented and tested in ways to assess both the functionality of the system and the baseline performance, under the assumption that, the system would provide these core functions in the same way regardless of the specific details of the application.

This report focuses on VIIC's developed and tested POC applications described in the following sections.

4.3 Dedicated Short Range Communications

The 75 MHz band in the 5.9 GHz frequency range allocated by the FCC offers significant data transfer capacity. However, to make use of this spectrum in a mobile environment required the development of new communications protocols. The core radio protocol used is based on the well-known IEEE 802.11a/b/g wireless Ethernet standard, often referred to as Wi-Fi. Because of the unique mobile environment, the IEEE 802.11a standard was modified to allow what is known as an "association-less" protocol, identified as IEEE 802.11p. This means that the system does not establish a conventional network with all of the mobile terminals as nodes, all of which know about each other. The reason this is not done is that the mobile terminals (OBEs in the POC) are entering and leaving the hot spot rapidly, and there is insufficient time available to set up a new network identity for each new arrival and inform all other nodes in the network before the network changes again, because a terminal has left, or a new one has arrived.

The higher levels of the protocol are defined in a suite of standards known as IEEE 1609 Wireless Access in Vehicular Environments (WAVE). This suite addresses security (IEEE P1609.2), networking and messaging (IEEE P1609.3), and channel management (IEEE P1609.4). In particular, IEEE P1609.3 defines a WAVE Short Message Protocol (WSMP) that allows a simple way for a terminal to send messages in the local vicinity.

The current DSRC standards divide up the 75 MHz spectrum into 10 MHz channels. This allows RSEs in local proximity of each other to provide services without causing interference. It also allows for use of existing commercial IEEE 802.11 radio components. Since it is critical for safety reasons to ensure that all terminals can hear each other, and because the standards developers did not want to assume the use of multiple radio receiver systems (or very wide-band receiver systems), a method for channel management was developed and described in IEEE's Standards, P1609.3 and P1609.4. The approach splits the use of channels into two time intervals called the Control Channel (CCH) interval and the Service Channel (SCH) interval. All terminals are required to monitor the CCH during the CCH interval. Provider terminals (typically RSEs) transmit a WAVE Service Advertisement (WSA) on the CCH during the CCH interval, and since all terminals are monitoring this channel at that time, they all receive the WSA. The WSA contains a list of the services that the provider will provide during the SCH interval along with the SCH channel number they will be using. If a device receives a WSA continuing a service of interest, the device will switch to the appropriate SCH during the SCH interval, and will make use of that service. Because all terminals are required to monitor the CCH during the CCH interval, all high priority safety messages are sent on the CCH during the CCH interval.

While somewhat more complex than typical protocols, DSRC achieves the unusual feat of administering communications resources in real time, assuring that critical safety messages will have top priority, but also allowing lower priority messages, both local messages and messages bound for distant servers, to simultaneously use the system.

4.4 Network Description

The infrastructure network is shown schematically in Figure 4-1.

The SDN is composed of interfaces to the Backbone (to other SDNs), the backhaul (to RSEs) and the Access Gateway (to Network Users), routing functions to properly direct messages traffic, and a set of core services.

The RSE is composed of the DSRC Radio subsystem, a routing function, and a set of proxy applications that extend the services residing at the SDN (described above) out to each RSE associated with that SDN.

The ENOC is used by system operators to control and manage the overall network and RSE suite.

The CA issues security credentials to elements of the system that require them. It also manages the overall security state of the system.

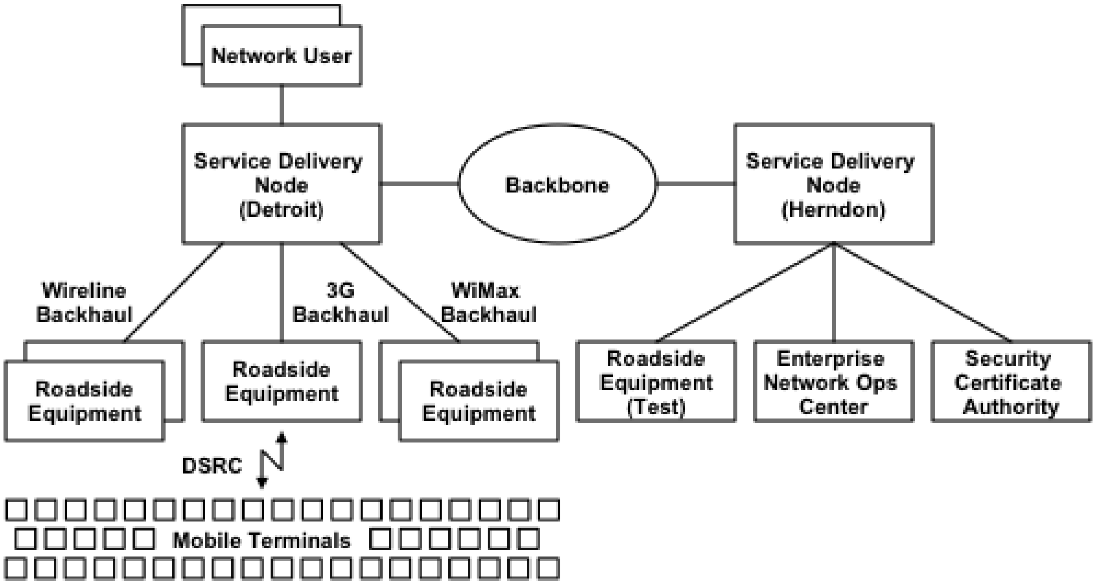

Network User
Service Delivery Node (Detroit)
Backbone
Service Delivery Node (Herndon)
Wireline Backhaul
3G Backhaul
WiMax Backhaul
Roadside Equipment
Roadside Equipment
Roadside Equipment
Roadside Equipment (Test)
Enterprise Network Ops Center
Security Certificate Authority
DSRC
Mobile Terminals

Figure 4-1 POC System Diagram

The POC network core services include:

Advisory Message Delivery Service (AMDS) accepts submitted messages from network users via the Access Gateway. These messages include delivery instructions such as RSE ID(s), repeat timing and message lifespan. The AMDS then passes these messages to the AMDS proxies resident in the appropriate RSEs for local broadcast to OBEs in the vicinity.

Probe Data Collection Service (PDCS) interacts with the Probe Data Proxy in the RSE to accept a stream of probe data messages gathered as OBEs pass the RSE. The PDCS then passes this data to the Probe Data Distribution Service.

Probe Data Distribution Service (PDDS) accepts a stream of probe data messages from the PDC. It then distributes elements of these messages to individual network users, based on the data parameters they have specified in their subscriptions.

Information Lookup Service (ILS) is a support service used by network users to determine information about the system. It is most often used to identify RSEs according to location, so that a subscriber or provider can then properly reference the RSE.

4.5 On-Board Equipment Description

The OBE is a self-contained computing system that supports a wide variety of applications and services.

As shown in Figure 4-2, the OBE uses shared services architecture. This means that key services expected to be used by most applications are provided as resources in the OBE. Any application needing these resources can then make use of them through simple software interfaces. Since many VII applications involve similar kinds of data and operations, the shared services approach avoids the need to implement these functions within each application.

The OBE implementation provides the following basic shared services:

Vehicle Interface provides a common referencing scheme and means for accessing vehicle data. Also allows the OBE to be used in a variety of vehicle types without needing to customize each application to interface with each vehicle type.

Positioning Services provides vehicle position and time information for applications, including notifications about geographic events.

Communications Management provides an interface between applications and security and DSRC Radio subsystems.

Security Services provides specialized security functions (signing, verification, encryption and decryption) for use directly by applications, and also for use on behalf of applications by the Communications Manager.

Human Machine Interface Management (HMI) arbitrates HMI resources between applications and provides a toolbox of graphical components to support user interface for applications.

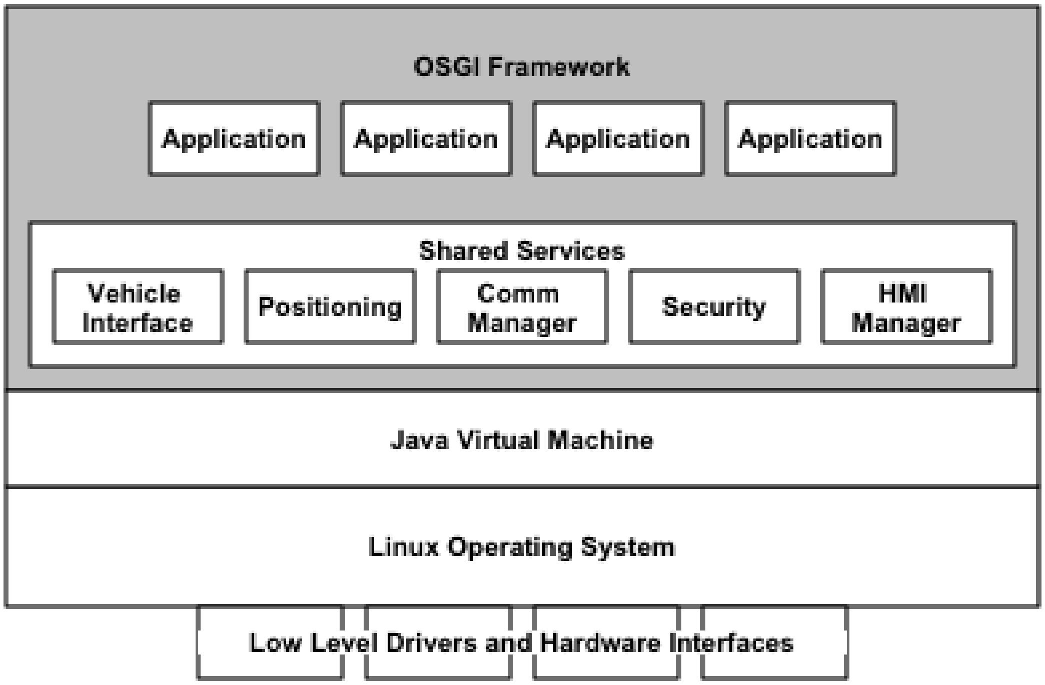


Figure 4-2 OBE Software Architecture

A typical OBE vehicle installation is shown in Figures 4-3, 4-4 and 4-5. This setup provides basic OBE functionality as well as power filtering and management, external Global Positioning System (GPS) and other interface components. As can be seen in Figure 4-4, the OBE includes a dash-mounted touch screen display system to provide information to the vehicle occupants. The dual purpose DSRC and GPS active antenna on a magnetic base is shown in Figure 4-5.

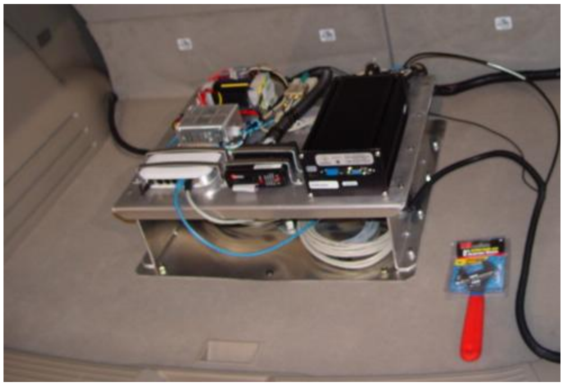


Figure 4-3 OBE Unit

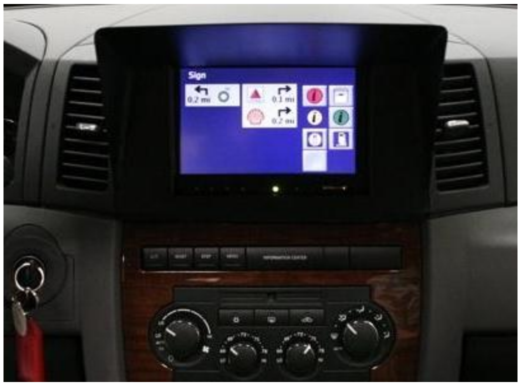


Figure 4-4 OBE Display

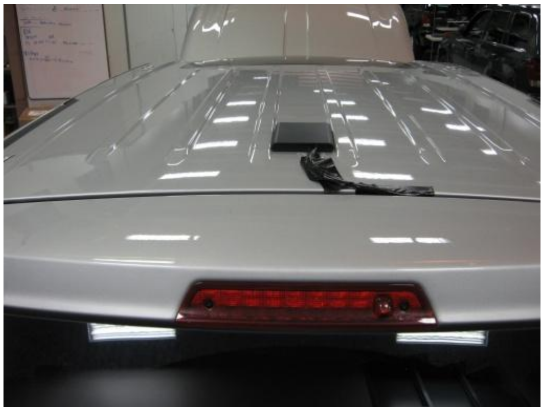


Figure 4-5 Dual Purpose Active Antenna

4.6 Application Description

The VIIC POC effort developed seven applications that used and exercised the core system functions. These applications are:

In-Vehicle Signage receives electronic advisory messages from roadside units, and, based on location and timing information, presents the message content in graphical and audible form using the OBE HMI.

Probe Data Collection gathers vehicle operating data from the vehicle interface and position location information from the Positioning Service, and compiles a “snapshot" of the vehicle state at that time, saves snapshots in a set and then uploads the snapshot set to the network-based PDCS when the vehicle encounters an RSE.

Electronic Payments-Toll sends out an announcement from the local processor via an RSE announcement containing toll plaza location information. When the OBE application determines it is inside the toll plaza zone, it obtains toll payment information and toll payment zone information from the local toll processor. When the vehicle enters a payment zone, the OBE application notifies the payment service, which sends a payment message to the local toll processor. All messaging relating to user identity and payments is encrypted and transactions occur at vehicle road speed.

Electronic Payments-Parking operates on same principles as tolling, but speeds are slower and payment and plaza zones are smaller and more complex.

Traveler Information/ Off-Board Navigation sends a request for a route from the current OBE location to a pre-set destination. Request is forwarded by a web services system to a navigation service provider, which computes the route including turn-by-turn directions. Directions are sent back to the OBE at the same RSE as the request is received. If delivery of the route is interrupted, for example, by the vehicle leaving the RSE zone before the route download is complete, then at the next RSE encountered the process starts where it left off. The route may also be updated based on real-time traffic data collected, for example, from the probe system.

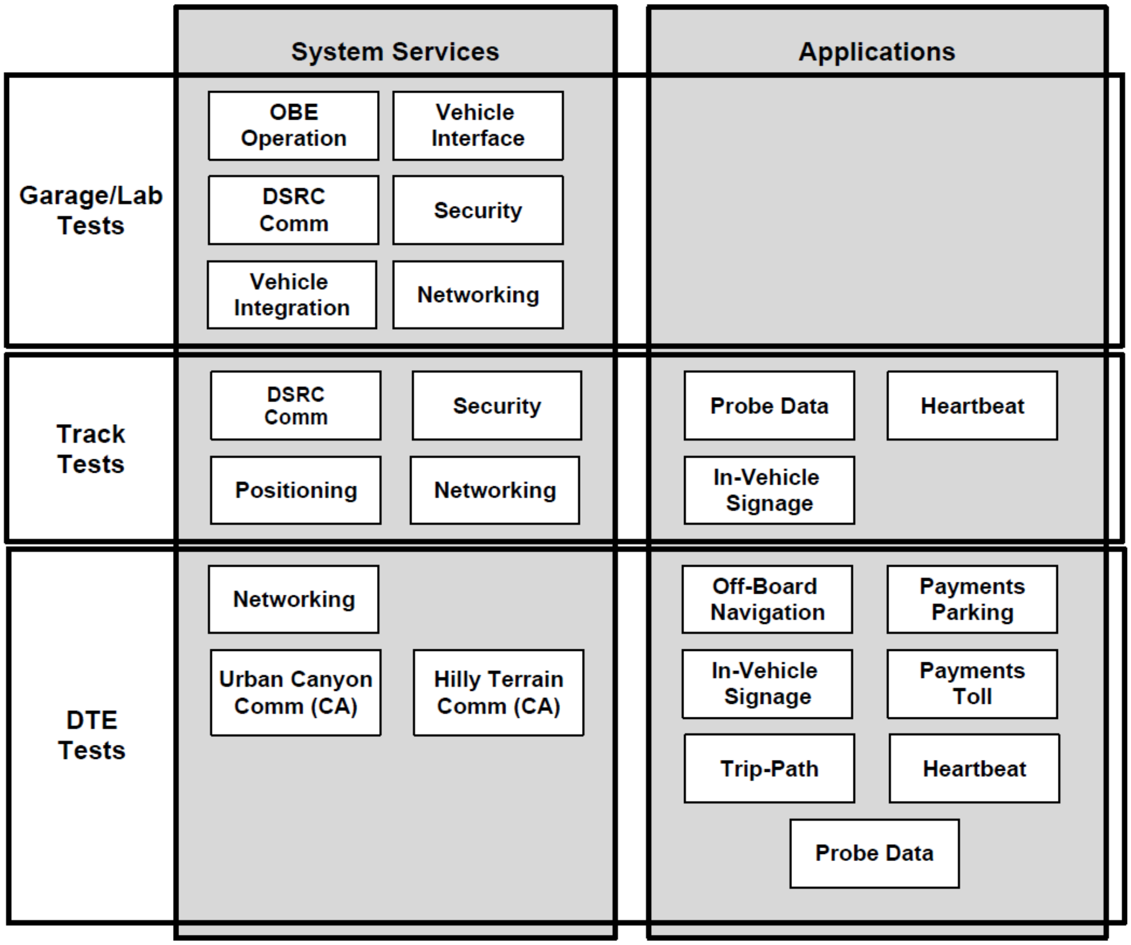
Heartbeat compiles a regular vehicle status message containing speed and position data; sending messages out at regular intervals (typically every 100 ms). Also receives the same type of message from other vehicles. Primary output is a log of sent and received messages (current application does not do any safety processing on the message). This application is primarily used to assess high message rate generation and reception.

Traffic Signal Indication is a stub application. A traffic signal controller sends a Signal Phase and Timing (SPAT) message to a local RSE at regular intervals. The RSE transmits the message, and the OBE receives it. The Traffic Signal Indication Application decodes the message and presents the current signal state and the time remaining in that state using the HMI display. This application is used to test the effectiveness of the system in handling and prioritizing safety messages while supporting lower priority operations.

4.7 Integration and Test Program

The system integration and test program was performed in three multi-phase segments. As shown in Figure 4-6, the OBE functionality and vehicle integration was initially tested in a garage/lab environment. This allowed rapid troubleshooting and early assessment of functionality. The system services were then tested in both laboratory and test track environments. This provided for detailed quantitative measurement of the capability and performance of these services. Some system services, for example, the DSRC communications, were also assessed in open road environments in California (hilly, curved roads and urban canyons). Detailed assessment of the POC applications began using the test track environment which allowed for early troubleshooting and refinement of the applications, and they were fully assessed in the open road DTE.

The Garage, Track and DTE segments were carried out in several phases, each of which built on the prior phases of all three segments.



	System Services	Applications
Garage/Lab Tests	OBE Operation Vehicle Interface DSRC Comm Security Vehicle Integration Networking	
Track Tests	DSRC Comm Security Positioning Networking	Probe Data Heartbeat In-Vehicle Signage
DTE Tests	Networking Urban Canyon Comm (CA) Hilly Terrain Comm (CA)	Off-Board Navigation Payments Parking In-Vehicle Signage Payments Toll Trip-Path Heartbeat Probe Data

Figure 4-6 System Integration and Test Approach

5 VII POC Program Key Findings

The POC testing generally indicates that the system performed all of the core functions (See Section 4.2) identified for the VII system. The program involved implementation and test of numerous features defined in the original VII architecture and resulted in the development of a significant knowledge-base related to feasibility and future implementation of these subsystems and features. The POC tests indicate that the system concept is technically feasible and performs well under most conditions. The tests clearly identified areas where performance can be improved, and areas where the concepts can be refined, but overall the POC development and system test results represent a significant step forward in achieving the original vision that VII may offer.

The sections below summarize the key findings gained from the variety of laboratory, track and on-road tests. These are laid out in terms of the specific system services to which they most closely relate. Commentary has also been provided to link these findings to the core operational objectives and viability criteria of the system.

5.1 System Services Key Findings

5.1.1 Communications Service

Communications Services were tested through a set of structured laboratory, test track and open road experiments.

Finding Number	*Finding*
COMM-1	DSRC range between taller vehicles (for example SUVs) and for V2I communications for all vehicle types is adequate and in many cases better than expected (Under best case antenna conditions <10% Packet Error Rate (PER) for ranges >800m for WSMP messages and >1000m for Universal Datagram Protocol (UDP) messages).
COMM-2	Range for V2V between low height vehicles (for example sedans) is not adequate (<100m at 90% PER), and appears to require antenna improvements. A 99%+ PER is achievable at ranges up to 50m for all vehicle types.
COMM-3	There is a consistent communications dropout between 100m and 300m range (about 50m wide) depending on the relative heights of the transmitter and receiver in open field environments. This appears to be due to multi-path fading and can probably be addressed using diversity antennas.
COMM-4	Highly complex environments (high multi-path) tend to reduce impact of two-ray multi-path fading. Urban canyons tend to improve Radio Frequency (RF) performance (range) and reduce effects of multi-path.
COMM-5	Antenna height from the ground has significant impact on range using the antenna design procured for the POC and is especially significant in V2V situations.
COMM-6	Antenna pattern and orientation has a significant impact on range, and appears to be quite sensitive to the vehicle installation and body configuration; this indicates that antenna design will need to be vehicle specific.

COMM-7	UDP/IP communications exhibit significantly better range vs. PER performance than WSMP. This appears to be because, in the applications tested, the UDP packets were addressed to a specific recipient (known as unicast transmission); this protocol includes low level packet acknowledgement, and retries transmission if no acknowledgement is received.
COMM-8	Range is not significantly dependent on the relative speed of the transmitter and receiver.
COMM-9	DSRC range is heavily dependent on line of sight; terrain effects are thus line of sight limited.
COMM-10	The PER of WSMP deteriorates progressively as message traffic (the number of messages being sent per second) increases (approximately linear relationship between frequency and PER). This appears to be due to a combination of packet collisions (packets sent at the same time, and the lack of packet retries described in COMM-7).
COMM-11	UDP does not exhibit significant PER dependence under message interference situations (presumably due to Medium Access Control (MAC) Layer retries).
COMM-12	WSMP Burst Error Rate (BER) (the number of times five or more packets in a row are lost) is much more sensitive to interference than UDP.
COMM-13	Radio channel throughput and channel capacity is better than expected, and appears adequate for expected applications.
COMM-14	Use of Internet Protocol Version 6 (IPv6) resulted in very effective Internet Protocol (IP) data operations, but newness of IPv6 limits equipment and software choices, and often results in complex work-arounds.

Table 2 Communications Service Test Results

5.1.2 Positioning Service

Positioning Services were tested during development and observed as part of many overall POC tests.

Finding Number	***Finding***
POS-1	Low cost GPS receivers, as used in the POC, are not capable of delivering <1m 95% Circular Error Probable (CEP) (best performance was about 4.5m 95% CEP).
POS-2	Augmentation, High Accuracy National Differential GPS (HANDGPS), did not improve position accuracy (generally made it worse). Appears to be due to limitations in commercial receivers that could not make use of these corrections.
POS-3	Dead reckoning and track smoothing (filtering) added significant errors (95% CEP 6-9m) in dynamic situations (curving roads). Appears that filters used do not make use of vehicle dynamics, and may use incorrect vehicle dynamic models.
POS-4	Dead reckoning serves to improve accuracy of the basic GPS receiver on straight roads (95% CEP 2-4m) (appears to be due to improved averaging of GPS position fixes).
POS-5	A commercial Wide Area Augmentation System (WAAS) receiver performed better than embedded units but did not have dead reckoning capability.

POS-6	Used without any GPS inputs, dead reckoning positioning maintains usable position accuracy over distances of up to 2 miles (distance traveled without GPS).

Table 3 Positioning Service Test Results

5.1.3 Security Service

Security Service operations were observed during testing of the security subsystem in lab and track tests.

Finding Number	***Finding***
SEC-1	Security system generally works as expected, but testing is difficult since all systems must operate properly. Security system has a tendency to be brittle in that any minor anomaly can cause it to prevent communications; although security system is functioning properly, it cannot always discriminate between other system anomalies or errors and false or malicious messages.
SEC-2	WSM verification works properly, but verification performance at higher rates could not be assessed due to operational issues with the OBE.
SEC-3	WSA Signing checks effectively ignore WSAs if out of geographic, time or operational scope; however, errors in position can lead to erroneously rejected messages.
SEC-4	Messages can be signed by system and successfully validated (or not) based on location, and time (message age); however, misalignment of OBE clocks can cause erroneous rejection of messages.
SEC-5	System can replace certificates (identified and anonymous) over the air during typical RSE encounters at road speeds.
SEC-6	System successfully rejects messages with expired or revoked credentials.
SEC-7	Anonymous certificate functionality (system to prevent the ability to track) was not measured (cost and schedule issues).
SEC-8	Certificate Revocation List (CRL) capability appears to be acceptable for moderately sized CRLs; the system was able to download CRLs with up to 30K entries at 65 mph past an RSE.
SEC-9	End-to-End encryption of IP packets using IEEE 1609 protocol was successful and operated at usable data rates.
SEC-10	Overall viability of anonymous authentication system needs to be refined to determine manageability and to refine management policies and processes.

Table 4 Security Service Test Results

5.1.4 Advisory Message Service

Advisory Message Service operations were observed during testing of the Signage Application in the DTE.

Finding Number	***Finding***
AMS-1	Most AMDS messages were received numerous times (often hundreds of times). The redundancy is due to the fact that the OBE DSRC Radio is required to visit the service channel, even if the service does not contain any new messages (a radio implementation shortcoming).

AMS-2	Observed multiple radio link disconnects at RSE coverage fringe areas. Appears due to omissions in the DSRC standard for multiple RSE arbitration, and resulting limitations of the POC radio implementation.
AMS-3	OBE received all messages sent when in the range of an RSE.
AMS-4	CCH messages included in WSA result in visits to the Service Channel, but the lack of any messages on the SCH results in the OBE quitting the service soon after it joins. This results in many rapid join/unjoin cycles. Appears to be due to limitations in RSE service setup process (See 5.1.7).
AMS-5	Observed some jitter in signage display due to positioning noise (vehicle position being reported inside and then outside activation zone).
AMS-6	Geographic and directional relevance were well addressed and proven in POC. Messages meant for one region or directions of travel were properly displayed (See AMS-8 and AMS-9).
AMS-7	Time relevance (OBE timeout) and Lifetime (RSE timeout) were not adequately defined or tested. It is unclear what specific circumstances should make a message disappear from an RSE, or be ignored as either out of date, or already received by the OBE.
AMS-8	Approach used to define and use directionality for messages is incorrect. Current approach is unnecessarily sensitive to variations in heading caused by measurement errors and road variations. Needs to be based on actual direction of road, not vehicle heading (e.g. “northbound” versus “north”).
AMS-9	Approach using polygons to define activation regions is prone to errors and ambiguities. Need to define a simpler and more robust approach to directionality and activation criteria.
AMS-10	Message relevance/activation (geographic and temporal) rules are not sufficiently defined to avoid ambiguity and problems from inadvertently old messages or variations in vehicle motion.
AMS-11	AMDS updates do not always "take.” Often requires multiple attempts to get message into playlist and send message. Appears to be an implementation flaw (See 5.1.7).
AMS-12	HMI prioritization scheme is complex and results in unexpected system operation at times. Thus, the system operator has difficulty configuring the system since competing priorities often conflict and, unless this is coordinated; it provides unexpected system behavior.

Table 5 Advisory Message Service Test Results

5.1.5 Probe Data Service

Probe Data Service operations were observed during testing of the Probe Data Application in the DTE.

Finding Number	***Finding***
PDS-1	VII-Datagram Transport Layer Security (V-DTLS) implementation (required to secure probe data messages) limits probe collection to one OBE at a time at any given RSE. This is an implementation limitation that can be fixed in the future.
PDS-2	Probe collection and privacy rules cause significant loss of probe data when the link fails, for example at long ranges (current rules require data to be deleted, and not re-sent to protect privacy).

PDS-3	Probe data transport from OBE to SDN is generally reliable and accurate (>90%).
PDS-4	Snapshot reliability (getting all snapshots within a Probe Sequence Number (PSN) group) is hampered by a combination of link reliability, radio join logic and V-DTLS blocking.
PDS-5	PDC consumes more Central Processing Unit (CPU) time than expected. This was partially attributed to non-optimized code.
PDS-6	Probe Data Subscription system appears to operate as expected.
PDS-7	Use of Probe Data Management (PDM) messages is problematic. The PDM causes state changes in the OBEs that receive it. There is no way to know which OBE is changed. If the OBE state doesn't revert back to some default over time, then it may cause instability in the rate of reporting, and since there is no geographic limit on the PDM effect, it may also cause rate conflicts as the OBE moves from one area to the next. There is currently no jurisdictional limitation to PDMs or their effect.

Table 6 Probe Data Service Test Results

5.1.6 Heartbeat Service

Heartbeat Service operations were observed during testing of the Heartbeat Application in the DTE and in a controlled environment.

Finding Number	*Finding*
HB-1	Appears that >99% Heartbeat message reliability within ±50m range can be achieved, and >90% reliability within 75m range. Range, at first reception, was better than expected (≈180m open road, no other vehicles).
HB-2	Existence of other vehicles reduces range significantly; however, occlusion from other large vehicles appears to place lower bound on useful range (≈ 70m).
HB-3	Range for crossing vehicles in intersection is better than expected (≈60m) with occluding buildings. Multi-path apparently allows moderate non-line-of sight communications.
HB-4	Average distance between vehicles when first Heartbeat received was not significantly different between congested traffic and free-flow traffic.

Table 7 Heartbeat Service Test Results

5.1.7 Network Management Service

Network management observations were made during the structured testing of applications in the DTE.

Finding Number	*Finding*
NMS-1	3G backhaul did not perform well under some situations due to limited bandwidth of 3G systems when many users are online.
NMS-2	WiMax backhaul was prone to interference and did not always perform well.
NMS-3	RSEs are generally able to be remotely managed; however, the units cannot be power cycled without a maintenance crew on site.

NMS-4	RSE service setup is complex and prone to errors (attributable to design that requires changing several data items in different places to add service).
NMS-5	Complex array of firewalls and tunnels results in a very difficult to manage system.
NMS-6	RSE Health Monitor System typically did not accurately reflect the real state of the RSE at any given time.

Table 8 Network Management Service Test Results

5.1.8 Network Enablers Service

Network Enablers Service operations were observed during testing of the Off-Board Navigation Application (OBNA) in the DTE.

Finding Number	*Finding*
ENA-1	Most routes (up to about 40 maneuvers) are able to be downloaded at single RSE encounter (faster than expected).
ENA-2	Routes over about 40 maneuvers often extend beyond RSE coverage.
ENA-3	Host Identity Protocol (HIP) effectively resumes session at next RSE encounter and allows migration of data transfer session from one RSE to the next.
ENA-4	Simple Internet Transition (SIT) Tunnels require care in setup due to Maximum Transmission Unit (MTU) restrictions and other IP setup details.
ENA-5	HIP requires new Ether type and this is not compatible with some conventional equipment.
ENA-6	Enterprise Service Bus (ESB) systems utilized in Web Service Architectures were found to be compatible with the intermittent connectivity of DSRC systems.
ENA-7	HIP should be part of the system, and not external to it, but this raises privacy protection issues.

Table 9 Network Enablers Service Test Results

5.2 System Core Requirements Findings Cross Reference

Core Requirement	Observed Examples
The system shall deliver broadcast messages from network providers to OBEs at specified geographic locations.	The system was shown to perform this function through numerous tests of the Advisory Message system, and through many of the DSRC, Positioning and Security tests. See Findings: COMM 1, 3, 4, 6, 7, 9-11, and 14; POS 1-6; SEC 3 and 4; AMS 1-11; and NMS 3-6.
The system shall deliver broadcast messages from local systems such as traffic signals or toll stations to OBEs at specified geographic locations.	The system was shown to perform this function through tests of the Tolling, Parking and Traffic Signal Indication Applications and the DSRC, Positioning and Security tests. See Findings: COMM 1, 3, 4, 6, 7, 9-11, and 14; POS 1-6; SEC 3 and NMS 3-6.

The system shall deliver broadcast messages between OBEs.	The system was shown to perform this function through tests of the Heartbeat Application and the DSRC, Positioning and Security tests. See Findings: COMM 2-7, 9-11, 13 and 14; POS 1-6; SEC 3 and 4 and HB 1-4.
The system shall collect data from OBEs and distribute topical information extracted from the data to network subscribers.	The system was shown to perform this function through tests of the Probe Data Applications and the DSRC, Positioning and Security tests. See Findings: COMM 1, 3, 4, 6-10, 12, and 14; POS 1-6; PDS 1-6 and NMS 1-6.
The system shall provide OBEs access to remote private service providers, and this access can be carried over from one RSE to the next without disrupting the service.	The system was shown to perform this function through tests of the OBNA and the DSRC, Positioning and Security tests. See Findings: COMM 1, 3, 4, 6-10, 12, and 14; POS 1-6; SEC 3; NMS 1-6 and ENA 1-7.
The system shall provide security functions to protect against attacks and to protect the privacy of the individual users.	The system has been designed to meet these criteria, as detailed in Section 5.1.3, Security Service Finding Numbers SEC 1-10. Further testing is still required to determine the ability of the system to protect privacy.

Table 10 System Core Requirements Findings Cross Reference

5.3 Viability Criteria – Key Findings Cross Reference

5.3.1 Safety

Viability Criteria	Viability Findings
Provides for infrastructure-initiated safety applications.	Demonstrated intersection collision avoidance functions, SPAT and Geographic Intersection Description (GID) using a traffic signal controller to produce signals transported by a system to vehicles.
Supports vehicle-initiated safety applications.	System supported V2V messaging to facilitate a variety of V2V safety functions. Safety benefits were not assessed.
Safety benefits are bi-directionally scalable (i.e. the benefits can be achieved by equipped vehicles at low levels of deployment penetration, and can be achieved at 100% deployment penetration levels).	Did not perform analysis to demonstrate or prove these criteria. However, system has been designed for scalability which should be the subject of further study.
Sufficient number of safety applications exist or have been described in sufficient detail to develop useful benefits assessments.	Did not perform analysis to demonstrate or prove this criterion. However many safety applications and their benefits have been described in related technical literature.

Table 11 Safety Viability Criteria

5.3.2 Mobility

Viability Criteria	Viability Findings
Provides for collection of various mobility data from vehicles.	Collected variety of static and event-based data from vehicles through the Probe Data Application.
Provides for use of collected mobility data by state and local authorities.	Demonstrated ability to deliver collected data on a topic-by-topic subscription basis to users.
Sufficient numbers of mobility applications exist or have been described in sufficient detail to develop useful benefits assessments.	Demonstrated PDC, Free Flow Tolling, and Signage. Some sample applications utilizing the probe data have been developed and demonstrate potential usage. Benefits have not been assessed.
Exhibits sufficient benefit in terms of road and traffic management and transportation efficiency.	Did not assess the benefit of the Mobility Applications as part of POC.

Table 12 Mobility Viability Criteria

5.3.3 Private Services

Viability Criteria	Viability Findings
Vehicles can access private services through system.	Demonstrated ability of system to support private services using web services paradigm. System is effective despite intermittent DSRC connectivity.
Private services can access vehicles through the system.	Services can access vehicles once vehicle has made contact with the network (to define its operating region in network).
Co-existence of private services with safety and mobility services is economically viable.	Initial multi-application testing indicates system supports this. However, radio implementation, and DSRC standards need to be improved for support-to-support situations with multiple RSEs and to improve applications/services prioritization.
Private services can be implemented in a manner that does not interfere with Safety and Mobility applications.	Initial multi-application testing indicates system supports this. However, Radio implementation and DSRC standards need to be improved to allow local dynamic applications state to be used to prioritize services. Specifically, if an application has already received and processed a message, its “local” priority should be lower (or zero) relative to a message that has not yet been received, even if the new message has a lower overall general priority level.

Table 13 Private Services Viability Criteria

5.3.4 Security

Viability Criteria	Viability Findings
Security compromises are fail-safe (cannot result in life threatening behaviors).	Security system appears slanted toward over-protection. The system has many security checks, and it is often possible to fail the checks because of simple inconsistencies between units (for example clock offsets, position errors, etc.). The current security scheme appears to have tolerances that are set a bit too tightly, for example, requiring microsecond synchronization of clocks to assure that messages are not being replayed.
System is resistant to denial of service, "replay" and intrusion attacks.	Not tested in POC, but used as a design parameter for security system. Risks to the system were assessed in a vulnerability analysis.
Security compromises can be identified and mitigated.	POC system demonstrated delivery of CRL, but did not address optimal distribution strategies. Network security management detected attacks and prevented intrusions during the course of POC development and testing. No formal testing of OBE attacks was performed.
Security credentials can be properly distributed and managed at all levels of deployment.	Demonstrated ability to anonymously deliver security credentials over the air. Approach uses scalable internet architecture for back-end.
Security Authorities and processes are established.	Created double-blind anonymous CA for POC.

Table 14 Security Viability Criteria

5.3.5 Privacy

Viability Criteria	Viability Findings
System provides effective safeguards to avoid use of privately collected data to be used to track a vehicle or to identify an individual vehicle as violating a traffic law.	System designed to support this objective. Testing in progress.
Cannot track an individual vehicle over any road segment longer than 2 km.	System designed to support this objective. Testing in progress.
Cannot identify any individual vehicle as violating a traffic law through publicly collected data.	System designed to support this objective. Testing in progress.
System's ability to protect consumer privacy can be clearly communicated to the public.	System design principles to protect consumer privacy adhered to. Not yet communicated to the public.

Table 15 Privacy Viability Criteria

5.3.6 Maintainability

Viability Criteria	Viability Findings
Added functionality over time can be deployed remotely across the system.	POC OBE was implemented using a remote service management system, although this feature was not directly tested over the air. System is functional, but system represents significant software overhead load, and is likely dependent on individual Original Equipment Manufacturer (OEM) implementation decisions.
RSE software can be remotely managed through network.	Demonstrated remote management of RSEs from ENOC.
VII-related vehicle software can be securely maintained over the vehicle life cycle.	Program priorities prevented addressing this criterion during the POC.

Table 16 Maintainability Viability Criteria

5.4 Implementation Related Findings

In addition to the findings described, which related directly to the system's ability to meet the objectives it was designed for, numerous implementation findings were identified. In general, these related to details of the application implementations, and limitations of the hardware, operating systems and software used to construct the POC systems that affected efficiency and speed of operation. These will need to be improved to make the system easier to use and to improve the overall performance of the system, but they do not relate to the fundamental ability of the system to meet its basic requirements. These findings are provided in more detail in the subsequent volumes of the VIIC Final Reports.

6 VII POC Program Recommendations

The section below outlines high-level observations regarding core elements of the VII systems and recommendations. These are provided in more detail in the subsequent volumes of the VIIC Final Reports.

6.1 Communications

In general, the VII POC Communications system met the basic requirements. However, the POC tests identified numerous shortcomings in the DSRC standards that need to be addressed. Most of these relate to the dynamic nature of the users in the roadway environment. It appears that the fact that the transmitters and receivers are in motion relative to each other was not adequately considered in the specification of the protocols. These limitations were apparent in nearly all of the POC application tests. Specifically, the DSRC standards and the resulting radio implementations need to be refined to include measures of signal quality, improved service decision logic (specifically UDP and IP based two-way transactions), improved management of the application state and arbitration of competing services from nearby providers (e.g., overlapping RSEs).

6.2 Positioning

Positioning functionality is required by user terminals in order to provide accurate state information (e.g., speed at a given location), so the system requirements need to impose some basic accuracy requirements on user devices to assure that data provided to the system or to other users is valid. However, the specific means by which this position determination is carried out should not be prescribed. This is especially important since some low cost terminals may not be able to include a GPS positioning system for economic reasons.

The positioning requirements must be significantly refined and extended to account for observed variations under static and dynamic conditions and to align the positioning accuracy with the types of expected applications that use position information.

While the system should not prescribe a particular positioning solution, it is apparent that significant development work needs to be performed in order to improve positioning accuracy and to assure accurate position availability under all expected operational situations. This work should address improvements in GPS solutions, but it should also include non-GPS schemes, multiple sensor systems (data fusion) and low cost relative positioning methods.

6.3 Network Enablers

The Network Enablers functionality is composed of two parts; 1) the function that allows users to migrate from one RSE to another while maintaining a service session, and 2) the web services back-end that allows multiple services to be combined easily and efficiently. The POC demonstrated that the web services approach is compatible with the dynamic vehicle environment where intermittent and somewhat short connectivity sessions are the norm. However, these systems are heavily dependent on the choices of the service providers, and, other than providing the knowledge that they are compatible with the system, no additional development work is required.

The session migration capability requires further consideration. In the original system requirements and system architecture, this capability was considered to be external to the system. This decision was primarily due to the need for protecting the privacy of users as they move a service session from one RSE to another. This is still a concern but the POC experience also indicates that this is a capability that the system must provide. Not requiring it means that it will be implemented in different ways by different providers and this will significantly complicate both the terminals and the data traffic.

As a result, it is recommended that the functionality associated with migrating service sessions between RSEs are included in the system requirements as a system function, so it is implemented in a consistent way across the system; but it is also imperative that such a function not have the capability to track a user. Such a competing set of requirements will either require additional security development work to create a scheme that operates as part of the system, but cannot be used by the system operators or their agents to track users, or it will require a common way of implementing these functions so that they are interoperable between different users.

6.4 Security

The Security system is a large parallel subsystem that was implemented in a “bare-bones” fashion on the POC program. The POC program demonstrated that the basic security functions can be implemented and can work in the context of the system. However, only a small amount of work was done to analyze the threats and understand how to identify and mitigate attacks. In addition, while an anonymous signing system was demonstrated, no work was done to demonstrate how such anonymous signatures can represent assurance that the terminal has not been altered in some way. The system implemented for the POC has known issues related to management of large-scale attacks. Work done on the POC indicates that the current concept can be refined to address these issues, but the detailed analysis and subsequent development work remains to be performed.

It is recommended that the anonymous signing scheme be further analyzed, simulated and refined to assure that the anonymous signatures are meaningful (that they certify the legitimacy of the terminal). This work should include development of a secure software provisioning system. The message signing and verification strategy used for high rate messages such as Heartbeats should be revisited and simulated to arrive at an optimal blend of security and system throughput. In addition, the work begun on the POC program to identify and mitigate attacks should be further extended and developed into an overall security management definition. Finally, the security implementations should be further refined and optimized and then the entire security system should be tested by third parties to assess its strength.

6.5 Advisory Message Delivery Services

The AMDS and associated OBE Signage Application performed well in the POC. The POC used simple geographic regions to activate signs, but the definition of these regions in the current concept of operations is complex, and it is not clear if this is the best way to manage activation of messages. In addition, the system is slightly unstable in terms of when messages actually appear at RSEs, and how persistent they are. The system operates well enough to demonstrate the concept, but it could be improved and made easier to use and be more robust. Section 5.1.4 describes these areas that can be refined.

It is recommended that the system be refined to improve how priorities should be interpreted in the context of other user activities (for example, should the message be displayed in the current circumstances?). The activation criteria (when is a message relevant?) needs to be significantly refined, and the overall management of the system in terms of properly setting configuration parameters and defining AMDS parameters must be automated so that erroneous combinations cannot occur.

6.6 Probe Data Service

The PDS was shown to work during the POC, but the concept is not particularly refined. It is not clear as of yet that collecting this volume of data from all vehicles is necessary (under most conditions messages sent from vehicles on the same roadway are heavily redundant), and the rules developed to maintain user privacy and prevent the availability to track are very complex. During POC, the slightly unreliable nature of radio communications coupled with the privacy rules imposed on the probe data system resulted in a significant difference in the amount of data collected in the vehicle and the amount of data that could be sent (under the privacy rules). It is likely that many of the Communications Services improvements described in Section 6.1 will alleviate some of the problems seen in the POC Probe system; however, since it represents a significant privacy and performance element of the system, the conceptual basis for the probe system also needs to be refined and better understood.

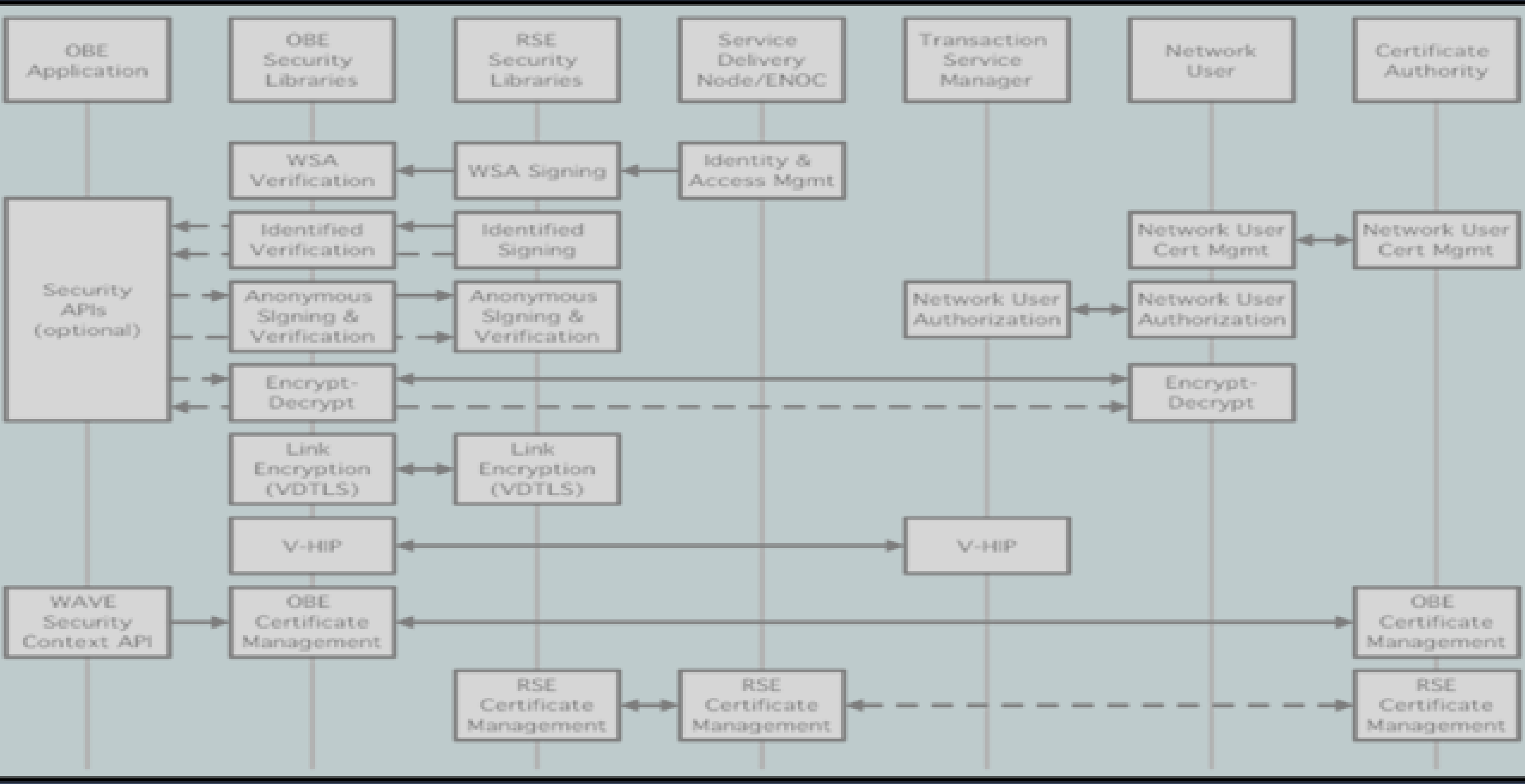
It is recommended that the probe data collected in the POC be analyzed and that representative models of probe data user applications be developed in order to assess the true mathematically relevant requirements on vehicle sampling density and scope of vehicle parameters sampled. This may include new concepts such as linking Heartbeat messages with the probe system to optimize the sampling of the roadway environment, while minimizing the total volume of data collected. The privacy rules associated with PDC need to be more fully integrated into the data collection strategy in order to better understand and control when PDC is and is not appropriate, and how this works given the existence of intermittent and not always reliable radio communications. In addition, the system data throughput and subscriber capacity needs to be assessed.

6.7 System Operations Management

The POC system and the system described by the VIIC and BAH National System Requirements provide a “bare-bones” approach for network users to interact with the system. Essentially, the ILS provides a mechanism for a user to query the system and identify which RSEs to use to make services or messages available in the system. This is an effective way to use the system, but it is very inefficient. For example, it is likely that many private network users (private service providers) will not care specifically which RSEs their services are provided from (the more the better), and it is equally likely that road management organizations will care about roads and intersections much more than about RSE identifiers. Clearly, the system as currently configured is usable, but it seems reasonable that simpler, more intuitive and more relevant interfaces should be available for service and data providers. This could be left to each road authority to develop independently, but since the basic needs of these users are quite similar, it seems that this system element could be improved to the benefit of all users.

In addition, the system has numerous configuration parameters at numerous points, and these parameters must all be properly configured for the system to operate properly. During the POC, incorrect configuration of these parameters resulted in unstable and unusable operation. When configured properly, the system works well, but as one user pointed out, “getting all of the stars aligned properly,” is not always a straightforward process.

It is recommended that the overall system operations be more fully automated and supported by better operator tools, so that the acceptable combinations of configurations are defined, and so that improper combinations cannot occur. In addition, the network management interfaces need to be improved to allow efficient and accurate setup of the system elements including firewalls and tunnels, and to allow operators to accurately see the operational state of the system at any moment by enhancements to the RSE Health Monitoring System.



EDL14443

FHWA - JPO- 09- 003