



VEHICLE INFRASTRUCTURE INTEGRATION (VII)

VII Architecture and Functional Requirements

Version 1.0

April 12, 2005
ITS Joint Program Office
US Department of Transportation

VEHICLE INFRASTRUCTURE INTEGRATION (VII)
VII Architecture and Functional Requirements

Draft

Prepared for the ITS Joint Program Office
by PB Farradyne
April 8th 2005

Table of Contents

VII Architecture and Functional Requirements.....	4
1. Executive Summary.....	4
2. Introduction	12
2.1. Background	12
2.2. Purpose of this Report	13
2.3. Structure of this Report.....	13
2.4. Related Work	14
2.4.1. The IVI Program	14
2.4.2. DSRC- FCC Allocation and Licensing and Prototyping.....	15
3. VII: The Big Picture.....	17
3.1. What is VII?	17
3.2. Who is involved in VII?.....	18
3.3. What are the Institutional Issues?	19
3.3.1. Customer Requirements.....	19
3.3.2. Security.....	20
3.3.3. Privacy	20
3.3.4. Data Ownership.....	20
4. VII Use Cases	21
4.1. Approach.....	21
4.2. Public Sector Applications	21
4.2.1. Safety.....	22
4.2.2. Operations.....	22
4.2.3. Maintenance.....	23
4.3. Public Sector Use Cases	23
4.4. OEM and Other Commercial Applications.....	24
4.5. OEM and Other Commercial Use Cases.....	25
4.6. Continuing Efforts	25
4.7. Consolidated Use Cases.....	26
5. Architectural Overview	29
5.1. Architectural Elements.....	29
5.2. Vehicle Data.....	30
5.3. Network Users	31
5.4. Data Quantity Problem	32
5.5. Communications Model.....	34
5.6. Dedicated Short Range Communications.....	35
5.7. Network Centric Approach	37
5.8. Publish and Subscribe Processes	38
6. On-Board Units and Equipment	40
6.1. OBU and OBE Introduction	40
6.2. OBU and OBE Functions	41
6.3. OBE Functional Requirements	42

6.3.1.	Local Safety Messaging	42
6.3.2.	Public Sector Messaging.....	42
6.3.3.	Private Sector Messaging.....	43
6.3.4.	Vehicle to Vehicle (V-V) Messaging	44
7.	Road Side Units and Equipment	45
7.1.	RSU and RSE Introduction	45
7.2.	RSE and Safety Applications.....	46
7.3.	RSE Registration and GPS.....	46
7.3.1.	Local Safety Applications	47
7.3.2.	Installation of RSEs	48
7.4.	RSE Operations and Support.....	48
7.4.1.	Update Service Table	50
7.4.2.	RSE Updates	50
7.4.3.	RSE Health Check	50
7.5.	Messaging With Vehicle	51
7.5.1.	Message Scheduling.....	51
7.5.2.	Receive Messages from OBU	52
7.5.3.	Send Message to OBU.....	52
7.5.4.	RSU Broadcast Messages	53
7.6.	RSU Networking	53
7.6.1.	Networking RSEs.....	53
7.6.2.	RSE Registering With System	53
7.6.3.	Formats Message for Publishing	54
8.	VII Message Switch.....	55
8.1.	VII Message Switch Introduction.....	55
8.2.	VII Message Switch Requirements.....	56
8.3.	Registration Requirements.....	57
9.	Mapping Requirements	58
9.1.	Mapping Introduction	58
9.2.	Mapping Data Flow from Probes	58
9.2.1.	Provisioning of Map Servers	59
9.3.	Map Servers Coverage.....	60
9.4.	Register	60
9.5.	Application.....	61
9.5.1.	Mapping Services.....	61
9.5.2.	Perform DGPS Correction.....	61
9.5.3.	Corrected GPS Locations	61
9.5.4.	Publish Map Correction Data	62
10.	Network Management.....	63
10.1.	Network Management Introduction.....	63
10.2.	Network Geographical Scope	63
10.3.	Network Management Requirements	63
10.4.	Management of the VII Network.....	64
10.5.	Communications Network.....	65

10.6.	Service Level Agreement	66
10.7.	Network Security	67
10.8.	Network Monitoring.....	67
10.9.	Provisioning of RSEs	68
10.10.	Provisioning of VII Message Switches.....	69
10.11.	Connectivity of Network Users	69
10.12.	Reports	70
11.	Network User	71
11.1.	Network User Introduction	71
11.2.	Network User Requirements	71
11.2.1.	Registration and Connectivity.....	71
11.2.2.	Subscription Control and Management.....	71
11.2.3.	Network User Data.....	71
11.2.4.	OBE Specific Messages.....	72
12.	Security.....	74
12.1.	Security Introduction.....	74
12.2.	Certification Authority	74
12.3.	Certificate Content	74
12.4.	Digital Signature in RSU	75
12.5.	Digital Signature in OBUs	75
12.6.	Certificate Revocation Lists	75
12.7.	OBU Physical Protection	75
12.8.	RSU Location Checking	75
12.9.	RSU Data Security.....	75
13.	Appendix A – VII Public Data Items from the Vehicle.....	77
14.	Appendix B VII Acronyms and Glossary.....	79
15.	Appendix C FHWA Vehicle Types	83
16.	Appendix D. Example Use Case.....	84

List of Figures

Figure 1-1	VII Architecture Overview	8
Figure 3-1	Highway Fatalities per 100 Million Vehicle-Miles for Selected Vehicle Types: 1992–2002	18
Figure 5-1	Simplified Architecture Data Flow.....	30
Figure 5-3	Flow from Vehicle to Application.....	33
Figure 5-4	DSRC Channel Allocation	35
Figure 5-5	DSRC Data Rate v Range.....	37
Figure 6-1	In-vehicle Elements	41
Figure 7-1	Roadside Equipment Logical Layout.....	47
Figure 9-1	Mapping and Positioning Process	60
Figure 11-1	VII Public Data Message Format.....	72
Figure 12-1	Asymmetric PKI Message Security.....	74

List of Tables

Table 4-1 Priority Public Sector Use Cases	24
Table 4-2 Consolidated Use Cases.....	27
Table 5-1 FCC Designated DSRC Channels.....	37

VII Architecture and Functional Requirements

1. Executive Summary

Purpose

Reducing the number and severity of surface transportation incidents is a top priority of the US Department of Transportation.¹ Development of a system supporting communication between vehicles and the surface transportation infrastructure has the potential for contributing significantly to the government's goal of promoting public safety. This report provides a description of work to date on the technical issues associated with Vehicle Infrastructure Integration (VII) using Dedicated Short Range Communication (DSRC) as a communications medium. It is recognized that there are other communications technologies in the industrial-scientific-medical frequency (ISM) bands that can support some VII functions. However, only 5.9 GHz DSRC can meet the safety requirements and have co-primary status within the licensed spectrum. This is a reasonably high level document and, as such, there are detailed design issues associated with VII that still need to be resolved.

This report describes the proposed VII DSRC system architecture and articulates, at a high level, the functional requirements of the system. It is intended to elicit responses from the various potential users and providers of the system and to stimulate discussion such that the various interested parties can come to agreement on the technical issues within VII. This report is about technical issues only; other related issues, such as potential business models and institutional issues such as privacy, data ownership, and security are being addressed elsewhere within the VII Program. This is a second draft and will be subject to multiple review cycles.

The VII Program

VII involves communication between individual vehicles, and between vehicles and the infrastructure enabling a variety of systems to be developed which significantly improve safety, operations and maintenance. It also enables a variety of applications to support the needs of the vehicle manufacturers and other private interests.

The VII program is a cooperative effort involving State Departments of Transportations (DOT) through the American Association of State and Highway Transportation Officials (AASHTO), local government agencies, vehicle manufacturers, and the US Department of Transportation (USDOT).

This report was prepared under a USDOT contract through which technical resources have been made available to help advance the VII program effort.

Related Work

In addition to the work reported on here, much related work is being conducted in parallel with the VII effort. This includes:

¹ [Federal Highway Administration, FY 2003 Performance and Accountability Report.](#)

- Dedicated Short Range Communications (DSRC) – There are several parallel sets of DSRC activities related to the VII effort. There has been an important sequence of activities related to frequency allocations from the Federal Communications Commission (FCC) watched closely by participants of the VII program. The USDOT has initiated the development of DSRC prototypes through the DSRC Industry Consortium (DIC) Prototype team that are to be built to the DSRC standards. Other related activities include DSRC standards being developed by the Institute of Electrical and Electronic Engineers (IEEE), the American Society for Testing and Materials (ASTM) and the Society of Automotive Engineers (SAE).
- The USDOT's Intelligent Vehicle Initiative (IVI) – The objectives of which are to prevent driver distraction and facilitate accelerated development and deployment of crash-avoidance systems.
- The Vehicle Safety Communications (VSC) project – A cooperative research projects in conjunction with a project between the USDOT and the Crash Collision Avoidance Metrics Partnership (CAMP) was establish to research and test the safety potential of 5.9 GHz DSRC. Collaborators were General Motors, Ford, Daimler-Chrysler, Toyota, Nissan, BMW and Volkswagen.
- The Enhanced Digital Map (EDMap) project was a three-year effort sponsored in part by the USDOT and launched in April 2001. The objective of EDMap was to develop and evaluate a range of digital map database enhancements that might enable or improve the performance of driver assistance systems under development or consideration by automakers. The partners in the EDMap project included automotive manufacturers DaimlerChrysler Research and Technology North America, Inc., Ford Motor Company, General Motors Corporation, Toyota Technical Center U.S.A., Inc., and map supplier, NAVTEQ. The project investigated various mapping approaches including traditional digitizing, survey vehicles equipped with differential GPS and computer vision systems, and the use of probe vehicles.
- The Federal Communications Commission (FCC) Rules have allocated the spectrum in the 5.9 GHz range. This is discussed in detail later in this report.
- The Vehicle Safety Communications (VSC) project was a thirty-one month effort sponsored in part by the USDOT and launched in May, 2002. Amongst the objectives of VSC was to evaluate various wireless protocols and safety applications, and create a body of research to serve as a foundation for DSRC at 5.9 GHz. wireless, automotive, active safety systems. The partners in the VSC project included automotive manufacturers BMW of North America LLC, DaimlerChrysler Research and Technology North America, Inc., Ford Motor Company, General Motors Corporation, Nissan Technical Center North America, Inc., Toyota Technical Center U.S.A., Inc., and Volkswagen of America, Inc.
- There are a wide variety of standards associated with the VII effort. Many of the teams working on differing elements of the VII design are active participants in IEEE, SAE, ISO and other standards organizations. Wherever feasible, existing or draft standards are being adopted for use within VII. However, the timescale of some standard development is longer than the available schedule for VII. In these cases preliminary draft standards may be used.

Approach

In the summer of 2003, the public sector VII participants focused on identifying applications that could take advantage of the vehicle sensor data that vehicle-infrastructure communications would enable. Beginning in the fall of 2003, the emphasis shifted to

analyzing the communications loads associated with transmission of the vehicle sensor data needed to support these safety, operations and maintenance applications. In order to conduct this communications analysis, a VII architecture concept had to be developed. It was then expanded and modified to accommodate transmission of data to support other applications involving local and Vehicle to Vehicle (V-V) communications using 5.9 GHz DSRC as a communications medium.

Requirements

The set of priority public sector applications was identified through a cooperative process involving representatives of the USDOT and various State DOTs. These are listed in the body of the report, and are more fully described in a report entitled, "Vehicle Infrastructure Integration (VII): Requirements Summary," dated April, 2004, and available from the USDOT's ITS Joint Program Office. A set of data elements, available from vehicle sensors, was identified as being needed to support these priority applications. The size of the data packet needed to accommodate the transmission of these data elements from a vehicle to the roadside was estimated.

In addition to the public sector applications the VII architecture could accommodate applications that support the needs of OEMs and other commercial parties, such as in-vehicle information services, monitoring of vehicle performance, processing of electronic payments, and many others. Separate work efforts, including the IVI and DSRC initiatives, have identified a broad range of these. A consolidated set drawn from the priority public sector applications identified through this work, and the IVI and DSRC initiatives, is presented in the body of the report. These are categorized as local and network applications. Local applications rely on communications between the vehicle and a specific location (e.g., an intersection). Network applications require connection to a communications network and a remote processing site such as a Transportation Operations Center (TOC).

It is likely that there will never be a single definitive set of VII applications because innovators will continue to think of new uses for the vehicle sensor data being communicated. The examination of potential VII applications performed to date has focused on estimating the general sizes of the data loads that would be communicated along various communications segments for public sector applications to determine the feasibility of the concept and to begin to define design parameters.

Vehicle Data

The multiple computers in modern cars have several hundred data types that can be accessed. However, there are two types of data that are of interest to the public users of the VII system:

- Periodic data – Information that is constantly changing such as speed and position. The vehicle will collect a series of samples of these data at regular time or distance intervals.
- Event data – Data that is of interest only occasionally and is of short duration, such as the deployment of an airbag system.

To standardize the format of data from the vehicle a 'snapshot' is proposed, incorporating both periodic and event data fields along with GPS time stamp and position data. When it is time to record periodic data or when an event of public interest occurs, the vehicle will fill in

the appropriate fields of the next snapshot. When the vehicle comes within range of an appropriate roadside unit (RSU), all stored snapshots are sent to the RSU from the vehicle and immediately forwarded to a VII Message Switch for subsequent dissemination. The VII Message Switch keeps the information for only the time necessary to determine and publish the data to subscribers.

Data Users

Seven general categories of public users have been identified. These were used to evaluate the likely size and frequency of queries that may be made. These categories together with example uses include:

- National users such as the USDOT monitoring major evacuations
- State TOCs collating data across their interstate system
- Regional TOCs providing data sharing across jurisdictional boundaries
- Individual City or State TOCs providing speed maps to web sites and using weather inputs for maintenance activities
- Local Safety Systems (LSS) at the roadside using precise vehicle data to warn of collisions
- Controllers and processors to provide input to adaptive signal control algorithms
- Other vehicles for vehicle-to-vehicle safety applications

The needs of the various users and the associated applications include both low latency applications (e.g., local and vehicle-to-vehicle safety applications where the allowable time that elapses between a stimulus and a required response is very low), and higher latency applications that typically involve the off-site aggregation and processing of data. This information was used by a communication model to investigate the bandwidth requirements for the public sector data.

Architectural Approach

The proposed architecture is a framework for information flow to the various system users. The scale of the data to be transmitted requires that it be a highly distributed architecture.

An analysis of the data communications loads associated with a worst case transmission of several snapshots of data under congested traffic conditions across a wide geographic area leads to the conclusion that there is too much data to store in a series of databases, and that it is being transmitted too frequently to write to a user friendly relational database. An approach where data is transmitted only by exception is not suitable because, for example, certain safety applications such as lane change warning systems require constant knowledge of the position of all vehicles.

These considerations led to an approach that involves an RSE (Roadside Equipment) communicating with an I/O controller in the immediate vicinity of the RSE to support local applications, and an RSE publishing its data to a VII Message Switch to support network applications. A network application is a system that is designed and maintained by a public or private entity that uses the data being provided by the VII System. Only a small fraction of the sensor data within the vehicle is transmitted to the RSUs (Roadside Unit) to support VII applications. The data needed to support the local applications is communicated and processed at the intersection to ensure low latency. Data needed to support the network applications is forwarded to a VII Message Switch. The VII Message Switch does little

processing beyond parsing out the vehicle data and sending it to Network Users who have subscribed to the data stream. It is the Network Users who will need to create network applications to use the data that they request.

Thus, the architecture can be described as network centric where its main function, like the Internet, is to provide a connection between a user and the data source with a minimum of interference.

The architecture is illustrated in the figure below

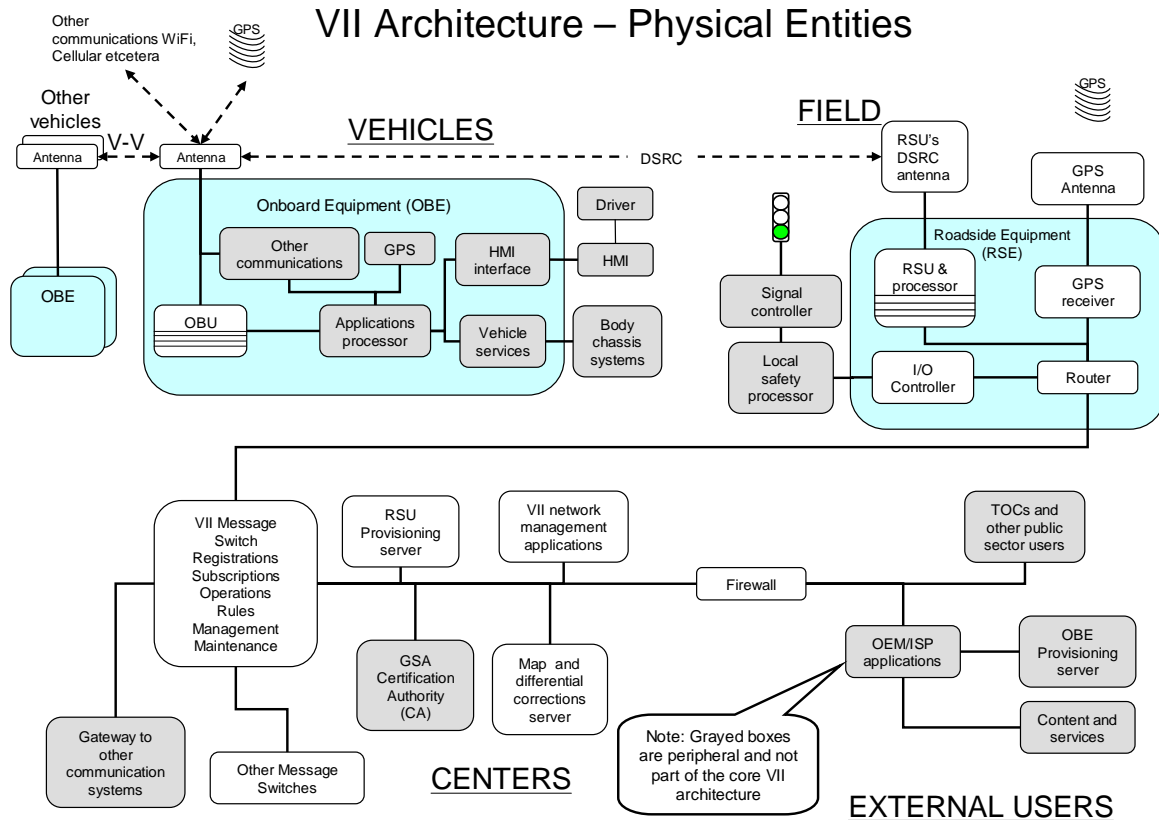


Figure 1-1 VII Architecture Overview

Architectural Boundaries

The architecture shown in the figure above includes peripheral elements that are not part of the architecture documented here. These peripheral elements are shown in grey either:

- Use the architecture - for example as a traffic operations center sending data to a group of vehicles, or
- Provide services – such as the provision of a certification authority to support secure messaging

These peripheral elements are not included in the requirements defined here.

The map and differential correction server elements are a borderline case. Although the differential correction data is likely to be derived from an external source such as the US Coast Guard the maps will be supplemented with probe data from the vehicles. The associated mapping requirements are part of the architecture and are included in this report.

The figure illustrates the general layout. It is too early to define quantities and locations of the various architectural elements. The OBU and its relationship with the various elements of the vehicle system is likely to vary between different auto makers and model types. In the RSE the local safety processor is kept separate from the RSU as this is likely to differ dependent on the safety application. Additionally there are expected to be many RSUs without local safety processors and providing standard units will help achieve economies of scale.

The Government Services Agency (GSA) currently provides digital certificates² and will act as the Certifying Authority (CA) for the VII system.

Communications Model and Analysis

A communications model, implemented as a spreadsheet, was developed to assist with developing an understanding of the requirements of the communications system needed to support the high latency network applications. The model was used to quantify, at a high level, the required bandwidths, for public sector use cases in order to determine the feasibility of using various technologies to meet these estimated loads.

The modeling analysis reflects numerous assumptions related to several model variables:

- Data elements available from vehicles
- Message data size
- Number of RSUs deployed
- Size of equipped vehicle fleet
- Peak RSE data loading
- Peak system data loading
- Frequencies of user data queries

The model used a set of default input values on the likely size and availability of data from vehicles. , It assumed peak traffic flows, market penetrations, and worst case scenarios for user demands. The modeling analysis indicates that, in general, demands for data for these network applications can be readily met with current technology.

DSRC

The DIC Prototype program generated an Applications Supported Document (DIC004) describing the parameters that the prototype units will support. The program also developed a reference³ stating that DSRC is a radio communications system intended to provide seamless, interoperable services to transportation. These services include those recognized by the US National Intelligent Transportation Systems (ITS), Architecture and Design

² <http://www.ntis.gov/products/pages/aces.asp>

³ IEEE P1609.3™/D04 Committee SCC32 of the IEEE Intelligent Transportation Systems Council Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services

Document (DIC006), and a Prototype Requirements Document (DIC005)⁴. They also include vehicle-to-roadside as well as vehicle-to-vehicle communications. Networking services provide addressing and routing services within and to DSRC devices as well as management services to all layers.

DSRC is a general purpose radio frequency communications link between the vehicle and the roadside. It is an enabling communications technology for many VII applications, and has been specifically designed to accommodate the security and latency requirements of vehicle safety applications. It is a member of the 802.11 family of communications protocols, identified as 802.11p

Standards for the DSRC communications link are being developed through the American Society for Testing and Materials (ASTM), the Institute of Electrical and Electronic Engineers (IEEE), and the Society of Automotive Engineers (SAE). Details related to channeling, control, public safety messages, transmission power, and frequencies are provided in their report. The Vehicle Safety Communications Project: Task 3 Final Report⁵ reported that DSRC is the only known communications medium that will support the safety applications of VII.

On-Board Equipment (OBEs)

The OBEs are the vehicle side of the VII system. In this document, references to the OBEs are used to describe the functions performed within the vehicle in addition to the radio transmission element. An OBE is logically composed of a 5.9 GHz DSRC transceiver (OBU), a GPS system, an applications processor and interfaces to vehicle systems and the vehicle's human machine interface (HMI). OBUs provide the communications both between the vehicles and the RSUs, and between the vehicle and other nearby vehicles. The OBUs may regularly transmit status messages to other OBUs to support safety applications between vehicles. At intervals, the OBEs may also gather data to support public applications. The OBEs will accommodate storage of many snapshots of data, depending upon its memory and communications capacity. After some period of time, the oldest data is overwritten. The OBEs also assemble vehicle data together with GPS data as a series of snapshots for transmission to the RSU.

Roadside Equipment (RSEs)

RSEs may be mounted at interchanges, intersections, and other locations providing the interface to vehicles within their range. An RSE is composed of a DSRC transceiver (RSU), an application processor, and interface to the VII communications network. It has a GPS unit attached. Through an additional interface, it may support local infrastructure safety applications. Using its interface to the VII communications network, it forwards probe data to the VII Message Switches.

The RSE may also manage the prioritization of messages to and from the vehicle. Although the OBE has priorities set within its applications, prioritization must also be set within the RSE to ensure that available bandwidth is not exceeded. Local and vehicle-to-vehicle safety applications have the highest priority; messages associated with various public and

⁴ Copies of these document can be obtained from Broady Cash of ARINC

⁵ *Vehicle Safety Communications Project: Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*; available from USDOT's ITS Joint Project Office.

private network applications have lower priority. Entertainment messages will likely have the lowest priority.

There are two types of Unit-to-Unit communications, the Internet Protocol (IP) datagram with IP version 6 addresses and the WAVE Short Messages (WSM) that are used to send datagram traffic without IP addresses. The WSM have a low latency (bypass the IP datagram message queue) and high priority channel access and are intended for transmission of safety related data traffic⁶.

There are seven channels for data exchanges that can be used to support VII. A Control Channel is used for application announcements (that is transmitting a Provider Service Tables (PST)) and for the WSM. All IP data traffic uses five of the Service Channels. The remaining channel is designated as High Availability Low Latency (HALL Channel) and used when very quick exchange of safety data traffic is required. This exchange can use IP datagram or WSM traffic⁷. In order to efficiently manage the operation of the several hundred thousand RSEs that may be deployed nationwide, RSEs will be equipped with GPS units. Upon connecting to the network, they register their position, network address, services provided, and requirements for publishing and subscribing to the VII Message Switch to which they are assigned.

VII Message Switch

The VII Message Switch is a pass-through for all of the data needed to support the network applications. Each VII Message Switch is connected to multiple RSEs, perhaps on the order of several thousand. Each VII Message Switch is also logically connected to all other VII Message Switches on the network. The data received by the VII Message Switch consists of all the data snapshots that were uploaded from the vehicles passing through an RSU communications zone for all of its assigned RSEs. Information in the VII Message Switch will be stored for only the time needed to publish it to those that have subscribed to the data. Network User applications with the proper level of security may subscribe to specific types of data from specific geographic locations. When the VII Message Switch receives data that fits the subscription criteria, the data will be published to that Network User.

VII Message Switches monitor the RSEs that are assigned to them, assuring that the RSE remains online. If an RSE drops offline, the associated subscriptions will be deleted. Subscriptions for its data will be reentered when the RSE rejoins the network. The VII Message Switch also performs message management functions, accommodating message priorities in accordance with network bandwidth. The VII Message Switch does not have any data storage capacity. There is no historical file or smoothing of data. Data storage and archiving is the responsibility of the subscribing Network User. Data to which there is no subscription terminates at the VII Message Switch.

Mapping Requirements

⁶ IEEE P1609.3™/D11 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services Sponsor Committee SCC32 of the IEEE Intelligent Transportation Systems Council

⁷ IEEE 1609.4 Medium Access Control (MAC) Extension & the MAC Extension Management Entity for DSRC 5.9 GHz – see www.ieee.org

For certain safety applications, for example, lane change warning systems, accurate positioning of the vehicle must be known and matched against a similarly accurate electronic map within the vehicle. This allows the vehicle to be located relative to its surroundings, including other vehicles.

Certain applications, such as electronic brake warning, require vehicle-positioning accuracies greater than that provided by the standard GPS (about 10 meters). Various Differential GPS (DGPS) systems can provide better accuracies (perhaps 1 meter or less by the time VII is implemented).

Maintaining the accuracy of map databases requires significant effort because of frequent changes, for example, when a construction zone is established. VII offers the potential to build accurate maps based on the collection of raw position data from a large number of vehicles connected to a Map Server through a VII Message Switch. Local maps are fed back to vehicles through the RSEs to keep the map information on all of the links to the next downstream RSEs maintained accurately.

Network Management and Security

The VII Network is the element that delivers data from the vehicle to the various Network Users, as well as data and updates from the Network Users to the vehicles. This network is made up of the RSE at the roadside, VII Message Switches, Certification Authorities (CA), Map Servers and Firewalls as well as the data communications infrastructure supporting communications between these elements and the Network Users. Management of the VII Network will be carried out centrally from VII Operations Center(s). The number and placement of these centers and hardware and software contained within will be a function of network traffic and redundancy requirements.

A VII Network Operations Entity will be responsible for management of the design, implementation, expansion, operations and maintenance of the VII Network. It is envisioned that this [non-profit] entity will consist of representatives from the USDOT, the various States and the OEMs. All messages on the network will be digitally signed, incorporating public and private keys issued by a CA. The system will maintain and publish revoked certificates so that all entities on and users of the system can verify that a particular message is from a valid source and can be trusted. All users must obtain authorization to access the system and the VII Network Operations Entity will determine their access privileges.

2. Introduction

2.1. Background

Reducing the number and severity of surface transportation incidents is a top priority of the Federal Highway Administration.⁸ Development of a system supporting communication between vehicles and the surface transportation infrastructure has the potential for contributing significantly to the government's goal of promoting public safety. To that end, the Vehicle Infrastructure Integration (VII) program is a cooperative effort involving State Departments of Transportations (DOTs) through the American Association of State and Highway Transportation Officials (AASHTO), local government transportation agencies,

⁸ [Federal Highway Administration, FY 2003 Performance and Accountability Report.](#)

Original Equipment Manufacturers (OEMs), and the US Department of Transportation (USDOT). The work of the VII program is governed by an Executive Leadership Team consisting of senior managers of the State DOTs, OEMs, and USDOT organizations. VII program work is planned and guided by a Working Group consisting of senior technical personnel of these organizations.

In the summer of 2003, much of the public sector effort related to VII was focused on identifying applications that could take advantage of the vehicle sensor data that vehicle-to-infrastructure communications would enable. Beginning in the fall of 2003, the emphasis of the work shifted to analyzing the communications loads associated with transmission of the vehicle sensor data needed to support certain public agency safety, operations and maintenance applications. In order to conduct this communications analysis, a VII architecture concept had to be developed.

The VII architecture continues to evolve from that initial formulation, which facilitated the communications analysis associated specifically with transmission of a block of vehicle sensor data of interest to the public sector to Transportation Operations Centers (TOCs) or other processing sites. In addition to this public interest, the VII architecture must accommodate safety applications, such as those identified through the USDOT's Intelligent Vehicle Initiative (IVI) program that require vehicle-to-vehicle communications, as well as commercial applications and technologies of interest to the OEMs and Content Service Providers (CSP). As the VII architecture continues to evolve, it is imperative that it reflects ongoing related commercial activities and the work efforts of the USDOT, the States, and their partner organizations.

2.2. Purpose of this Report

This VEHICLE INFRASTRUCTURE INTEGRATION (VII): VII Architecture and Functional Requirements report describes the work conducted since the fall of 2003 to develop the VII architecture concept and articulates, at a high level, the functional requirements of the system. It is intended to elicit responses from the various potential users and providers of the system. There are numerous detailed design issues associated with VII that are still to be resolved. This report is intended to stimulate discussion such that the various interested parties can come to agreement on the technical issues within VII.

This is a report about technical issues only. Other related issues, such as potential business models and institutional issues including privacy, data ownership, and security policies, are being addressed in parallel as part of the VII program. While this report touches on some of these latter institutional issues, it is only in the context of presenting the relevant requirements that the architecture must address.

2.3. Structure of this Report

This report describes the current concept of the VII system architecture, including how the primary entities or elements of the system are envisioned to interact and the associated functional requirements. Throughout this document specific defined requirements have been assigned an alphanumeric identification that includes an acronym identifying the relevant element. For example: the notation **{RSE 7}** refers to the 7th requirement relating to Roadside Equipment.

The remainder of the report consists of the following sections:

- **VII: The Big Picture** describes VII in terms of its intent, the major institutions and their interactions.
- **VII Use Cases** defines what VII will be used for in terms of a variety of use cases. These have been developed by various public sector agencies in addition to the OEMs. The level of development of the uses cases is only deep enough to produce high level requirements. A consolidated list of use cases has been developed that reflects the needs of both the public and private sector.
- **Architectural Overview** introduces the concept of vehicle data and what data elements may be used to support the use cases.
- **On Board Equipment (OBEs), Roadside Equipment (RSEs), and VII Message Switch** introduce the three primary physical elements and define their specific high level requirements.
- **Mapping Requirements** describes how lane accuracy positioning of the vehicle and a corresponding accuracy of maps in the vehicle may be obtained using the vehicles as probes.
- **Network Management** describes how the nationwide connectivity requirements need to be developed, operated and maintained.
- **Network User** deals with how the institutions that the VII System is designed to serve can access the VII Network.
- **Security** deals with necessary processes to ensure that messages are valid and that the best possible options are used to prevent, detect, mitigate, and recover from attacks on the system.

2.4. Related Work

Much related work has preceded and is being conducted in parallel with the VII effort. The following sections describe key results from two bodies of work that have impacted the evolution of the VII architectural concept.

2.4.1. The IVI Program

The focus of the USDOT's Intelligent Vehicle Initiative (IVI) program is to prevent crashes by helping drivers to avoid hazardous mistakes. The objectives of the program are to prevent driver distraction, and to facilitate accelerated development and deployment of crash-avoidance systems. A variety of partners, including the OEMs, are contributing to the program through cooperative agreements. Information on the IVI program can be found at: <http://www.its.dot.gov/ivi/ivi.htm>.

The IVI program has a cooperative agreement with the Crash Avoidance Metrics Partnership (CAMP). Under this structure the Vehicle Safety Communications Consortium (VSCC) was formed, comprising BMW of North America LLC, DaimlerChrysler Research and Technology North America Inc., Ford Motor Company, General Motors Corporation, Nissan Technical Center North America, Inc., Toyota Technical Center USA Inc., and Volkswagen of America, Inc. A project completed under the VSCC partnership resulted in the report Vehicle Safety Communications Project: Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC. This report is available from the USDOT's ITS Joint Program Office. The report identifies more than 75 application scenarios that were

analyzed, resulting in a final set of 34 safety and 11 non-safety application scenario descriptions. Preliminary communications requirements were developed for these application scenarios. The analysis identified Dedicated Short Range Communications (DSRC) as a potential enabler for a number of vehicle safety applications

2.4.2. DSRC- FCC Allocation and Licensing and Prototyping

DSRC is a wireless (radio) communications approach that enables short-range communications among vehicles, and between vehicles and the roadside for a variety of purposes. As suggested in the VSCC project report mentioned above, DSRC is a key enabling communications technology for many VII applications. An important sequence of activities related to the frequency allocation, licensing and prototyping of DSRC technologies is summarized below.

In October 1999, the Federal Communications Commission (FCC) allocated frequencies in the 5.9 GHz band for DSRC. Since then, an American Society for Testing and Materials (ASTM) standards committee has been working on developing the standards for DSRC use. ASTM approved the first DSRC standard for transportation, ASTM E2213-02, in May 2002 for layers 1 and 2, the physical and data link layers of the Open Systems Interconnection (OSI) model of network architecture. The committee is currently working on DSRC standards for the upper OSI layers in cooperation with the Institute of Electrical and Electronic Engineers (IEEE). The full title of ASTM E2213-02e1 is "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications." The standard extends IEEE 802.11a into the high-speed vehicle environment called "p". IEEE 802.11 is a standard governing wireless Local Area Networks (LANs). Basing 5.9 GHz, using DSRC, IEEE 802.11 allows expedited development of devices from available chip sets and promotes the interoperability of DSRC devices in wireless LAN environments. IEEE 1556 is the standard for security, IEEE 1609.1,3,and 4 are the standards for upper layer protocols, and IEEE 802.11p is the standard being developed to describe the Physical and Data link layer operation. The FCC rules currently require the use of ASTM 2213.

An overview of these standards can be found on the FHWA's website at: <http://www.its-standards.net> and at <http://www.astm.org/>

In a report released on August 3, 2004, the FCC adopted licensing and service rules for the DSRC in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850-5.925 GHz band (5.9 GHz band). The concept behind the licensing includes the notion that providing On-Board Units (OBUs) on all new motor vehicles will enable life saving applications. In addition, the report states that the allocated frequencies will be made available for both public safety and non-public safety uses. It is the intent that public safety activities will be the dominant use of the band and be given priority over private transmissions. The recommendation by the FCC, is that public safety and private users should share the band so that a larger overall market for DSRC devices and services will be created quickly.

Although the architecture described in this report uses DSRC for transmission of data between the infrastructure and the vehicle, there are many other available paths for the data. The use of the VII architecture does not limit the opportunities to make use of these services either separately or in conjunction with the VII system. For example, a request

could be sent from a vehicle over the DSRC link to a CSP who may respond to the request over a WiFi connection.

3. VII: The Big Picture

3.1. What is VII?

Several different trends and events have led to the realization that a potentially beneficial, communications-based relationship between vehicles and the transportation infrastructure is now technically feasible. More and more sensors are being implemented on vehicles for a variety of functions necessary for their efficient and safe operation. The safety benefit that could accrue from enabling real-time data communication between individual vehicles and between vehicles and the infrastructure is potentially very large.

Such communication between vehicles could be used to alert drivers to potential collisions in sufficient time to enable avoidance maneuvers. Communication between the vehicle and the infrastructure will enable a variety of systems to be developed to warn drivers of impending conflicts and of the status of devices such as traffic signal controllers.

Additionally, the transportation infrastructure and its various control systems suffer from a dearth of the real-time data needed for efficient operations. The ability for the infrastructure to read data from the vehicle sensors will greatly enhance transportation systems management and operations, including system maintenance functions. A link between the vehicle and the infrastructure will allow for traffic warning and data messages to be transmitted directly into all equipped vehicles.

A major safety difference that VII provides is the ability to affect accident rates rather than just mitigate the impact of the accidents. The cost of accidents is astonishing⁹. A comprehensive study released on May 9, 2002, by USDOT's National Highway Traffic Safety Administration (NHTSA) shows that the economic impact of motor vehicle crashes on America's roadways has reached \$230.6 billion per year, or an average of \$820 per year for every person living in the United States. The new report, based on calendar year 2000 data, calculates the U.S. economic costs of an average roadway fatality at \$977,000 and estimates the economic costs associated with a critically injured crash survivor at \$1.1 million. Current accident mitigation techniques are approaching an area of diminishing returns which is illustrated in the graph, below. VII has the potential to significantly reduce the occurrence of accidents by sharing real-time data, predicting potential conflicts and warning drivers accordingly. By reducing the number of collisions, VII is likely to be a highly cost-effective development.

⁹ USDOT Bureau of Transportation Statistics
http://www.bts.gov/publications/national_transportation_statistics/2004/html/table_02_03.html

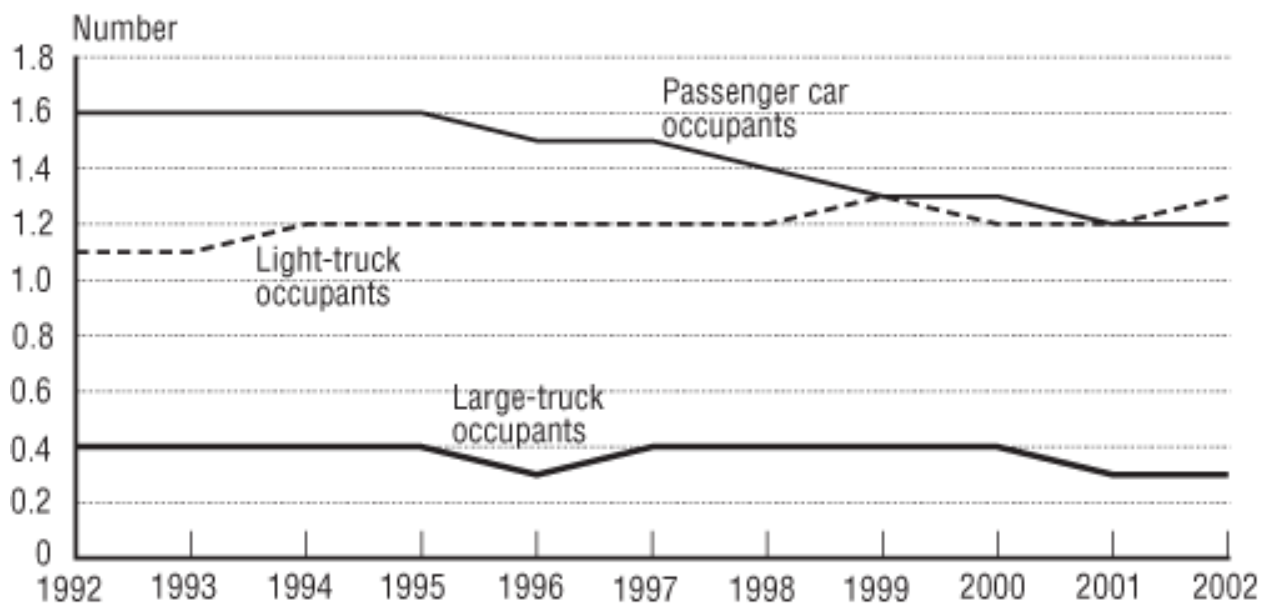


Figure 3-1 Highway Fatalities per 100 Million Vehicle-Miles for Selected Vehicle Types: 1992–2002¹⁰

3.2. Who is involved in VII?

VII has three principal user groups:

- **Drivers** will benefit from increased safety, the provision of traffic information and a range of other data services.
- The **OEMs or the automakers** will be able to perform diagnostics and updates in vehicles and provide new services to their customers.
- The **various DOTs** will be able to obtain vehicle sensor data in order to develop a comprehensive understanding of current road surface, weather, and traffic conditions, and to gather information such as road surface conditions. In addition they will be able to send messages to passing vehicles providing them timely and accurate information. Cities will be able to adopt adaptive signal control strategies that will reduce delay.

These three user groups have been the main players in VII to date. The system, however, is intended to support commercial activities as well. Consequently, other important players will necessarily become active participants as the program progresses:

- **Content Service Providers (CSPs)** will be able to provide information services such as financial transactions, entertainment, and other data services. It is possible that the CSPs will support some of the services that the OEMs want to provide to their customers.

¹⁰ Bureau Of Transportation Statistics
http://www.bts.gov/publications/transportation_statistics_annual_report/2004/html/chapter_02/figure_09_03.html

- The **Communications Industry** may provide the communications infrastructure that will transmit the vehicle sensor data that is being assembled at the roadside to various destinations for processing and response.

In this report, the principal players are referred to as members of the categories named above. These references should be considered generic; that is, drivers can include emergency service vehicles, DOTs can include cities and toll authorities, and CSPs may include institutions or companies such as OEMs that have a contractual arrangement with a CSP.

3.3. What are the Institutional Issues?

Through technical exchanges among the principal user groups who have been involved with VII to date, a number of principal themes that the VII system architecture and functional requirements must accommodate have emerged. These include:

- Customer Requirements – what kinds of applications will the VII system support and what are the priorities when there is contention for system resources?
- Security – how will the system secure data being transmitted on the system?
- Privacy – how will the system protect the privacy of drivers while at the same time allow private transactions between the driver or vehicle and OEMs?
- Data Ownership – what data will be in the public domain and what will be private?
- Certification and Registration – how will the system ensure that the devices communicating on the system are authorized?

3.3.1. Customer Requirements

The proposed system will support a wide range of applications that can occur both in vehicles and in the infrastructure. The system will support low latency applications that are intended to increase safety at intersections and between vehicles. These safety applications will have the highest priority both in access to the various processing capabilities and in their usage of the VII communication networks.

The VII system will also be designed to support low latency applications intended to support the operations and maintenance requirements of public agencies.

The system must also support the requirements of the Original Equipment Manufacturers (OEMs). Some of these applications may require multiple message transfers while one vehicle is within range of a single RSU.

The technology and FCC licensing allows for commercial applications, these are considered private transactions between the OEMs and the CSPs with the VII architecture having no knowledge of the content of such transactions. However, the architecture is designed to support such private transactions and to ensure they are kept so.

3.3.2. Security

The VII system will ensure, through encryption techniques, that the data transmitted is secure. All messages will be digitally signed, incorporating public and private keys issued by a Certification Authority (CA) run by the General Services Administration (GSA)¹¹. The GSA will maintain and publish revoked certificates so that all entities on and users of the system can verify that a particular message is from a valid source and can be trusted. All users must obtain authorization to access the system and the entity with operational responsibility for the VII system will determine their access privileges.

3.3.3. Privacy

The intent of the VII system is to ensure that the data being made available to the public sector shall avoid the identification of individual vehicles or drivers, and to make it impossible to trace data to individual vehicles. Transactions between the OEMs and their customers will be kept private and the VII system will have no facility to interpret or store these transactions.

3.3.4. Data Ownership

The VII system will support two types of data:

- Data that has no individual identifying characteristics that will be in the public domain.
- Data that is private between the OEMs and other Content Service Providers (CSPs) that will remain confidential from all public sector databases and systems. This data will be transmitted by the VII system infrastructure, but would remain inaccessible to all system users apart from the authorized sender and receiver. All users of the VII network must publish privacy policies that are in accordance with the overall VII policy guidelines.

¹¹ http://www.digsiqtrust.com/federal/aces_public.html

4. VII Use Cases

4.1. Approach

The process of developing the VII architecture concept began with a definition of high-level requirements in the form of use cases for a set of priority public sector applications. Use cases make up one element of a technique for capturing the functional requirements of a system. As defined in system engineering texts, a use case captures a goal-oriented set of interactions between external actors and the system under consideration. Actors are parties outside the system that interact with it; for example, system users.

Use cases capture who (actor) does what (interaction) with the system, for what purpose (goal) without dealing with the internal working of the system itself. A complete set of use cases specifies all the different ways to use the system, and therefore defines all behavior required of the system, bounding its scope.

Use cases are typically produced in a system development or programming context. In this situation, however, the task at hand was not to develop a system or software package. Rather, the intent was to identify the priority public sector applications, in order to determine the data available from vehicle sensors needed to support them, and in turn to provide a first order assessment of how much data would need to be communicated to support selected applications.

Once the set of public sector use cases was developed, a quantified analysis of the data flows through a national communications network needed to support certain public agency safety and operations applications was conducted. The purpose of this analysis was to refine the architectural concept as needed to accommodate the timely transmission of the volume of data anticipated. Consideration was then given to applications involving strictly localized communications (e.g., at a signalized intersection) and applications involving vehicle-to-vehicle (V-V) communications. Accommodation of these considerations was largely based upon technical exchanges with experts involved in the other work efforts described in Section 2.4 Related Work.

Currently not all use cases have been developed. Appendix D contains an expanded example of a use case entitled: Infrastructure-Based Curve Warning.

4.2. Public Sector Applications

The surface transportation public sector is concerned with three primary issues: safety, operations, and maintenance. These classes of applications for a VII system have driven the development of the VII effort from the public sector's perspective. While some safety applications require only localized communication, many of the crash, incident response, and other safety applications require data transmission to and from a TOC or other central processing site through a communications network. This also applies to other applications of interest to the public sector, including transportation systems management and operations, and roadway maintenance functions.

4.2.1. Safety

There is unanimous agreement that the primary motivation for VII is to improve highway safety. The majority of priority public sector applications fall under this category, and certain applications classified as ‘maintenance’ could reasonably be considered safety related. Safety applications in this paper shall include active safety warning system applications, crash and incident response applications, advance warnings of hazards, and data collection to improve traffic and roadway safety.

Active safety warning systems aim to prevent crashes by helping drivers to avoid hazardous mistakes. For example, warnings could be provided to drivers, through either roadside or in-vehicle displays, whenever it is determined that a potential signal violation may occur. This determination would be based upon speed, roadway condition, and location data available from the vehicle and other vehicles, as well as signal phase and timing information provided by the signal controller. Similarly, warnings could be provided to drivers regarding potential conflicts with opposing vehicles when left turning movements are intended, or to warn drivers that their speed must be reduced to safely traverse an impending curve.

Active safety warning system applications only require transmission of data among vehicles, local roadside units, and local safety systems. That is, the processing and data flow occurs within the local area of the intersection or roadway.

Crash and incident response applications take advantage of the potential of VII to help achieve the safety benefits associated with faster response and improved interagency cooperation. When a crash or incident occurs, its location could be communicated to a Public Service Answering Point (PSAP), or to a private service that communicates with the PSAP. When a crash is involved, the communication could contain data characterizing the nature and severity of the crash. En-route to a hospital, data on patient medical condition could be shared with appropriate organizations.

Other safety applications that can take advantage of data that could be made available through VII include provision of in-vehicle advance warnings of incidents, work zones and other hazardous situations, including approaching trains at highway/rail crossings; the transmission of information to assist in commercial vehicle safety inspections; the process of checking credentials and safety compliance; and emergency vehicle preemption at traffic signals.

VII may also be used to gather large quantities of position data from vehicles. It has been shown that this data can be used to derive very accurate map databases, which, in turn, may form the basis of active safety systems in the future, as positioning capability improves. This data can also be used to maintain and validate local maps for intersection safety systems and other infrastructure assisted systems.

4.2.2. Operations

Public agencies are constantly seeking ways of moving traffic more safely and efficiently. VII offers the promise of providing traffic managers with speed data that they can use to paint an accurate picture of current conditions on all freeway and major arterial routes.

Traffic managers need to be able to continuously monitor flow on a region’s freeways and major arterials to quickly detect unexpected traffic jams, including those associated with

incidents and work zone lane closures. They also need to provide advice regarding the status of the network to those planning trips and to those drivers already en-route. This may be accomplished through in-vehicle systems or Content Service Providers (CSPs). The capacity to do this becomes especially important when evacuations are necessitated by a major emergency event.

Other operations applications that could be supported with VII data include the provision of traffic signal priority to improve transit schedule adherence as well as improved management of public vehicle fleets and other mobile assets such as snow plows and emergency vehicles.

Another new area where VII can provide functionality is in traffic operations where systems do not perform incident detection on arterial streets because of the uncertainties associated with arterial street detector data. However, this function could be enabled by use of the proposed VII System data from vehicles serving as probes.

4.2.3. Maintenance

Highway agencies spend over \$2 billion annually on winter maintenance activities. Data gathered from sparsely placed weather stations could be substantially supplemented by data available from vehicles, such as light level, temperature, wiper activations, anti-lock brake (ABS) state and traction control usage. VII could provide such information in real-time, thus enabling agencies to mobilize and deploy weather and emergency response resources in a more cost effective manner. VII would enable highway maintenance managers to make more timely and cost effective decisions regarding road treatments and crew deployments, thus saving lives and preventing injuries while maximizing resource utilization.

4.3. Public Sector Use Cases

Based on the potential public sector safety, operations, and maintenance applications of VII, a cooperative effort of representatives of the USDOT and various State DOTs designated by AASHTO developed public sector use cases. Table 4-1 lists high priority use cases by classification. More detailed descriptions of the use cases may be found in the report Vehicle Infrastructure Integration (VII): Requirements Summary dated April, 2004. It is available from the USDOT's ITS Joint Program Office.

The priority public agency use cases do not describe in detail the use of the data after it arrives at another location such as a TOC. When the data arrives at such a location, local applications will make use of it for a variety of purposes. Interfaces with these various other applications will be required. It is impossible to predict all the various ways in which a public agency might process or share the data so the use cases focus on a high-level description of the flow of events and the implied data needs.

Table 4-1 Priority Public Sector Use Cases

<p>Safety Infrastructure-based Signalized Intersection Violation Warning Infrastructure-based Signalized Intersection Turn Conflict Warning Vehicle-based Signalized Intersection Violation Warning Infrastructure-based Curve Warning Crash Data to Public Service Answering Point Crash Data to TOC Advance Warning Information to Vehicles Highway Rail Intersection Commercial Vehicle Safety Data Commercial Vehicle Advisory Commercial Vehicle Electronic Clearance Emergency Vehicle Preemption at Traffic Signals</p> <p>Operations Vehicles as Traffic Probes Travel Time Data to Vehicles Transit Vehicle Priority at Traffic Signals Public Sector Vehicle Fleet/Mobile Device Asset Management Electronic Payment</p> <p>Maintenance Vehicle Probes Provide Weather Data Vehicle Probes Provide Road Surface Conditions Data</p>

4.4. OEM and Other Commercial Applications

Applications which a VII system would enable that have been presented thus far focus solely on applications/use cases thought to be of priority interest to the public sector. VII, however, would also enable the development of applications that would use vehicle sensor data to support the needs of OEMs and other commercial parties.

OEMs could install DSRC-capable OBUs that would enable vehicle safety applications that require communications with roadside devices. They could also use VII to establish direct communications with their customers in order to assess functionality of safety systems and their performances at a specific location, provide a variety of in-vehicle information services, to monitor vehicle performance for maintenance purposes, and even to assist in distributing vehicle safety recall notices.

By enabling the acquisition of data from and the transmission of information to vehicles, VII opens a wide array of commercial opportunities for the information services industry. Transactions such as processing of electronic payment for goods and services, downloading a movie, or providing travel information, present interesting opportunities for business relationships and sales. And because many of the applications require that the information be passed along a communications network from and to some processing site, VII also generates business opportunities for the communications industry.

4.5. OEM and Other Commercial Use Cases

A broad range of use cases has been defined through separate, but related work efforts. The Automotive Multimedia Interface Collaboration (AMI-C) is a non-profit corporation made up of motor vehicle manufacturers. Their objective is to enable consumers to safely use a wide variety of emerging media, computing, and communications devices in their vehicles by providing standardized interfaces. AMI-C has compiled a set of use cases that represent possible customer experiences in terms of in-vehicle multimedia functions and features. This document can be found at <http://www.ami-c.org>.

- Use cases are grouped in 19 categories: commerce, customer relationship management, emergency, entertainment, fleet management, guidance, home automation, information, messaging, mobile devices, customer preferences, productivity, security, service and maintenance, user interface, Bluetooth, intelligent transportation systems, and combination use cases. 80 high-level (generic) uses cases, and 72 lower-level use cases (with more specific ways of performing functions) are defined in the AMI-C compilation. Ten examples of high-level use cases that could take advantage of a VII communications infrastructure are:
 - Diagnose vehicle system faults
 - Sharing information between vehicles
 - Submitting vehicle transit data (for commercial fleets, car rentals, etc.)
 - Obtaining roadside (travel) information
 - Obtaining traffic information from a vehicle service provider
 - SmartCard access
 - Vehicle theft countermeasures
 - Activating home devices from vehicle
 - Food discovery and purchase
 - DVD movie rental at a service station

Another related body of work was the Vehicle Safety Communications Consortium (VSCC) developed by the Vehicle Safety Consortium (VSC). Based on a safety benefits analysis of the 34 safety applications,¹² eight high potential safety benefit cases were identified and more detailed communications requirements developed. Examples are listed below.

- Traffic signal violation warning
- Curve speed warning
- Emergency electronic brake lights
- Pre-crash warning
- Cooperative forward collision warning
- Left turn assistant
- Lane change warning
- Stop sign movement assistance

4.6. Continuing Efforts

Under the auspices of the VII Working Group, the Society of Automotive Engineers (SAE), and NHTSA, work continues on the definition, prioritization and refinement of use cases and

¹² *Vehicle Safety Communications Project: Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC*; available from USDOT's ITS Joint Program Office.

their development as the foundation for subsequent system engineering steps that help define and support the VII vision.

The OEMs are actively working on defining standard message sets within the Society of Automotive Engineers (SAE), to define use cases in more detail and determine standardized message sets to support them. Both OEM and public sector use cases have been consolidated in a master list¹³ that is used as a reference to support continuing efforts to realize VII.

4.7. Consolidated Use Cases

The table below contains a consolidated list of use cases drawn from three sources:

- The set of Priority Public Sector Applications listed above and described in the aforementioned Vehicle Infrastructure Integration (VII): Requirements Summary report.
- Through the IVI program as described in the previously referenced Vehicle Safety Communications Project: Task 3 Final Report; and
- The applications considered in the DSRC standards development process (as filed with the FCC).

The table categorizes these use cases into local or network applications. Local applications rely on communications between the vehicle and a specific location in the infrastructure, e.g., with a traffic signal controller at an intersection. The V-V applications identified by the IVI program have been listed within the category of local applications. Network applications do not require knowledge of the specific position of the vehicle at the time of the data exchange, and require connection to a communications network to send data to a TOC or other processing site. The table also provides a reference to the use cases as they are identified in the master list.

Obviously, there is considerable overlap in the use case sets developed under each of these efforts. Further, it is possible for use cases to appear in both the local and network categories. For instance, signal preemption can be done locally or through a network, depending on how the signal system is configured. The list contains 107 unique applications: 47 local applications and 68 network applications.

¹³ [VII Use Cases Final Draft 2005_3_17 on VII Working Group web site

Table 4-2 Consolidated Use Cases

LOCAL USE CASES	NETWORK USE CASES
<ul style="list-style-type: none"> • Infrastructure-based Signalized Intersection Violation Warning • Infrastructure-based Signalized Intersection Turn Conflict Warning • Vehicle-based Signalized Intersection Violation Warning • Infrastructure-based Curve Warning • Highway Rail Intersection- 	<ul style="list-style-type: none"> • Vehicles as Probes <ul style="list-style-type: none"> ○ Traffic information ○ Weather data ○ Road surface conditions data • Crash Data to Public Service Answering Point (PSAP)
<ul style="list-style-type: none"> • Emergency Vehicle Preemption at Traffic Signal • Emergency Vehicle at Scene Warning • Transit Vehicle Priority at Traffic Signal • Stop Sign Violation Warning • Stop Sign Movement Assistance • Pedestrian Crossing Information at Designated Intersections • Approaching Emergency Vehicle Warning • Post Crash Warning 	<ul style="list-style-type: none"> • Crash Data to Transportation Operations Center (TOC) • Advance Warning Information to Vehicles • Electronic Payment <ul style="list-style-type: none"> ○ Toll collection ○ Gas payment ○ Drive-thru payment ○ Parking lot payment
<ul style="list-style-type: none"> • Low Parking Structure Warning • Wrong Way Driver Warning • Low Bridge Warning • Emergency Electronic Brake Lights • Visibility Enhancer • Cooperative Vehicle-Highway Automation System 	<ul style="list-style-type: none"> • Public Sector Vehicle Fleet/Mobile Device Asset Management • Commercial Vehicle Electronic Clearance • Commercial Vehicle Safety Data • Commercial Vehicle Advisory • Unique Commercial Vehicle Fleet Management • Commercial Vehicle Truck Stop Data Transfer • Low Bridge Alternate Routing
<ul style="list-style-type: none"> • Pre-Crash Sensing • Free-Flow Tolling • Cooperative Glare Reduction • Adaptive Headlight Aiming • Adaptive Drivetrain Management • GPS Correction • In-vehicle Signing <ul style="list-style-type: none"> ○ Work Zone Warning ○ Highway/Rail Intersection Warning 	<ul style="list-style-type: none"> • Weigh Station Clearance • Cargo Tracking • Approaching Emergency Vehicle Warning • Emergency Vehicle Signal Preemption • SOS Services • Post Crash Warning • In-vehicle AMBER Alert • Safety Recall • Just-in-Time Repair Notification • Visibility Enhancer • Cooperative Vehicle-Highway Automation System
<ul style="list-style-type: none"> • Vehicle-to-Vehicle <ul style="list-style-type: none"> ○ Cooperative Forward Collision Warning ○ Cooperative Adaptive Cruise Control ○ Blind Spot Warning ○ Blind Merge Warning ○ Highway Merge Assistant ○ Cooperative Collision Warning ○ Lane Change Warning ○ Road Condition Warning ○ Road Feature Notification 	<ul style="list-style-type: none"> • Cooperative Adaptive Cruise Control • Road Condition Warning • Intelligent On-Ramp Metering • Intelligent Traffic Flow • Adaptive Headlight Aiming • Adaptive Drivetrain Management • Enhanced Route Guidance and Navigation <ul style="list-style-type: none"> ○ Point of Interest Notification ○ Food Discovery and payment ○ Map Downloads and Updates ○ Location-based shopping/advertising ○ In-route Hotel Reservation
<ul style="list-style-type: none"> • Rollover Warning (see curve warning above) • Instant Messaging • Driver's Daily Log • Safety Event Recorder • Icy Bridge Warning • Lane Departure-inadvertent • Emergency Vehicle Initiated Traffic Pattern Change • Parking Spot Locator • Speed Limit Assistant 	<ul style="list-style-type: none"> • Traffic Information <ul style="list-style-type: none"> ○ Work Zone Warning ○ Incident ○ Travel Time • Off-Board Navigation • Mainline Screening • On-Board Safety Data Transfer • Vehicle Safety Inspection • Transit Vehicle Data Transfer (gate) • Transit Vehicle Signal Priority • Emergency Vehicle Video Relay • Transit Vehicle Data Transfer (yard)

LOCAL USE CASES	NETWORK USE CASES
	<ul style="list-style-type: none"> • Transit Vehicle Refueling • Download Data to Support Public Transportation • Access Control • Data Transfer <ul style="list-style-type: none"> ○ Diagnostic Data ○ Repair-Service Record ○ Vehicle Computer Program Updates ○ Map Data Updates ○ Rental Car Processing ○ Video/Movie downloads ○ Media Downloads ○ Internet Audio/video • Locomotive Fuel Monitoring • Locomotive Data Transfer • Border Crossing Management • Stolen Vehicle Tracking

Further development of the VII architecture needs to ensure that the local and network data transmission requirements associated with both public sector and OEM and other commercial applications can be accommodated. However, it must be recognized that there will likely never be a single definitive list because innovators will continue to conceptualize and develop new applications for the data that VII can provide. No rigorous analysis has been performed of the communications requirements associated with the consolidated list presented above. Instead, the examination of potential VII applications performed to date has focused on estimating the general sizes of the data loads that would be communicated along various communications segments of the VII architecture in order to examine the feasibility of the concept, and to begin to define design parameters.

5. Architectural Overview

This chapter describes the type of data that is envisaged to flow through the VII system. The estimates of the data requirements that are needed for the public sector are easier to formulate than those of the private sector as they are better defined at this time. The architecture proposed, however, is intended to support all users.

The proposed architecture is highly distributed. The scale of the data requires distribution, and the approach minimizes the communication loads between the various elements. This distribution of functionality applies to all the external applications that wish to make use of the data. The architecture described provides a framework for the information to flow to the user.

5.1. Architectural Elements

Considering the applications and use cases identified for VII it becomes clear that there are several key architectural elements involved with the system.

- The vehicle, and its onboard systems, is the source of data supporting many of the public sector use cases. It also provides the human machine interface (HMI) for conveying information to the driver, a key system element, from both public and private data providers. An onboard unit (OBU) in the vehicle allows communication with entities outside of the vehicle.
- Communications links provide the means for transmitting information to and from the vehicle. DSRC is a key enabling communications technology for the short-range communications needs of many of the VII applications. Other types of communications may also be used.
- A network of Roadside Equipment (RSE), placed strategically across the country, provides data collection and dissemination points. Placed at intersections or other high-risk locations, they may be connected to local safety applications, traffic signal controllers, and ITS devices such as signs or warning beacons.
- The external applications of public network users, who, want to receive data from the vehicle to support their applications. They may also want to send information to drivers, such as safety-related warnings or traveler advisories. Private or commercial users also want to be able to provide new services to their customers.
- A telecommunications network supports the data flow among all users. Multiple message switches distribute the communications load needed to route all the information. A VII Network Operations Entity, expected to be managed by an oversight group representing both public and private interests, will have responsibility for and authority over network configuration, management and maintenance as well as access by users.

The information flow within VII can be simplified as shown in the diagram below.

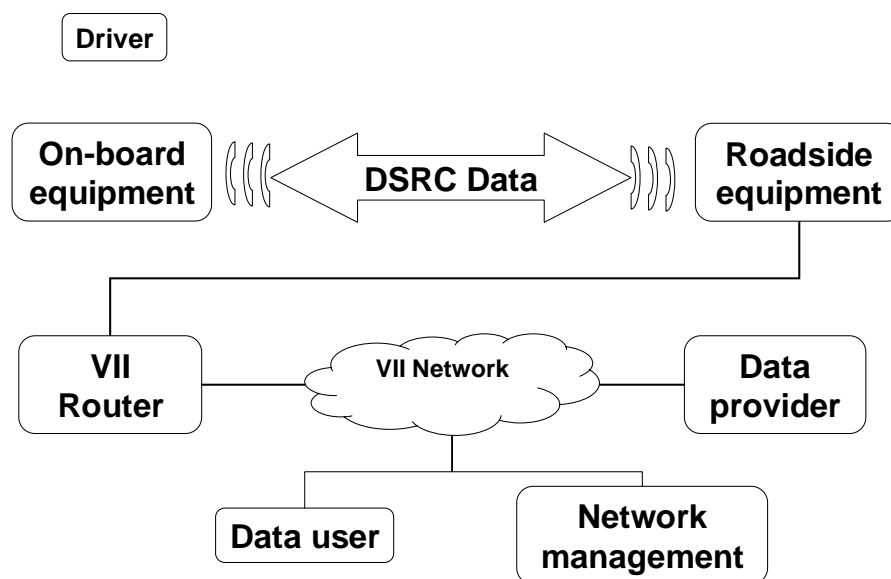


Figure 5-1 Simplified Architecture Data Flow

The OBU will collect and store a series of data elements on a regular basis. When the OBU is within range of an RSU, the data will be sent to the RSU, which will forward the data to a VII Message Switch that will distribute the information over a network to all users of the data. The VII network consists of a series of communication paths, hubs and routers that provide connectivity between the message switches and the users. The OBU will also communicate with both other vehicles and the roadside unit to support a variety of safety applications. Data providers such as Traffic Operations Centers will be able to send messages to the drivers warning of traffic conditions. Cities and states will be able to gather the data from RSUs to support their operational needs.

5.2. Vehicle Data

The body of AMI-C work includes a variety of documents describing the very wide range of data types that either currently or eventually will exist in the vehicle. Most of these are not of use to the public sector applications that the VII architecture is intended to support. There are two types of data that can be used to support the public use cases defined earlier: periodic data and event data. Periodic data includes information that is constantly changing, such as speed and position. Event data only occurs occasionally and is over a short period, an example of which would be the activation of an antilock braking system. These periodic and event data would be combined to create a probe data message.

To support the safety systems and use cases, VII requires more data than can be collected within direct range of the various RSUs. In order to extend the reach of data collection, it is proposed that the vehicle will take snapshots of its probe data and keep a certain number of the latest snapshots for uploading to the next RSU it encounters.

The data elements identified as being needed to support the priority public sector applications are shown in appendix A.

These vehicle data categories are not yet definitive, nor is it known which model year will incorporate each of the appropriate sensors and systems. However, it is understood from various OEMs that the plans for new features do include some subset of the data elements on the list.

Each vehicle will be equipped with a GPS receiver. To meet the safety requirements, the vehicle must know where it is and have the ability to send and receive this data between itself and other vehicles, and itself and RSUs. (The issue of maps and positional accuracy is addressed later.) The OBE or other systems within the vehicle will likely be equipped with alternate communication devices that support additional communication links.

The GPS unit within the vehicle is likely to not require a differential unit. . It is the intent that the GPS correction signal will be sent over the DSRC connection thus simplifying the device within the vehicle. The HMI systems of the vehicle are under development by a wide range of institutions and auto manufacturers. Audible, visual and tactile interfaces are all being investigated.

5.3. Network Users

From the public sector viewpoint there are seven categories of Network Users of the data:

- National – These include those institutions that may wish to obtain information from a data set larger than one state, and possibly of all states. For example, those institutions that track hurricanes and other natural disasters may wish to monitor traffic across a wide area.
- State TOC – The Traffic Operations Center (TOC) of a state would have the capability to monitor major traffic flows and weather movements.
- Regional TOC – Would perform similar operations to the State with more emphasis on controlling and monitoring their management devices; several regional TOCs may cover more than one State.
- Local TOC – Would be on alert for accidents and dealing with operational problems, possibly including arterial control on local streets
- Local Safety Systems – This is a category of user similar to a traffic signal on-street master controller that would monitor a local network of controllers and develop adaptive timing plans and search for incidents.
- Local controllers and processors – These include the local controller that may perform features such as signal preemption and also processors that will perform the various safety functions at the intersection such as intersection warning.
- Other vehicles – There are a range of these applications described in the earlier referenced VSCC report. Other vehicles are considered network users as use cases such as infrastructure based collision warning transfers data between vehicles through the RSE

The public sector users were categorized in this manner in order to evaluate the likely size and frequency of inquiries that may be made of the VII system. In the communications modeling analysis, estimates were made of the type and frequency of inquiry for each user category. This process developed the estimates for the communication loading and processor size.

The driving force behind the VII effort is the safety applications. The active safety warning applications must be performed in the vehicle, between vehicles, and at the roadside controller level. This is necessary as the system latency requirement (the time that elapses between a stimulus and the response to it) is very low. The relative motion of the vehicle dictates that the time period between actions is short – a vehicle at 60 mph moves about an inch in a millisecond. Thus, if actions have to be taken within a few feet, responses need to be fast. This need for low system latency is a common factor in the active safety warning applications. These applications are performed either in the vehicle or at the intersection to ensure the timely transmission of data.

An example of a low latency application that could work with a little higher response time would be traffic signal preemption. A vehicle with an OBU requesting preemption would send the information to the RSU; the RSE would contact the local safety system, which would in turn communicate with the local signal controller. The local signal controller would then respond by calling a preemption phase and sending an acknowledgement back to the RSE by the same route. The RSU would then forward this back to the vehicle, which would indicate to the driver that the call was successful.

At the next level of users, such as the various TOCs, the uses of the data allow for a higher latency. For example, for the map display on a web site that shows traffic data, latencies of tens of seconds is acceptable. For operational data where information is displayed to the driver, latencies of a minute are acceptable, since for some displays, such as messages to drivers, it is desirable to avoid changing the information too frequently.

Other users such as planning departments developing traffic pattern data from vehicle movements may consider even longer latencies acceptable. In these cases, the users may wish to collect data from selected geographic locations, archive it, and then analyze the files at their leisure.

This wide variation in users, their needs, and required latency drives the architecture to have two elements:

- Low system latency applications that need to take place between the vehicles and at the controller and RSU on the side of the road, and
- Higher system latency functions that typically aggregate data and can be performed at locations away from the roadside.

5.4. Data Quantity Problem

The use of a database structure for the VII is impractical because of the large amounts of data. Reasonable assumptions on the size of each message, the number of messages, and the number of RSUs result in a total data flow of several Gigabits. Not all RSUs will have this flow and the peaks will occur at different times; consequently, the information could be spread across multiple databases. However, a series of reasonable assumptions quickly leads to the conclusion that there is too much data to store even in a series of databases, and it is coming in too fast to write to a user-friendly relational database.

These assumptions do not make any allowance for use of the VII Network by either OEMs or other commercial operations. Such usage will certainly increase the data flow.

It is also not possible to consider data by exception. The user of traffic speed data may maintain that a few speeds are sufficient, and a snowplow dispatcher might use only a small percentage of the temperature data. However, data by exception will not accommodate either the safety applications where all vehicle positions are required, or allow the OEMs to maintain communication with an individual vehicle.

Each user of the data has individual needs and may require that their specific data have to be archived. This, together with the quantity problem, leads to the VII Message Switch approach. The VII Message Switch would be logically connected to a large number of RSEs. When a vehicle sends a message, the RSE will determine whether this message is:

- A local message that needs to be sent to the local controller,
- A message for another qualified user, such as an OEM, or
- A message containing the public sector data

In the first case, the message is immediately sent to the local controller or safety application processor. In the latter two cases, the message is sent to a VII Message Switch that forwards it to a subscribing Network User. Note that in the case of non-public data, the ability to subscribe to those message types will be highly restricted. This is illustrated in Figure 5-2 Flow from Vehicle to Application

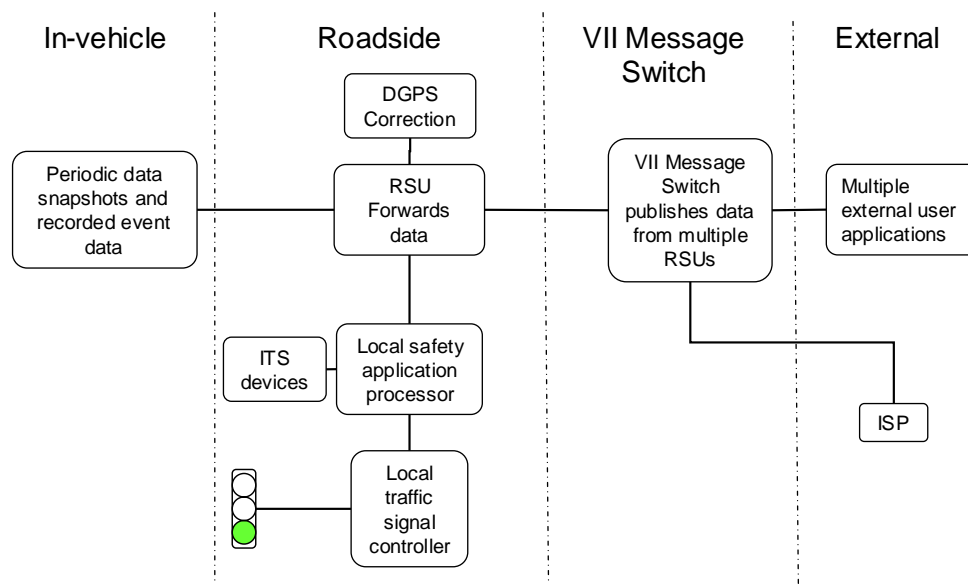


Figure 5-2 Flow from Vehicle to Application

In the vehicle, the periodic data is kept as a series of snapshots together with a series of events. The DGPS correction at the RSU indicates a source for a GPS correction signal. The correction could be achieved by either placing a DGPS receiver at a selection of RSU, at cell towers within the network, or through the use of the US Coast Guard Signal. The optimal solution requires additional study. The GPS signal is used to time stamp and position all this data. When the vehicle comes within range of an RSU, the data is sent from the vehicle and immediately forwarded to the VII Message Switch or the Local Safety System. The VII Message Switch keeps the information long enough to determine the Network Users that have subscribed to the applicable messages, and publish the messages to them.

This approach allows the Local Safety Systems to have the low latency required for safety applications and avoids the large data problem. The Local Safety Systems processor would run its applications and provide messaging to and from the local ITS equipment such as a signal controller.

5.5. Communications Model

A model, implemented as a spreadsheet, was developed to assist with understanding the requirements for the communication system needed to support public use cases for the VII architecture. The objective for developing the model was to be able, at a high level, to quantify the necessary bandwidths in order to determine the feasibility that current technology would be able to meet the expected demands of the public sector. In order to develop the model, some initial assumptions were made about the architecture of the system. The communications model envisioned a network of VII message switches. External applications or users would make geographic-based inquiries that could require queries to several switches.

The communications model included several elements:

- The kind and size of data available from new vehicles and when (model year) certain data elements would be supported
- The size of messages, including protocol overhead, that OBE equipped vehicles will transmit to RSUs
- The number of RSEs expected to be deployed system-wide
- The percentage (increasing over time) of equipped vehicles in the traffic stream
- How much data will be transmitted to individual RSUs
- At peak traffic flows system-wide, how much data will be transmitted to a VII Message Switch
- How much data different classes of external applications or Network Users receive from the system, from how many VII Message Switches, and at what interval

Key outputs of the model include the memory requirements at the RSE and the VII Message Switch assuming peak traffic conditions together with the data flows from the vehicle to the RSU, from the RSE to a VII Message Switch, and from a VII Message Switch to various Network Users.

The set of default input values for each element was developed using input from the automobile manufacturing industry on the likely size and availability of data from vehicles, assuming peak traffic flows and market penetrations, and assuming worst-case scenarios for user demands for data. Under these assumptions, the results of the model indicate that in general, public demands can be readily met with current technology. Making assumptions about the required number of bytes to describe each element in the probe data snapshot results in about 40 bytes. Assuming there are twenty snapshots of data this results in an 800 byte probe message. This makes no allowance for security and assumes no messages are sent to the vehicle. Assuming that, at peak flow conditions of 1800 vehicles/lane/hour, 10 lanes of traffic, and all vehicles in the traffic stream equipped, results in a 40 kilobit bandwidth is the requirement. This is within the capacity of a normal phone line. However, these are just the one way public sector requirements without the effects of the required security messages and without the demands from the OEMs and commercial operations.

Depending on the amount of data expected from subscriptions and the desired response time(s), public users requiring data from a large number of RSUs will require higher bandwidths to a VII Message Switch. Default assumptions for public demands were developed assuming a hurricane or large scale natural disaster scenario where the user will demand large amounts of data with fairly quick response times.

5.6. Dedicated Short Range Communications

Dedicated Short Range Communications (DSRC) is a general-purpose radio frequency communications link between different vehicles, and between the vehicle and the roadside. 5.9 GHz DSRC is a short to medium range (300m – 1000m) communications service that supports both public safety and private operations in roadside-to-vehicle and vehicle-to-vehicle communication environments.¹⁴ There is a guardband from 5.850-5.855 GHz.

DSRC has a range of up to 1000 meters but is typically 300 meters depending upon FCC power restrictions). It requires near-line-of-sight for transmission. The data rates that it supports vary from 6 to 27 Mbps per channel. It consists of seven channels as illustrated in Figure 5-3 DSRC Channel Allocation.¹⁵

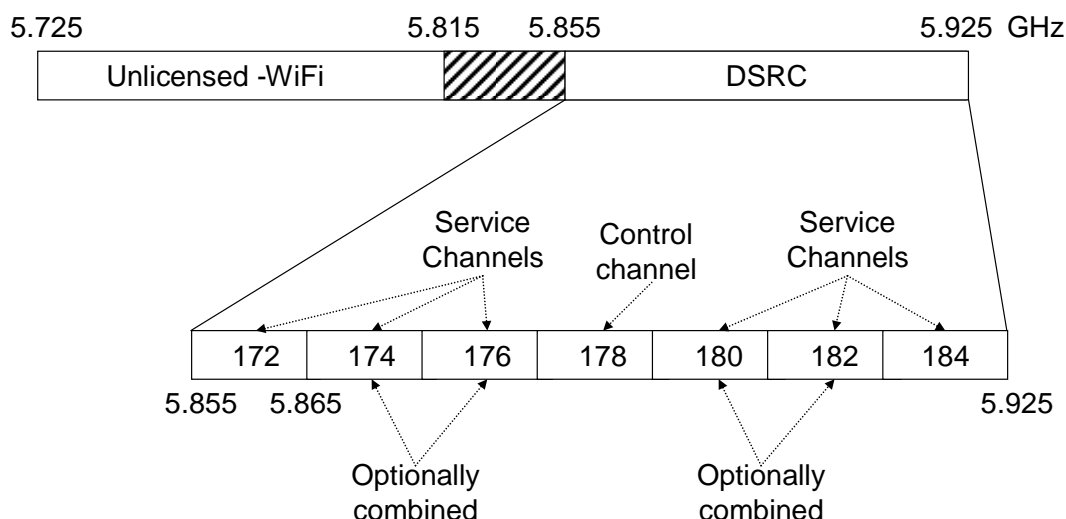


Figure 5-3 DSRC Channel Allocation

Each channel can support up to 27 Mbps. However, combining two channels allows this to be doubled. Provisionally, channel 184 has been proposed for public safety and channel 172 is reserved for high availability low latency communications using High Availability and Low Latency (HALL Channel).

Channel 178 is the control channel, a single (ten megahertz) channel accessible throughout the country that establishes a communications link between an RSU and an OBU or between OBUs. OBUs are required to periodically monitor the control channel for public

¹⁴ <http://www.learmstrong.com/DSRC/DSRCHomeset.htm>

¹⁵ FCC WT Docket No. 01-90 Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)

safety messages. The specific timing of the control channel monitoring is not fully defined. The length of messages on the control channel can vary, but are generally kept short to permit maximum access. When tuned to the control channel, all RSUs and OBUs, by default, will listen for a transmission. If an RSU or an OBU desires to transmit a message, but detects the broadcast of another message on the control channel, it must wait before attempting to transmit. An OBU or an RSU initiates a request to send, and the control channel will grant time first to high priority messages, i.e., a public safety communications, then to lower priority non-public safety communications. The Control Channel is limited to the RSU transmission of Provider Service Tables (PST) and WAVE Short Messages (WSM). The OBU transmissions on the control channel are limited to WSM. No IP traffic is allowed on the Control Channel. All IP data traffic must use Service Channels. The PST has the highest priority channel access and the WSM traffic channel access is defined by the WSM priority. See IEEE 1609.3 for details.

If an RSU or an OBU leaves the control channel to communicate on a service channel, a timer, defined by mandatory data transfer time limits, will be activated to indicate it should return to the control channel to listen for additional transmissions and distinguish between priority and non-priority calls. In this connection, the control channel implements the priority given to public safety communications through a priority interruption capability. Specifically, the control channel operates using a set of rules to provide a Quality of Service that includes access time, access priority, and channel capacity service to RSUs and OBUs. This is referred to as the control channel protocol.

The DSRC standard allows for the transmission power to be varied. For example, should one vehicle be communicating with a nearby charging point such as a gas station RSU, the power can be low. If an emergency vehicle is requesting a traffic signal preempt, then the power may be high to maximize the range. Figure 5-4 DSRC Data Rate v Range illustrates approximate ranges and data rates that would support the range of VII services.¹⁶

DSRC is half-duplex in that at any one time an OBU or an RSU can only either transmit or receive. The service channels of RSUs that are physically close to each other will be allocated to use different channels. For example, in the case of adjacent transmitters at a gas station and an intersection, the frequencies used (channels) will be allocated to prevent conflict.

¹⁶ Standard Specification for Telecommunications and information exchange between roadside and vehicle systems. Specific Requirements – 5GHz Band Dedicated Short Range Communications: Mac Extension and Lower Layer Management - DRAFT ASTM.

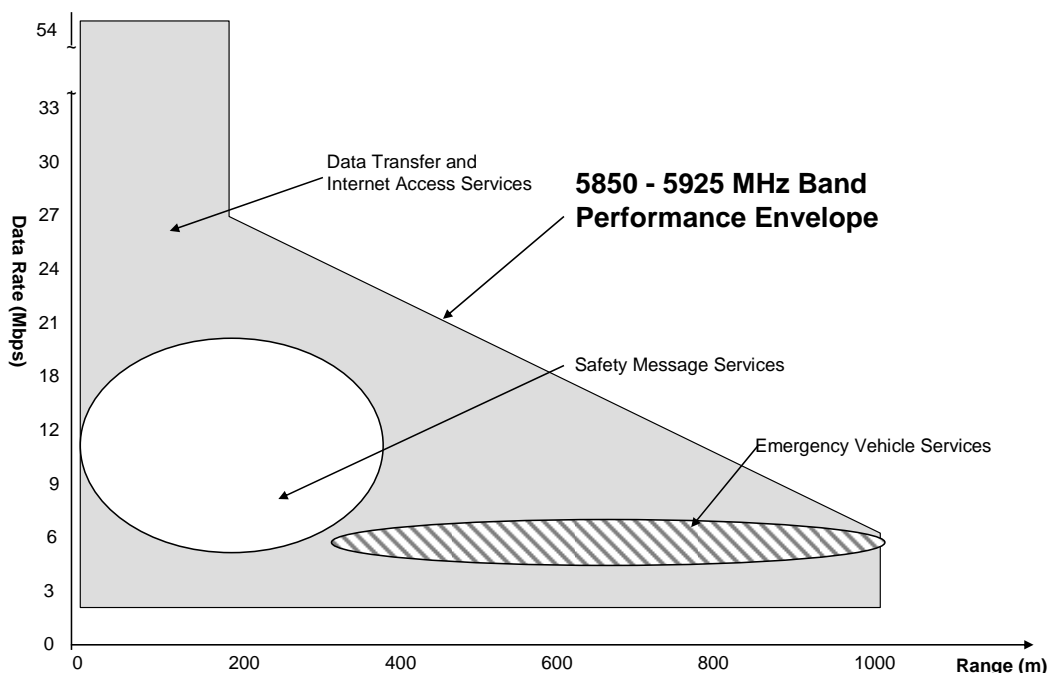


Figure 5-4 DSRC Data Rate v Range

The FCC designated a series of channel numbers and their use as indicated in Table 5-1 FCC Designated DSRC Channels.

Table 5-1 FCC Designated DSRC Channels

Channel #	Channel Use	Frequency (MHz)
170	HALL Channel	5850-5855
172	Service Channel	5855-5865
174	Service Channel	5865-5875
175	Service Channel	5865-5885
176	Service Channel	5875-5885
178	Control channel	5885-5895
180	Service Channel	5895-5905
181	Service Channel	5895-5915
182	Service Channel	5905-5915
184	Service Channel	5915-5925

5.7. Network Centric Approach

The VII architecture is highly decentralized. Most of the data within the vehicle is used by applications in the vehicle and only a small selection of this data is transmitted to the RSUs. Data used at the intersections is kept at the intersection and used to ensure low latency, as

many of these applications require a fast response. The data from vehicles that is transferred to the network is forwarded by the RSEs to the VII Message Switches. These do little processing beyond parsing out the vehicle data and sending it to the external users who have subscribed to the data stream. It is the Network Users that will need to add applications to use the data that they request.

Thus the architecture can be described as network centric where its main function, like the Internet is to provide a connection between user and the data source with the minimum of interference. The approach of distributing the processing as widely as possible is a consequence of the large amount of data. Simple assumptions on the data sizes indicate that there will be multiple gigabytes of data being passed in the peak hour. This data is only for probe messages and is a nationwide estimate. This quantity will increase over the years as the system, the data types and the number of equipped vehicles grows. Such a significant volume of data cannot be accommodated without distributing the processing. Each Network User will be responsible for their storage and archiving of their data.

5.8. Publish and Subscribe Processes

There are a variety of networking mechanisms that could be used for distribution of VII messages. The use of the publish and subscribe model has significant advantages as outlined by IBM¹⁷. Publish/subscribe applications are intended for situations where a single message is required by, and should be distributed to, multiple users. Its big advantage over other delivery methods is that it keeps the publisher separated from the subscriber. This means that the publisher in a publish/subscribe application doesn't need to have any knowledge of either the subscriber's existence or the applications for which it may use the published information. Likewise, the subscriber or subscriber applications don't need to know anything about the publisher application. Put as simply as possible, a publish/subscribe application has one or more publishers who publish messages from an application, and a group of subscribers who subscribe to some or all of those published messages. The system matches the publications to the subscribers and allows for all the messages being made available and delivered to all the subscribers in a timely manner

There will be several hundred thousand RSEs collecting data from many millions of vehicles that are only in contact for short time periods. Each vehicle will be producing many tens of messages per trip. If all states and most large cities are data users, there are likely to be several hundred recipients of the data. Any direct connection mechanism between so many entities would not be viable. The various elements that make up the VII Network need to communicate with each other in a robust manner such that the sender and the receivers of the data are not dependent on maintaining a connection. . The OBU and the RSU communicate using DSRC. All other elements will use publish and subscribe methods of communications. This involves three processes:

- Registration – where the device joining the VII Network sends a message to the device(s) with which they are logically connected. This message includes the requestor's identity, desire to publish particular messages in the future, and various technical data concerning the mechanism for communications.

¹⁷ <http://www.redbooks.ibm.com/redbooks/SG246282.html>

- Subscription – where the device wanting the data sends a message, subsequent to registering, to a device to which they are logically connected asking for a particular data type.
- Publish – where the device with the data sends it to its subscribers on receipt. Rules within the publishing data server determine which entities are allowed to subscribe to which data.

The use of the publish and subscribe model for information dissemination is well accepted and is used for data dissemination by institutions such as Stock Exchanges that need to distribute large data flows to many users intermittently.

6. On-Board Units and Equipment

6.1. OBU and OBE Introduction

An On-Board Unit (OBU) is a DSRC transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The manufacturer and not the vehicle owner will be the licensor of the OBUs.

There is a category known as Public Safety OBUs or PSOBUs. An example of this would be an OBU mounted on an emergency vehicle providing its location to oncoming vehicles. Portable RSU such as may be mounted in work zones are also allowed under the FCC rules.

The OBUs will provide the communication both between the vehicles and the RSUs, and the vehicle with other vehicles. The OBU is similar to an 802.11 wireless transceiver. The On-Board Equipment (OBE) includes the OBU plus:

- Applications processors
- Interfaces with the vehicle services
- The Human Machine Interface (HMI) and
- The GPS and vehicle position processors.

Many of the functions described here will occur in the application processor which in turn will be gathering data from other devices in the vehicle. Each vehicle manufacturer will likely be configuring their internal systems in different ways. For ease of understanding, these are referred to in this document simply as the OBEs.

The figure illustrates the scheme within the vehicle.

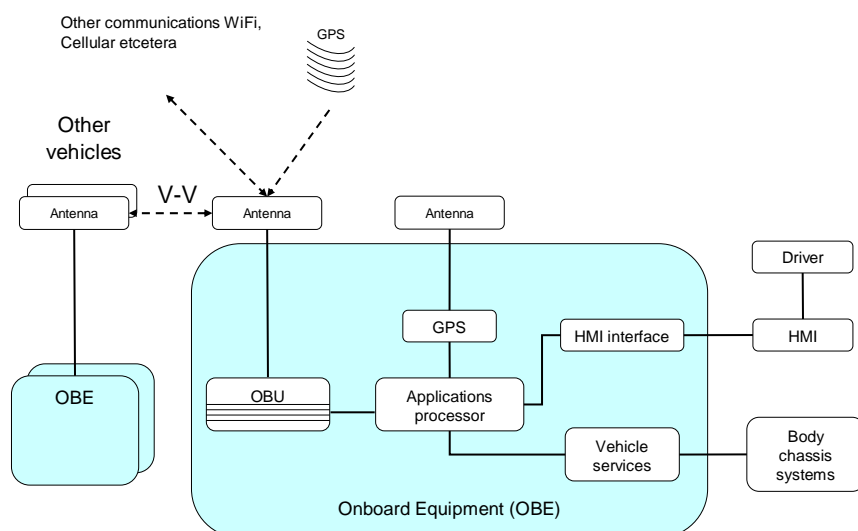


Figure 6-1 In-vehicle Elements

6.2. OBU and OBE Functions

The Onboard Equipment (OBE) is considered to include the radio section known as the Onboard Unit (OBU). The parts of the vehicle that will communicate with the OBU and hence the rest of the VII processes are entirely within the purview of the specific automaker. Indeed not only will the OBE be defined differently by manufacturer, but also by model and by year. The requirements listed here are labeled as OBE requirements which include the OBU requirements and are needed to ensure that the vehicle will fit within the VII architecture.

The OBE will be responsible for reading the GPS data together with a variety of in-vehicle sensors. Several of the vehicle-to-vehicle applications and the safety applications running at the intersection require regular low latency communication (on the order of 100 msec). To accommodate this, the OBU may be transmitting regular safety messages perhaps once every 100 msec. The content of this message is currently not finalized, but it is likely to include, among other things, a temporary ID, message type, time stamp, and location as defined by SAE. The OBU may also regularly transmit other routine messages with more content, but these are likely to be at greater intervals as well as transmitting specific messages on the occurrence of certain events.

The OBE will gather the messages of interest on a regular basis. It is anticipated that the OBE will gather the public-sector, periodic data as a snapshot at intervals developed as an inverse function of speed plus when vehicles start and stop occur. It is proposed that the default be every 30 seconds at high speed reducing to every 10 seconds at lower speeds. This is intended to accommodate lower densities of RSUs that are expected on high speed roads. The starting and stopping data will also provide information on incidents and may be used for optimizing traffic signals. The interval between snapshots could be determined dynamically upon instruction from an RSU as an aid to mapping. After some period of time, the oldest data can be overwritten. This approach is designed such that if the spacing between RSUs in rural areas is 10 miles then 20, snapshots of data every 30 seconds for a

vehicle traveling at 60 mph should provide significant coverage the road network. All the snapshots that are kept in the OBE's memory will be sent to the RSU, as appropriate. The number of snapshots and the interval between them is dependent on the size of the OBE's memory and its communications capacity. It is the intent of this approach that the snapshots provide data on portions of the network not within range of an RSU.

The OBE will gather event data with the snapshots of periodic data. An event is a transitory occurrence that is of interest to the public sector. For example, the activation of traction control could result either from enthusiastic driving or from degradation in the pavement surface. A State maintenance division may have an application that makes inquiries of VII for information on all traction control activations on its roads. To do this, the application might subscribe to the traction control activation locations and weather related information published by appropriate RSUs. These could be stored in the State application and then the activation locations could be mapped to display locations of concern. Such data could then be used in an asset management process, for example, to determine resurfacing priorities.

The OBE needs a GPS unit, possibly with some enhancement, in order to meet the location requirements of various use cases. The accuracy of the GPS system without any enhancements is only adequate to identify the road and not the lane in which the vehicle travels. It is required that the VII system provides lane data to meet some of the safety use cases, in particular those that require segregation of vehicles into lanes. One solution is to add local differential correction to the data broadcast by the RSU. This approach is discussed later in section 8. A variety of other solutions are possible, including both terrestrial and satellite differential transmissions.

6.3. OBE Functional Requirements

6.3.1. Local Safety Messaging

{OBE 1} The OBE shall communicate with and receive broadcast messages from the Local Safety Systems that are connected to the RSU at the roadside. This communication will consist of the delivery of a Provider Service Table (PST) that describes the functions supported by that RSU and its related LSS.

{OBE 2} Following the reception of an appropriately configured PST message, the OBE shall provide to the Local Safety System through the RSU its unique, randomly generated address and the data required for that application. The roadside safety system will use that address to send information back through the RSU to that specific OBU. The generation of the unique random address will be reset upon communication with the next new RSU whose PST includes a request for probe data.

{OBE 3} On appropriately equipped vehicles, when receiving a PST element for a vehicle preemption request, the OBE shall respond if its current status, position and direction warrants a preemption.

6.3.2. Public Sector Messaging

The OBE aggregates probe data from the vehicle and sends it to the public infrastructure. The OBE receives messages from the infrastructure and presents them to the driver. Since the DSRC connection supports two types of message traffic, Wave Short Message and IPv6, there are several permutations and combinations available to the designed. This

section does not allocate message type to individual requirements. However, the PST directs an OBU to a Service Channel where both WSM and IP traffic are allowed. For safety traffic the RSU and OBU can use WSM only, no IP traffic is allowed. Also the HALL Channel is typically used for OBU to OBU low latency exchanges using WSM traffic. The WSM can be Broadcast, Multicast or Unicast. The details are described in IEEE 1609.3 & .4.

{OBE 4} The OBE shall respond to the broadcast Provider Service Table (PST) message from the RSU with appropriate responses according to its programmed functionality.

{OBE 5} The OBEs that respond shall do so in the approved VII messaging format. (See Chapter 7 for a discussion of the PST.)

{OBE 6} Each OBE shall store as a minimum the last 20 probe data message snapshots. The data elements for the probe message are listed in appendix A. Refer to the IEEE 1609.1 standard for a discussion message storage, retention, and transmission to RSUs.

{OBE 7} The message set shall contain all or part of the data defined in the list in Appendix A – VII Data items from the Vehicle.

{OBE 8} All data elements on the list shall be restarted at key-on in the vehicle.

{OBE 9} The OBE shall store probe data message snapshots at the frequency defined by an algorithm such that the frequency of data collection is inversely proportional to speed where the minimum time between data sets is 15 second and the maximum is 60 seconds.

{OBE 10} In addition, the stopping and starting of the vehicle shall be considered events.

{OBE 11} As appropriate, the OBE will pass messages received from an RSU to the applications in the vehicle.

{OBE 12} When the OBU receives a public sector broadcast, it shall present this message to the driver within the constraints of the vehicle's human-machine interface

{OBE 13} The OBE functionality shall support digital signature on all messages using a series of certificates installed by the appropriate OEM.

{OBE 14} The OBE shall use its current position together with its GPS time stamp to compare its location and time with that of the transmitting RSU to add veracity to all received messages.

{OBE 15} When an OBE receives a message from a new RSU that supports a request for a probe message, it shall reset its unique random address. Thus there will be no possible association between data elements when the probe messages are sent. However, the intersection will know the current temporary address of the vehicle for the duration of time that the vehicle is within range of that intersection.

6.3.3. Private Sector Messaging

The OBE can initiate a transaction by the use of a User Service Table (UST) that can be transmitted to advertise the applications it can support. The OBE obtains data from a vehicle

proxy and pushes data to a server proxy. The OBE shall process messages from CSPs that are authorized to communicate with the OBE.

{OBE 16} The OBE shall respond to such messages with a transmission to the RSU. Such transmission shall be addressed to the recipient and shall be considered private.

{OBE 17} The OBE shall transmit a User Service Table (UST) upon request from an RSU.

6.3.4. Vehicle to Vehicle (V-V) Messaging

{OBE 18} The OBU shall, on a regular basis, transmit data concerning its status to other vehicles within range.

{OBE 19} The OBU shall receive messages from surrounding vehicles.

{OBE 20} OBUs that are mounted on service and emergency vehicles are designed Public Safety RSUs (PSRSUs). PSRSUs shall be intermittently connected to the VII Network.

7. Road Side Units and Equipment

7.1. RSU and RSE Introduction

An RSE is the VII equipment in the field that performs a variety of VII functions. These include, some and possibly all of:

- Transceiver and an antenna to send messages to, and receive messages from OBUs.
- An input output controller (I/O) that can communicate with a Local Safety System
- A router that can communicate with the VII Network
- A GPS receiver that is used to register the equipment's location
- A processor to execute indicated application functions

Although all these functions are required and could be provided by separate devices it is likely that they would be integrated into a single unit when production quantities are being manufactured.

Under the FCC license, an RSU may also be mounted on a vehicle or can be hand carried, but it may only operate when the vehicle or hand carried unit is stationary. An RSU transmits data to or receives data from OBUs in its communications zone. An RSU is restricted to the location where it is licensed to operate. However, portable and hand held units are permitted to operate on the control and service channels where they do not interfere with RSUs that have a site license.

An RSU communicates with an OBU by transmitting a Provider Service Table (PST). The PST is a list of information that defines the applications with which that specific RSU is involved. The PST can contain information such as:

- RSU identification
- Application identification(s) (AID)
- Application Context Marker - an optional field to distinguish between multiple services offered by the same application
- Channel assignment
- Transmit power limits
- Transaction instructions
- Data rate
- Modulation
- GPS Data Location and differential correction factors
- Other pertinent information

The RSE and its associated equipment will support multiple applications within its software. In addition to supporting the communications with the OBU, the RSU needs to support the safety functions associated with the applications running at the intersection. However, these safety functions are likely to run on an additional Local Safety System (LSS), further defined in section 6.3.1, that is connected to the RSU.

To obtain economic benefits associated with large production numbers, the RSE should be considered as a standard device consisting of a radio and a processor, which is logically connected to a Message Switch. This approach allows most RSEs to be electrically identical even though they may be running different software applications.

7.2. RSE and Safety Applications

Examples of safety applications include:

- Infrastructure-based curve warning
- Infrastructure-based signalized intersection violation warning
- Infrastructure-based signalized intersection turn conflict warning
- Post-crash warning
- Left turn assistant
- Stop sign movement assistant
- Emergency vehicle signal preemption

Some of these applications require that the RSU pass on information from one vehicle to another (V-V). OEMs in general agree that a vehicle should be given all the information and make its own decision on use of the information.. The RSE will need to prioritize the messages in some order such as safety; vehicle operations; and commercial services.

The RSE may be connected to an Input/Output Controller interface enabling the RSE to send standard messages to external devices. These could include signs, beacons, signal controllers and traffic detectors. Some of these applications, particularly those involving the real-time collecting of vehicle location data, could be configured as shown in Figure 7-1.

Although each RSE will be able to support multiple applications, when all the different roadside configurations in terms of differing geometries and user functions are considered, it is likely that other specialized processing functions may be needed. The RSE functions in a freeway location will be different from those on an arterial. These differences in some cases will be incorporated by differing AIDs in the PST. Other differences such as connections to Local Safety Systems can also occur. For example, signalized intersections may need to process inputs requesting preemption, or provide input to adaptive signal control. RSUs at un-signalized intersections may be required to communicate with and control a series of Intelligent Transportation System (ITS) surveillance and control devices. In addition, RSUs may be mounted on a vehicle or hand carried but, as noted above, may only operate when the unit is stationery and within its authorized geographical boundaries. Processing associated with local safety applications will be accomplished by the Local Safety System processor. Data needed for these processes will be delivered via the Input/Output Controller interface.

7.3. RSE Registration and GPS

It is anticipated that there will eventually be a few hundred thousand RSEs implemented to support the VII functions. External applications will often use Geographic Information Systems (GIS) to make inquiries. Maintenance, operations, and configuration management will require significant effort. The use of a GPS unit on the RSE helps support both of these functions. The role of GPS in making external inquiries is discussed later.

It is proposed that each RSE operate in a self-registering mode. When the connection is made between a VII Message Switch and an RSU, the RSU will provide its position from the GPS location together with its network address and publish/subscribe requirements. The VII Message Switch will be used to track the publish/subscribe data, and forward information on applications, version numbers, locations, addresses, etcetera of the RSE to subscribers of that information.

There is also a potential to use the GPS location of the RSU to assist in the validation of messages. It may be possible to download to vehicles the position of downstream RSUs such that vehicles will be able to compare known positions with RSU addresses. This process could be enhanced, if the vector of the vehicle is known, by only accepting RSU messages from a known sector ahead of the vehicle. This requires further investigation but has the potential to provide an additional element to the security system.

7.3.1. Local Safety Applications

Safety applications at the roadside that use the RSE will be located in the Local Safety System as indicated in Figure 7-1.

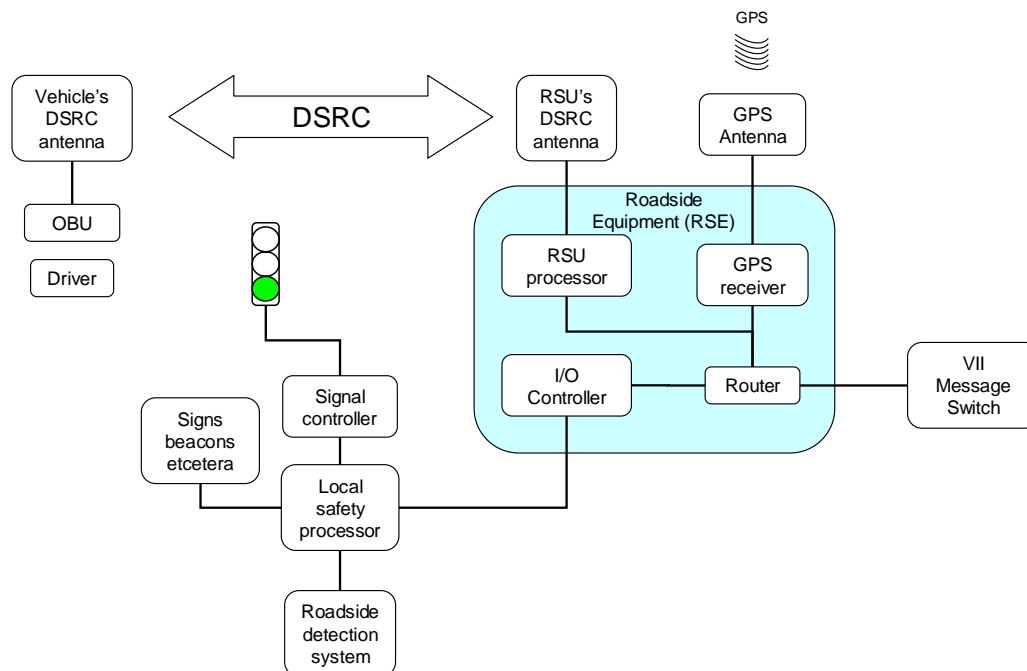


Figure 7-1 Roadside Equipment Logical Layout

The internal functioning of the Local Safety Systems is beyond the scope of this report and hence no associated requirements are included. The Local Safety Systems may be connected to a series of external ITS devices. These devices would be under the control of the Local Safety System and are not defined here.

{RSE 1} The VII system shall allow for the required interfaces to enable Local Safety System messaging.

{RSE 2} The system shall provide for a latency of 100ms or less for Local Safety System messages and treat Local Safety System messages with a higher priority than other message types.

{RSE 3} The RSE shall support an interface with local safety applications. The RSE will receive specific information from the OBUs and transmit this data to the Local Safety Systems. The RSU will transmit information from the Local Safety Systems back to specific RSUs.

{RSE 4} The RSU shall receive secured and private vehicle data in order to determine the location, direction, speed and other data concerning all OBU equipped vehicles within the range of the RSU.

{RSE 5} The RSE shall receive data through a separate I/O Controller (I/OC) from the Local Safety System, which may be connected to signal controllers and road weather detector data.

{RSE 6} The Local Safety System shall use a serial connection to the RSE.

{RSE 7} The Local Safety System shall receive the vehicle data from the OBUs, process it and return data to the RSE for transmission to the OBU as appropriate.

{RSE 8} The Local Safety System shall gather data for transmission to all OBUs, or to specific OBUs.

{RSE 9} The VII System, through the RSEs, shall allow the Local Safety System to access the OBUs with system latency of 100ms or less..

7.3.2. Installation of RSEs

{RSE 10} Indication of the location of the RSU shall be supplied by an attached GPS unit. The location of the RSU shall be communicated to the system as part of the RSE registration process.

{RSE 11} As part of the registration process, the RSE, when connected to a VII Message Switch, shall automatically register itself.

{RSE 12} As part of the registration process, at the time of installation or moving to a new location, the RSE shall request from the Certification Authority (CA) a PKI Certificate. The PKI Certificate shall be used by the RSU to create its digital signature to validate the RSE as a trusted node.

{RSE 13} The certificate shall include the GPS location data of the RSU in order for the OBU to determine if the message is being delivered by an RSU that is in its immediate area.

7.4. RSE Operations and Support

The messages from the TOCs to the vehicles can considerably extend the range of information that is provided to drivers. Significant research¹⁸ has taken place in the area of In-Vehicle Safety Advisory and Warning Systems (IVSAWS) that provide advance warnings to the driver of unsafe conditions and situations on the roadway ahead to permit the driver to take remedial action. These messages relate to relatively transient conditions, requiring modifications at irregular intervals.

¹⁸ http://itsdocs.fhwa.dot.gov/jpodocs/repts_te/57b01!.PDF

From the perspective of the operator of a TOC, VII has the capability of significantly extending the information that it can provide to drivers, offering far superior data in terms of geographical coverage and functionality. There may also be significant savings in capital and operating costs associated with the implementation and maintenance of ITS devices.

To keep the VII system operating effectively, it will be very desirable to have a single controlling authority with responsibility for maintaining the RSE software. OBEs will be developed in a series of versions over time as new features and facilities are added to the vehicle fleet. Older vehicle systems will need to be supported as these changes occur. This will result in a variety of message types that need corresponding changes in the RSUs. In order to keep the system viable, system managers will need to adhere strictly to comprehensive configuration management processes.

{RSE 14} The RSE shall have the responsibility of queuing messages to and from the vehicle. Its functions must include message management. Priority rules¹⁹ to be applied to messages include the following requirements.

1. The RSE shall ensure that safety applications are the first priority, including sending data to the local safety applications for low latency emergency control messages. This supports use cases such as infrastructure-based collision warning.
2. The RSE shall give information messages from the State DOT to the vehicle as a second priority. These could be added to the regular broadcast message for display to the driver.

Such a process would allow TOCs to perform the same functionality they currently perform with variable message signs, highway advisory radios, and other devices to keep drivers informed. However, the use of RSEs to perform this function will allow more timely information with better geographic resolution. In addition, the messages can be more complex as more characters would be possible than those on variable message signs.

3. The RSE shall have vehicle support messages, such as safety notices and diagnostics from the OEMs, to their vehicles as a third priority. The RSE will enable the OEMs to upgrade on-board software and to provide additional services to their customers.
4. The RSE shall have as fourth priority financial services – such as tolling, parking and purchases.
5. The RSE shall have data services such as messaging and entertainment as the lowest priority.

Some RSE may be dedicated to a limited number of services (such as tolling) such that an ETC RSE may be single service and single priority

¹⁹ IEEE P1609.4 and P1609.3 referred to earlier

7.4.1. Update Service Table

Services that are performed by an individual RSE will be dictated by the software installed and the needs of the Network Users. As the needs change for data from a specific area the RSU's PST will be updated as described in IEEE 1609.3.

{RSE 15} The RSE shall update the PST that it broadcasts to the OBUs when a new application is provisioned to the RSE processor or a new service becomes available and when instructed by an authorized Network User.

7.4.2. RSE Updates

The RSE will have the capability to have its internal software and Service Tables remotely updated to new releases. (Open System Gateway Initiative) OSGI provisioning processes will enable software upgrades.

{RSE 16} All Service Table entries that correspond to broadcast data will be required to have a time out such that without update activity the RSE will resort to the status quo.

{RSE 17} RSEs that are not generally connected to the VII Network shall have an external input device to enable the input of software and Service Table changes that have been released.

{RSE 18} Once software or Service Table upgrades have been received, the RSE shall use automated methods such as OSGI (the Open Systems Gateway Initiative)²⁰ to upgrade the software running on the RSE. (Provisioning services such as OSGI will be used to download applications and executable files to both the vehicle and the roadside. The publish and subscribe feature is concerned with data, not applications. Service Table is in the form of a Management Information Block (MIB) generated by a Simple Network Management Protocol (SNMP).

{RSE 19} The RSE and RSU shall operate a fault recovery system. The system shall allow automated recovery from commonly occurring faults including power failure, communications outages, memory loops, communication overloads and other likely causes of failure.

7.4.3. RSE Health Check

Given the number of RSEs that will exist on the network, an automated method is needed to indicate any problems that exist with individual RSEs.

{RSE 20} The RSE shall self monitor by periodically verify that all of its internal and connected systems are working correctly.

{RSE 21} In the case that the RSE determines that a problem exists in its system, that information shall be published for use by the VII Network Operations Entity.

{RSE 22} The RSE shall be capable of automatic reset if internal conflicts are detected and automatic restart following power failures.

²⁰ <http://www.osgi.org>

7.5. Messaging With Vehicle

Messaging between the RSU and the OBU will consist of the RSU sending messages to, and receiving messages from, the OBU. The messages sent and those received will be a function of the specific applications that have been enabled in the specific RSU and OBU.

A broadcast message, using a PST, will be sent out by the RSU that will perform various functions. This message will inform the OBUs, within communications range, that an RSU is active. As part of the message, the RSU will indicate the services that may be provided, and any public messages that may be active.

{RSE 23} RSU PST message shall be transmitted typically once per 100 milliseconds

{RSE 24} The RSU PST broadcast message shall inform local OBUs that the RSU is active and able to perform a certain list of applications.

{RSE 25} The broadcast messages shall contain the following items.

- **PKI Certificate** – The RSU’s digital signature along with the associated public key²¹. By decrypting the digital signature the OBU may trust the data being sent by the RSU.
- **Service Table** – A Service Table shall be included in the message being transmitted. The Service Table shall include an indication of the functions and services that are available from this RSU.

The broadcast message may contain the following items:

- **Public Message** – If a public message exists for the particular RSU, the public message shall be included in the message. If more than one public message exists for the RSU, a relative prioritization of public messages shall exist indicating which of the public messages shall be included. The system shall not restrict the content or type of information that is being disbursed as part of this public message.
- **GPS Correction** – If GPS correction data exists for this RSU location, the correction data shall be included in the message being transmitted.
- **Map Updates** – Geometric data concerning the current and adjacent roads.
- **Intersection System State** – Status data from the intersection that could include:
 - Map data
 - Signal timing
 - Stop and yield locations
 - Status of other vehicles

7.5.1. Message Scheduling

{RSE 26} The RSU shall transmit the regular broadcast messages via the DSRC control channel (#178) in a dynamically sequenced series of messages. The RSU shall switch to a service channel when insufficient time is available on the DSRC control channel to accommodate the transmission of the complete broadcast message

²¹ The IEEE 1556 document has not yet been released for public distribution

{RSE 27} The RSU shall support unicast messages that provide an acknowledgement to the sender. This approach will allow a CSP or an OEM to send messages to a specific OBU and know that it was received.

7.5.2. Receive Messages from OBU

In response to the PST message from the RSU, the OBU may send a message that corresponds to a response that is being offered by a particular PST application. For example, a fire truck OBU may have a traffic signal preempt application. If the intersection supports this application, then a Network User would download a preemption application which would provide the appropriate elements into the RSUs PST. The RSE would connect to the Local Safety System that will communicate with the signal controller. When the OBU receives the PST, it would respond with the appropriate request for a signal preempt. The RSE would forward this to the Local Safety System which would then interrogate the signal controller. The response from the controller (yes or no to a preempt) would then be sent to the RSE for transmission to the OBU. The local application in the vehicle would configure the appropriate message for the driver.

{RSE 28} Data from valid messages shall be published by the RSU to the VII Message Switch or sent to the Local Safety System.

{RSE 29} As part of the message being published to the VII Message Switch, the RSE shall include its own address so that a return message may be executed by the Network User, as appropriate.

7.5.3. Send Message to OBU

After an RSU receives a message from an OBU, the RSU may send subsequent messages back to the OBU. The architecture assumed that all messages between the OBU and RSU will take place between one specific OBU/RSU pair. Sending one message split across multiple RSUs will not be supported as a feature of this architecture. This does not prevent external users from selecting downstream RSUs to transmit the latter part of a message but this would be a feature of their external application.

{RSE 30} In order to send messages to the OBU, the RSU shall format the data into a message that is in conformance with the protocol accepted by the OBU. The OBU can receive WSM and PST traffic on the Control Channel. On a Service Channel, the RSU's PST will define the channel and the IP address information needed for IP communications. When the OBU responds to the PST on the Service Channel it will provide the RSU with the IP address information needed for IP traffic. If WSM traffic is used on the Service Channel then the OBU must have the proper WSM traps programmed into its WAVE Protocol Stack to process the WSM traffic. See IEEE 1609.3 for a detailed description.

{RSE 31} The digital signature shall be encrypted by the encryption algorithm that the OBU may accept. The message may then be sent to the OBU.

{RSE 32} A queue of message types shall be determined, so that in the case where there are multiple messages for an OBU, the order in which they are sent shall correspond to that priority.

7.5.4. RSU Broadcast Messages

In situations where a message is applicable to all drivers in the immediate area of an RSU, the safety message shall be broadcast to all OBUs. The message shall be sent together with the RSU PST Broadcast.

7.6. RSU Networking

The RSEs will be inter-connected VII Network in such a manner that when the connection between an RSE and a VII Message Switch is lost, the data will be automatically rerouted through alternate paths to an alternate VII Message Switch.

7.6.1. Networking RSEs

{RSE 33} RSEs that are at a fixed location shall be connected to a VII Message Switch that is part of the VII Network. The RSU will communicate to OBUs using DSRC. The RSU will communicate with the VII Message Switch using P&S methodology.

{RSE 34} RSEs that are transportable shall only be intermittently connected to the VII Network. Examples of these include RSU at work zones.

{RSE 35} The RSE shall communicate with the Network User through the VII Message Switch. Messages of various types will be published to VII Message Switches that have been assigned to the RSE. The assignment of a VII Message Switch will be a function of network tuning, that is, the dynamic adding and readdressing of elements as bandwidth needs change.

7.6.2. RSE Registering With System

Upon joining or rejoining the network, each RSE will register with their assigned VII Message Switch. The RSE will register with their assigned VII Message Switch as a publisher of data originating from the OBUs as well as internally generated information (e.g. RSE's GPS location). The RSE will also register with the assigned VII Message Switch as a subscriber of data that will be transferred to OBUs, and updates that are needed by the RSE (e.g., internal software updates or Service Table updates).

{RSE 36} The RSE shall register as both a publisher and a subscriber with its assigned VII Message Switch.

{RSE 37} Periodically, the RSE shall poll the VII Message Switch to ensure that it is still connected to the network.

{RSE 38} In the case that the VII Message Switch no longer exists, the RSE shall register with one of its designated backup VII Message Switches.

{RSE 39} The RSE shall periodically send messages to the VII Message Switch indicating the location of the RSE and the services available from the RSE. These messages may be combined to produce a report of all RSEs within any geographic area.

{RSE 40} The RSE's designated assigned VII Message Switch shall be able to be changed remotely by the Network Operations Entity. The change may be executed in order to tune the system which will equalize the load over the various VII Message Switches.

7.6.3. Formats Message for Publishing

Public messages may be stored in the RSE for inclusion in the RSU Provider Service Table Broadcast to all OBUs. No validation of the message content will be accomplished, therefore, the message may be any message that the authorized Network User has determined to display. The message will be sent to all OBUs within the range of the particular RSU. Public message may be the only function of the RSU. Examples of possible message-only RSUs are an RSU that is on a school bus indicating that it has stopped to pick up students, or an RSU on a fire truck indicating that an incident is ahead.

{RSE 41} The RSE shall subscribe to and store public messages.

{RSE 42} Public messages shall be included as part of the RSU Provider Service Table (PST) Broadcast transmission to the OBU.

{RSE 43} In the case that the RSE has received multiple public messages to display, a prioritization plan shall be executed to determine the public message(s) of priority.

{RSE 44} Public messages shall have an expiration date/time after which they shall not be sent.

8. VII Message Switch

8.1. VII Message Switch Introduction

A message switch in a telecommunications network is a device that channels incoming data from multiple ports (in the VII case, RSEs) to specific output ports that send the data to its destination, the users of the data.

The VII Message Switch will be an intermediate location to route subscribed messages to the indicated Network User. Each VII Message Switch may be logically connected to several thousand RSEs and all other VII Message Switches. When it receives public sector data from an RSE, it will determine which, if any, subscriptions the data will fulfill and will publish that data appropriately. Messages for which there are no subscriptions will be lost.

In the case of a Network User subscribing to data that is published by a different VII Message Switch than the one to which the Network User is assigned, the assigned VII Message Switch will subscribe to the publishing VII Message Switch for the data. Once the data has been received, the assigned VII Message Switch will then reroute the data to the requesting Network User(s).

Under these conditions, an application in a TOC that requires VII data must subscribe to the appropriate messages through a VII Message Switch. As part of the subscription process the VII Message Switch will ensure that the Network User has the proper level of authority and security to receive this data. This architecture makes the data available; it does not provide the external applications.

The public data published by the VII Message Switches will be anonymous that is it does not contain any vehicle identifiers. The data will consist of all of the snapshots that were uploaded from each vehicle. The principal information will be the data elements listed in Appendix A. Thus, the data from each vehicle will contain snapshots going back several minutes for a series of locations upstream of the RSU. However, these snapshots for an individual vehicle will not be associated and thus the path of one vehicle cannot be traced as the required information does not exist.

A characteristic of traffic flow is that it exhibits stochastic variation. The Network User receiving the data will in some cases need to take a statistical approach to the analysis of the data. For example, if a state wanted to develop an application that constantly monitored the rainfall on its interstate network, it could subscribe to the data in the relevant geographic areas and then select a wiper threshold above a fixed percentage. An external application could then display the appropriate areas on a map. The application would need to make threshold assumptions concerning when drivers turn their wipers on, how many do so and how this relates to current rainfall.

The AMI-C²² report identifies several hundred messages which relate to a system or data type within the vehicle. Much of these data will be useful to the OEMs for such functions as vehicle diagnostics, and could flow through the RSU if requested by an OEM interested in the status of a particular vehicle function.

²² AMI-C Common Message Set v1.01 2003-03-07

In addition to being a conduit of data between the Network Users and the RSE, the VII Message Switch will have some monitoring functions of their assigned RSEs and Network Users. RSEs will be subject to power outages, knockdowns, lightning strikes, communication failures, and all the other problems that commonly occur with traffic devices at the side of the road. The VII Message Switch will include such monitoring and reporting functionality.

8.2. VII Message Switch Requirements

{Message Switch 1} The VII Message Switch shall keep registration data and subscriptions of the authorized receivers of the VII data. Subscriptions will be delivered to the VII Message Switch via the network management application which shall be controlled by the Network Operations Entity.

{Message Switch 2} The VII Message Switch shall receive public sector data messages from the RSE and parse the data.

{Message Switch 3} The VII message switch shall receive private data messages and publish as appropriate to the validly subscribing recipient.

{Message Switch 4} The VII Message Switch shall publish requested data to all authorized subscribers.

{Message Switch 5} The VII Message Switch shall periodically poll all assigned devices. In the case where the device drops offline, all subscriptions related to that device will be deleted. The subscriptions shall be re-implemented upon the device reconnecting following verification that the subscription is still valid.

{Message Switch 6} The VII Message Switch shall report changes in the status of the assigned devices to the network management application.

{Message Switch 7} Subscriptions to messages originated by RSEs that are logically connected to VII Message Switches different than the Network User's shall be handled as follows. The VII Message Switch that is the logical connection for the Network User shall subscribe with the originating VII Message Switch for that message. After receiving the published message, the VII Message Switch shall check its subscription list and republish the message to the Network User.

{Message Switch 8} The VII Message Switch shall forward to the designated RSEs the broadcast messages from all authorized network users.

{Message Switch 9} The VII Message Switch shall apply prioritization rules to the messages. Each message type shall have an assigned priority that the VII Message Switch shall use to allocate the switching order.

{Message Switch 10} The VII Message Switch shall support two-way data transfer between network users and specific vehicles.

{Message Switch 11} The VII Message Switch shall be able to accommodate new data elements from the vehicle which should these be added to the public sector data list.

{Message Switch 12} The VII Message Switch shall configure the logically attached RSEs and keep current new RSEs as they are added to the system.

{Message Switch 13} The VII Message Switch shall support the security requirements of the VII System that are defined in the security section. The VII Message Switch shall report to the network management application all messaging events that for any reason fail the security requirements.

8.3. Registration Requirements

{Message Switch 14} The VII Message Switch shall, upon being connected to the VII Network, register to perform the needed functions of both publisher and subscriber with each of the other applicable devices on the VII Network.

{Message Switch 15} The VII Message Switch shall, upon connection, register with all other VII Message Switches in order to efficiently and effectively communicate with RSUs and Network Users that are on the VII Network.

{Message Switch 16} The VII Message Switch shall register as a subscriber of messages from all other VII Message Switches so that the messages may subsequently be published to RSEs and Network Users that are connected to this VII Message Switch as their primary connection. Messages that are received from other VII Message Switches shall then be published appropriately based upon the subscriptions that have been accepted.

{Message Switch 17} Since specific RSEs are logically designated as using a particular VII Message Switch as their primary connection, the VII Message Switch shall register with the RSEs that are communicating primarily with this VII Message Switch in order to effect the communications that will ultimately terminate with the OBU.

{Message Switch 18} The VII Message Switch shall also receive messages destined for RSUs. The VII Message Switch shall register with its primary RSEs as a publisher in order to communicate these messages to the RSU.

{Message Switch 19} Each Network User shall be assigned a VII Message Switch as its primary logical connection to the VII Network.

{Message Switch 20} The VII Message Switch shall have the capability to update its internal firmware and software to new releases using OSGI. Software and firmware upgrades shall be published to the VII Message Switch from the network management application. If necessary, the automated process shall include the ability to reboot the system.

{Message Switch 21} The VII Message Switch shall support an interface with gateway devices to connect to cellular and other communication systems

9. Mapping Requirements

9.1. Mapping Introduction

Mapping is an important issue within the VII architecture as several safety use cases either require the data or their functionality would be enhanced were it available.

VII offers the capability to build maps based on the efficient collection of raw position data over the VII network, coupled with the ability to feed accurate map data back to vehicles for use in various safety applications²³. This method has several advantages over other methods as it is a continuous process which will ensure that the information is current, can be developed in near real-time, and will be less subject to errors than conventional surveying methods due to the statistical nature of the approach.

Some of the VII use cases require lane information. To determine current lane, the combined vehicle position error and the map error must be less than about 1 meter. This may be achieved by using differential GPS in the vehicles and maps created through the VII network. The RSU may provide differential corrections by broadcasting the correction factors from the RSU to the vehicles.

Thus, after a vehicle has passed its first RSU, there should be an accurate map to support the safety applications in the vehicle and a recent and geographically close differential correction that the vehicle can use to perform positioning function.²⁴

This process provides a framework that can provide the accuracy of maps and position that is needed for some of the VII use cases. As technology changes, more satellites become available, GPS III and Galileo are deployed or other developments are implemented; use cases requiring high degrees of positional accuracy can readily be accommodated. If, for example, in the year 2015 there are freely available, high accuracy signals that the vehicle could receive when out of range of an RSU, then their use would enhance the system performance since the map accuracy will increase in those regions not within range of an RSU. As nationwide maps with lane resolution or better become available, these could be downloaded into the vehicle by a wide variety of communication techniques, not exclusively relying upon DSRC.

9.2. Mapping Data Flow from Probes

Vehicles will send up to multiple snapshots of data to the RSU, including position data, on the previously traversed roadway links. The RSU will forward all these vehicle positions, together with the other data elements, to the VII Message Switch. The VII Message Switch will publish this information to a Map Server, which will use the average positions from thousands of vehicles to develop accurate lane location data. Both GPS positioning and lane changing will introduce errors into this positioning process. However, the process running the application will be able to integrate many readings, and regression to the mean, will enable the development of maps with sufficient accuracy to discriminate individual lanes. As OBU penetration increases and high quality maps are developed the amount of data per

²³ Stefan Schroedal, et al Maining GPS Traces for Map Refinement. Data Mining and Knowledge Discovery, 9, 1-29, 2004. Netherlands

²⁴ <http://users.erols.com/dlwilson/gpsavg.htm>

vehicle may be reduced to the levels necessary to continually validate the accuracy of the refined map.

{Map 1} Each vehicle shall be equipped with a GPS receiver based positioning system or better.

{Map 2} There shall be Map Servers connected to the network collecting the vehicle positions from all vehicles. The Map Server shall register with assigned VII Message Switches and subscribe to all GPS data.

{Map 3} The Map Servers shall subscribe to the vehicle position data and apply appropriate filtering and smoothing algorithms.

{Map 4} A Map Server shall collect statistics on the data to derive current map data indicating lane information together with stop signs, yield signs and other traffic controls.

{Map 5} A Map Server shall publish new map data via the VII Message Switch to the RSEs for broadcast to the vehicles.

{Map 6} The Map Server shall subscribe to the inverted differential GPS calculations data from the US Coast Guard Nationwide DGPS service. The Map Server shall use this DGPS data, and apply the process to the uncorrected vehicle positions received from the VII Message Switch. This process is due to be available in 2006. Other options including local DGPS stations are possible.

9.2.1. Provisioning of Map Servers

{Map 7} The VII Network Operations Entity shall be responsible for determining need, acquiring, installing, maintaining, and debugging issues with Map Servers.

{Map 8} Additions of new Map Servers will be the responsibility of the VII Network Operations Entity. New Map Servers shall be added to the network as the volume and redundancy requires. Planning for future growth and adding associated Map Servers shall also be the responsibility of the VII Network Operations Entity.

{Map 9} Software support for Map Servers shall be the responsibility of the VII Network Operations Entity.

(a) Software support shall include initial installation of applicable software, and upgrades to software.

(b) Hardware support for Map Servers shall be the responsibility of the VII Network Operations Entity.

(c) Provided support shall include trouble shooting errors, preventive maintenance, and upgrades.

{Map 10} Real-time monitoring of Map Servers shall be performed by the VII Network Operations Entity. The monitoring shall be accomplished in order to determine the condition of each Map Server.

{Map 11} Map Servers shall be monitored to ensure that they are communicating to the network, and that they are operating correctly.

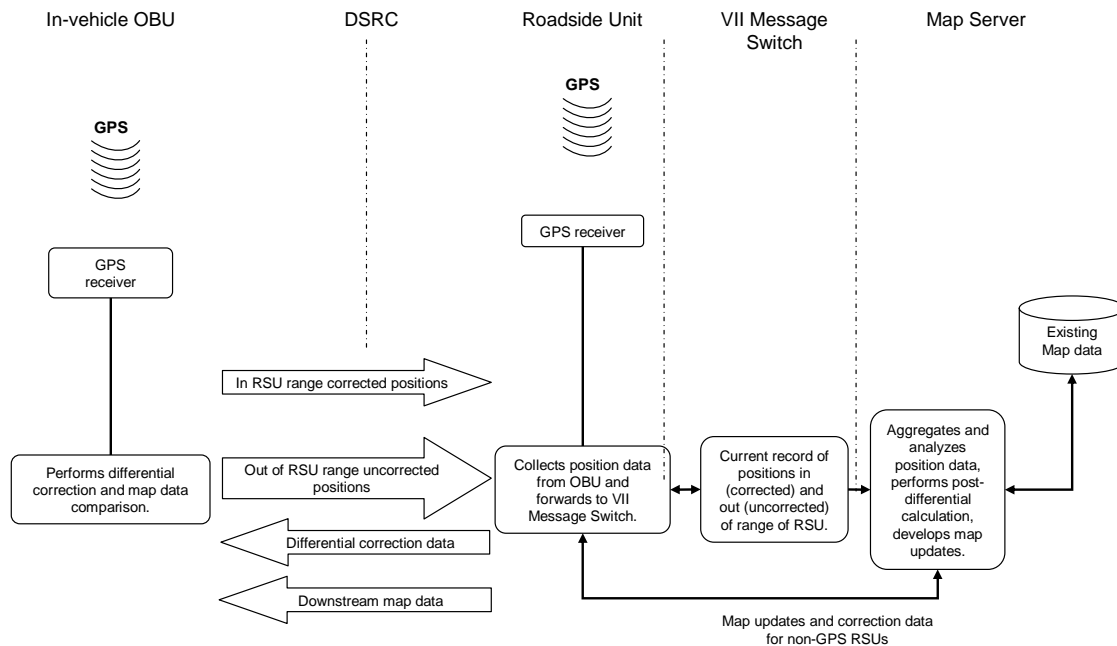


Figure 9-1 Mapping and Positioning Process

9.3. Map Servers Coverage

{Map 12} All RSEs that require map data shall subscribe to a VII Message Switch that shall subscribe to an assigned Map Server.

{Map 13} All Map Servers shall have a specific geographic responsibility to collect vehicle location data from the RSEs in one geographic area.

9.4. Register

{Map 14} The Map Server shall subscribe to all GPS readings from the VII Message Switch.

{Map 15} The Map Server, or if available a local DGPS station, shall publish GPS differential correction messages to the VII Message Switch. If there are local corrections available in addition to the US Coast Guard's Nationwide DGPS Service, the Map Server shall determine the most accurate data by using various techniques such as comparing the current RSU positions with historical positions. The techniques used by the map server to determine best current corrections will need to be updated as new services and data sources become available.

{Map 16} The Map Server shall periodically validate that its assigned VII Message Switch is online.

{Map 17} Should the Map Server detect that the VII Message Switch is currently unavailable, the Map Server shall register with its assigned backup VII Message Switch and continue operations. In the event that all assigned VII Message Switches are unavailable, the Map Server shall cease all operations with the exception of monitoring for valid assigned VII Message Switches and reporting errors.

9.5. Application

9.5.1. Mapping Services

{Map 18} The Map Server shall consist of an application that provides mapping services to the OBUs. These mapping services shall include the provision of accurate map data and the transmission of timely DGPS correction data.

{Map 19} The differential corrections information shall be obtained from the US Coast Guard's Nationwide DGPS Service, or local DGPS station. The Map Server shall be responsible for obtaining the data and producing the appropriate localized pseudo range correction factors for transmission to appropriate RSEs.

9.5.2. Perform DGPS Correction

{Map 20} The Map Server shall receive both current and historic GPS locations from the vehicle.

{Map 21} The Map Server shall store the required differential correction data together with the raw GPS code data for a period defined by a parameter that is set to be greater than the duration of the snapshot data cycle typically available from vehicles. This historic correction information shall be used to correct both the current and the historic GPS locations that the Map Server receives.

{Map 22}] The differential correction data shall be sent from the Map Server through the VII Message Switch to RSEs and into vehicles in a timely manner in order to not adversely affect the required location accuracy.

{Map 23} Note there are alternative differential processes that can be used to perform the correction. These need to be defined in conjunction with the OEMs whose in-vehicle equipment will be performing the calculation.

9.5.3. Corrected GPS Locations

{Map 24} The Map Server shall contain a map that has the capability to be incrementally corrected using probe data from vehicles.

{Map 25} The Map Server shall use statistical techniques to smooth the GPS corrected data to produce map elements. These map elements shall have sufficient integrity for safety applications with a known resolution to provide lane data to the vehicle when the vehicle is driving on those elements that are within transmission range of a RSU that is transmitting GPS corrections. Thus when a vehicle is within range of an RSU it will be able to receive updates to its local map.

{Map 26} The Map Servers shall develop the location of stop and yield signs to supplement the map data. These locations shall be obtained by performing statistical analysis on the GPS data.

9.5.4. Publish Map Correction Data

{Map 27} The map data broadcast from an RSU shall be for all updates within a defined area around an RSU.

10. Network Management

10.1. Network Management Introduction

The VII Network is the element that delivers data from the vehicle to the various Network Users, as well as data and updates from the Network Users to the vehicles. This network is made up of the RSE at the roadside, VII Message Switches, CAs, Map Server and Firewalls as well as the data communications infrastructure supporting communications between these devices and the Network Users.

The network is architected using a publish/subscribe message oriented middleware (MOM) methodology. By this methodology, devices that require data will subscribe for the types of data from the applicable locations which are needed. Data that meets the specifications is then published to the applicable subscribers. Security will be maintained by validation of access level of the specific Network User at the point a subscription is entered.

Management of the VII Network will be carried out centrally from a VII Operations Center(s). The number and placement of these centers and devices contained within will be a function of network traffic and redundancy requirements.

10.2. Network Geographical Scope

The VII Network will provide national coverage in order to receive data from and pass data and updates to vehicles. RSEs will be placed strategically on freeways, arterials and other roads in order to provide for safety and collect the data that is required by the Network Users. A network infrastructure will be in place that will connect all devices on the VII Network and provide for ports into which Network Users may connect.

To provide for management services, it is posited that there will be at least two control centers. Both centers will contain all the VII Message Switches. Each will act as a hot standby for the other and individually support the VII network during maintenance activities. Locating the centers on each coast provides protection during major power failures. There could be more than two centers to provide communication path efficiencies.

10.3. Network Management Requirements

This section deals with the more general network management needs.

{Network Management 1} There shall be a management application that will manage the entire VII infrastructure network including all RSEs on public land, all VII Message Switches, CAs, and Map Servers.

{Network Management 2} The network infrastructure shall provide for online access from any location in the United States.

{Network Management 3} The connectivity shall be through the use of common hubs onto the network.

{Network Management 4} There shall be a nationwide uniformity of network connectivity and functionality.

{Network Management 5} The connectivity and functions that may be provided at any location shall be the same as those provided at all other locations.

{Network Management 6} The VII Network shall consist of all hardware, software, and communications lines that are needed for receipt of messages from the OBU, processing and distributing those messages to the final Network User. The VII Network will not include the OBUs or Network User equipment or connections to the point of presence into the VII Network.

{Network Management 7} Specific devices that are a part of the VII Network shall include, but are not limited to:

- RSEs connected to network
- VII Message Switches
- Map Servers
- CAs
- Firewalls
- Connection all devices, and points-of-presence to Network Users.

Note: RSUs that are not connected to the network (i.e. movable RSUs in work zones) are not considered part of the VII Network.

10.4. Management of the VII Network

A VII Network Operations Entity will be responsible for the design, implementation, expansion, operations and maintenance of the VII Network. The structure of this entity is beyond the scope of this architecture document.

{Network Management 8} The management of the VII Network shall be conducted by the VII Network Operations Entity.

{Network Management 9} In this function, the VII Network Operations Entity shall have various responsibilities that include establishment, running, and managing the network.

{Network Management 10} The VII Network Operations Entity shall establish at least two Operational Centers, one on the east coast and one on the west coast to house much of the infrastructure equipment and manage the network.

{Network Management 11} An IPv6 network covering the United States shall be set up creating an extranet that shall be used to connect all VII Infrastructure equipment and allow points of entry for Network Users.

{Network Management 12} The points of entry shall each have a firewall in order to protect the network from possible destructive penetration.

{Network Management 13} The Operational Centers shall include VII Message Switches, CAs, Map Servers as well as communications infrastructure equipment.

{Network Management 14} Monitoring and oversight of the network and all of this equipment shall be managed by the VII Network Operations Entity.

{Network Management 15} Oversight of the VII Network by the VII Network Operations Entity shall include the oversight and management of the computer operating systems, server infrastructure, and the communications network. Operating systems and related applications running on the various servers will be under the management of the VII Network Operations Entity. This will include testing and installation of new releases and troubleshooting problems.

The computer hardware infrastructure in the Operational Center, which is mainly made up of server machines, will require oversight.

{Network Management 16} Oversight of the Operational Center shall consist of sizing and purchasing, preventive maintenance, installation, backups and restores, health assessments and additional hardware needs assessment.

{Network Management 17} The VII Network Operations Entity shall also be responsible for RSEs that are located at various locations outside of the Operational Center but are connected via the VII Network.

{Network Management 18} Responsibilities shall include installation, configuration, preventive maintenance, health assessments, troubleshooting and correction of errors that occur.

{Network Management 19} Oversight of the VII Network communication network shall be managed from the Operational Center by the VII Network Operations Entity.

{Network Management 20} As part of managing the communications network, capacity, tuning and real-time health shall be supervised. Installation, tuning, troubleshooting and monitoring the network firewall(s) shall be managed as part of the network oversight.

{Network Management 21} In the case that any failures, full or partial, occur, the VII Network Operations Entity shall take the necessary steps to rectify and/or circumvent such failures so as to make the system available to the OBUs and Network Users.

{Network Management 22} The VII Network Operations Entity shall be responsible for configuration management and appropriate updating of software within the VII Network.

{Network Management 23} Configuration management of the software shall consist of tracking the release level, version, and patches of each software component that has been installed on any hardware that is within the VII Network. Record of applicable software and hardware levels shall be maintained on a device basis.

{Network Management 24} The VII Network Operations Entity shall have the ability to install new software, roll-back to previous software, and track the software applications that are needed due to the specific requirements of the piece of equipment (i.e. the placement of the OBU, CPU model of specific servers, etc.).

10.5. Communications Network

With the various interconnections, the VII Network may be referred to as an extranet. The network is likely to use existing facilities from a variety of suppliers.

{Network Management 25} The Communications Network shall be an IP based network running the most current version of IP available at the time that the design of the network has commenced.

{Network Management 26} Communications network exchanges shall occur between: OBUs and RSUs; RSEs and VII Message Switches; VII Message Switches and Map Servers, Map Servers and the US Coast Guard Nationwide DGPS Service, VII Message Switches and CAs, and VII Message Switches and Network Users using an established point-of-presence.

{Network Management 27} Authorization for and support of Network Users connecting to the communications network shall be a function of the VII Network Operations Entity.

{Network Management 28} The support shall include supplying the Network User with documentation of protocols and definition of messages, configuration parameters, and expected service levels.

10.6. Service Level Agreement

A service level agreement is considered a necessary requirement to ensure that the VII system is highly available.

{Network Management 29} The VII Network Operations Entity shall supply a Service Level Agreement (SLA) that will establish operating parameters to be expected for the VII Network.

{Network Management 30} The Network availability shall be defined by the Operations Entity. The network shall be configured in a manner that allows for full time operation with, at a minimum of two fully redundant centers one located on each coast.

{Network Management 31} The SLA shall include definitions and support descriptions and related measurement metrics covering:

- Configuration management
- Version control and upgrades
- Support of communications and other system elements
- Maintenance of system elements
- Restores and disaster recovery
- Support hours
- Support of network users
- Enhancement support
- Systems administration support
- Maintenance of security levels
- System availability
- Notification of problems to network users and management
- Reporting

10.7. Network Security

{Network Management 32} The VII Network shall be designed as an extranet connecting various Network Users to the network operated by the VII Network Operations Entity. Network Users, being connected to their own networks in addition to the VII Network have the possibility of allowing access to the network from the Internet.

{Network Management 33} Protection of the VII Network is of paramount importance. In order to protect the network from attacks originating through an Internet connection, various protections shall be in place. Included are firewalls, virus protections, and access level security.

The VII Network shall include firewalls to protect all points-of-presence to the network.

The firewalls shall ensure that only authorized messages are passed between the Network User and the VII Network.

The firewall shall also be configured in order to prevent denial of service attack.

{Network Management 34} All devices on the VII Network shall include virus protection to prevent virus attacks to the system. The virus protection shall be updated as updates are available.

{Network Management 35} As a function of setting up a new Network User the VII Network Operations Entity shall assign their access security.

{Network Management 36} The assigned access security shall be at the appropriate level on a need to know basis.

It should be remembered that once data has been published to the Network User, the VII Network Operations Entity has no control of future data distribution or data retention.

10.8. Network Monitoring

{Network Management 37} The VII Network Operations Entity shall be responsible for monitoring the communications network in order to manage the current operations and future growth. The communications network shall be monitored to ensure that network errors are received and managed.

{Network Management 38} The communications network traffic shall be balanced to enable the best possible throughput of messages between the OBU and Network Users. This may be accomplished by changes to the network infrastructure, the number and assignment of VII Message Switches, and related configurations of hardware. Primary logical connectivity of devices to VII Message Switches shall be changed by the VII Network Operations Entity as needed in order to optimize the network message throughput.

{Network Management 39} The VII Network Operations Entity shall be responsible for ongoing capacity planning for the VII Network.

{Network Management 40} Proactively, the VII Network Operations Entity shall recommend upgrades that are needed to the network in order to continue to support the number of

messages that are to be received from the OBUs and the amount of data that will be sent to the Network Users.

10.9. Provisioning of RSEs

{Network Management 41} The VII Network Operations Entity shall be responsible for determining need, acquiring, installing, maintaining, and debugging issues with RSEs. Placement of new RSEs will be the responsibility of the VII Network Operations Entity. Requests for new placements may be made by qualified institutions to the VII Network Operations Entity. Once approved, the RSEs will be installed. As part of the installation, a security certificate shall be issued to the RSE which it may use as a part of the security infrastructure for the device.

{Network Management 42} Software / firmware support for RSEs shall be the responsibility of the VII Network Operations Entity.

Software support shall include initial installation of applicable software, upgrades to software, upgrades to Service Tables, additional software for new functions within an RSU, and changing the primary VII Message Switch connection for the RSU.

Where possible, the support shall be performed remotely from the VII Operations Center. Upgrades to the Service Table may also be initiated by Network Users with the appropriate security levels.

{Network Management 43} Hardware support for RSEs shall be the responsibility of the VII Network Operations Entity

Where possible the support shall be performed remotely from the VII Operations Center.

Provided support shall include trouble shooting errors, rebooting, preventive maintenance, and upgrades.

{Network Management 44} The VII Network Operations Entity shall monitor and support RSEs at times of power outages and loss of data lines.

{Network Management 45} The VII Network Operations Entity shall be responsible for adding new functions to RSEs. The functions may include additional software and/or additional hardware. The new hardware and software may be connected to the RSE via the I/OC as part of a Local Safety System.

{Network Management 46} Real-time monitoring of RSEs shall be performed by the VII Network Operations Entity.

The monitoring shall be accomplished in order to determine the condition of each RSE.

RSEs shall be monitored to ensure that they are communicating to the network, and that they are operating correctly.

10.10. Provisioning of VII Message Switches

{Network Management 47} The VII Network Operations Entity shall be responsible for determining need, acquiring, installing, maintaining, and debugging issues with VII Message Switches. Additions of new VII Message Switches shall be the responsibility of the VII Network Operations Entity.

New VII Message Switches shall be added to the network as the volume and flow of messages require.

Planning for future growth and adding associated VII Message Switches shall also be the responsibility of the VII Network Operations Entity.

{Network Management 48} Software support for VII Message Switches shall be the responsibility of the VII Network Operations Entity.

Software support shall include initial installation of applicable software, and upgrades to software.

{Network Management 49} The VII Network Operations Entity shall be responsible for setting and administrating rules within the VII Message Switch for data security of the system. The data security rules may include limiting the message sizing for specific Network Users, and authorization for individual Network Users ability to access specific types of data from specific types of vehicles.

{Network Management 50} Hardware support for VII Message Switches shall be the responsibility of the VII Network Operations Entity.

Provided support shall include trouble shooting errors, preventive maintenance, and upgrades.

{Network Management 51} Real-time monitoring of VII Message Switches shall be performed by the VII Network Operations Entity.

The monitoring shall be accomplished in order to determine the condition of each VII Message Switch.

VII Message Switches shall be monitored to ensure that they are communicating to the network, and that they are operating correctly.

10.11. Connectivity of Network Users

{Network Management 52} The VII Network Operations Entity shall set and execute rules allowing organizations to join the VII Network as a Network User.

{Network Management 53} Once approved for entry onto the network, a new Network User shall be given the appropriate level of access to data by the VII Network Operations Entity.

{Network Management 54} The VII Network Operations Entity shall supply the Network User with documentation that explains the applicable message protocols, methods for connecting to the hub, the assigned hub, and VII Message Switches.

{Network Management 55} Communications network support shall be supplied by the VII Network Operations Entity according to the standards that have been established in the SLA.

10.12. Reports

The VII system will provide too much data to store and it is not the intent to provide reports on the data passing through the network. The reports relate to network functions are the mechanism to be used in configuring and updating the network elements as the system expands and modifies.

{Network Management 56} The VII Network Operations Entity shall provide reports that indicate the state of the network.

1. The reports shall indicate the current environment within which the VII Network is working and metrics that describe the network utilization.
2. A report shall be available to subscribers that indicate the location and status of each RSE.
3. This report shall be produced dynamically in order to obtain current information.
4. These reports shall include historical and current metrics which will be able to show trends in network usage. The metrics shall be produced for the network as a whole, and for the selected portions defined by the enquirer.

11. Network User

11.1. Network User Introduction

A Network User, although connected to the VII system, will need to have authorization to access the VII data. There are no explicit functional requirements for the Network User applications as they are the responsibility of these institutions. The Network User requirements that are included here relate to connection to the VII network.

The Network Users will require applications outside the VII network that:

- Use the VII public data
- Supply data to be broadcast to vehicles within range of RSUs
- Perform private transactions with individual vehicles

11.2. Network User Requirements

11.2.1. Registration and Connectivity

{Network User 1} Each Network User shall register with an assigned VII Message Switch. In addition, the Network User shall register with a backup VII Message Switch for use when the assigned switch is unavailable. The assignment of the VII Message Switches shall be the responsibility of the VII Network Operations Entity.

{Network User 2} The Network User shall register to the VII Message Switch to ensure continuing connectivity.

{Network User 3} The Network User shall periodically validate that the VII Message Switch is on-line.

{Network User 4} The Network User shall register as a subscriber to obtain the data from the VII Message Switch.

11.2.2. Subscription Control and Management

{Network User 5} The VII Network Operations Entity shall control and manage functions that exist in all VII Message Switches. This control shall include VII Message Switch software updates, message priorities and rights concerning the publishing of data.

{Network User 6} Only authorized users shall be allowed to subscribe to VII data.

{Network User 7} The rules within the VII Message Switch shall limit the external users to those that are authorized. The public sector users shall be able to subscribe to all public sector data.

11.2.3. Network User Data

The data available to the public sector users will consist of the data elements defined in Appendix A. The public sector data will consist of the two data types, periodic and event.

These data will be parsed into individual data elements in the VII Message Switch. The figure illustrates a public data message format as the message leaves the OBU.

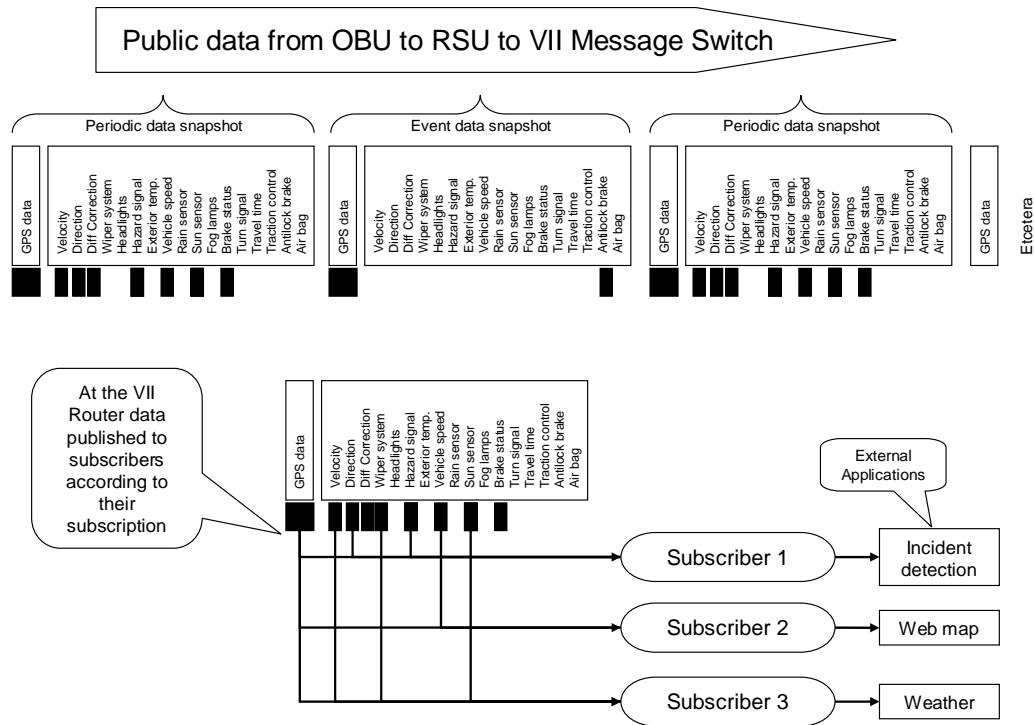


Figure 11-1 VII Public Data Message Format

{Network User 8} At the VII Message Switch, the data shall be published to the various subscribers in accordance with the subscriber requests and the rules that apply to that router.

11.2.4. OBE Specific Messages

These applications will reside in the vehicles. In several of these applications, the vehicles are looking at other vehicle locations and vectors to determine the potential for collision and then respond accordingly. These applications require the mapping support that was described earlier. Without the mapping process, several of these applications either would not function or would require equivalent functionality from other sources, such as an on-board accurate map.

This architecture does not explicitly address the data flow between vehicles. This is considered the province of the OEMs who are developing likely applications that will run within the vehicles. However, there are bandwidth limitations that will affect the link between the vehicles and the RSU since the V-V communications will use the same set of frequencies. There is a concern that the V-V communications load could affect the messaging to the RSUs. This issue and methods of reducing the potential conflicts are currently under investigation by the OEMs.

In addition, this architecture will support those functions such as airbag activation notifications and other emergency messages from the vehicle for those vehicles within range of an RSU. Although the RSUs by virtue of their licensing have limited range, within an urban environment their density is likely to be significant.

{Network User 9} Network Users may send messages to specific OBUs requesting data. These messages shall be private. The process shall operate as follows:

Step 1 – The Network User shall download to an RSE an element for the Service Table. The RSE shall incorporate this element into its Service Table.

Step 2 – The RSU shall periodically broadcast a Service Table indicating the services offered at that RSE.

Step 3 – If so equipped, the OBU shall respond with a response for the Network User application. When an OBU receives a PST, it will see if any of the application provided by the RSU exists in the OBU. If a match is found the OBU responds. If no match is found, the OBU will not respond.

Following the OBU response, the OBU/RSU will have to develop an IP address that can be used for communications. The Network User Application' shall then extract the OBU identification within the application and then direct traffic to the specific OBU. When an OBU leaves a communication zone of one RSU and enters the communication zone of another RSU the process must be repeated since a unique ID may be used by the OBU for each RSU transaction.

Step 4 – The RSU forwards the data, its address and the OBU address to its VII Message Switch.

Step 5 – According to its subscriptions, the VII Message Switch forwards the OBU's response and the address of the RSU to the Network User.

Step 6 – The Network User shall send a message to the VII Message Switch together with the RSE address.

Step 7 – The VII Message Switch shall send the message to the RSE that shall transmit it to the originating OBU.

Steps 3 through 7 may continue indefinitely within physical range and communications capacity limitations.

{Network User 10} Network Users shall have the capability to subscribe to the current status of all RSEs.

{Network User 11} Authorized Network Users shall have the capability to send messages to an RSE for broadcast. The RSU shall broadcast the message to all OBUs within range of an RSU. These messages to the RSE shall incorporate a timeout for the broadcast message, after which the RSU shall stop broadcasting it.

12. Security

12.1. Security Introduction

There are a range of security issues associated with VII. These include institutional, operational, physical and others. These have not yet been determined, and when they do, many of them will be beyond the scope of the architecture. However, it has been proposed that the Public Key Infrastructure (PKI) process be used for the messages on the VII network.

All messages within the VII system will be protected by the use of digital signatures. The process used will be asymmetric PKI as illustrated in the diagram.

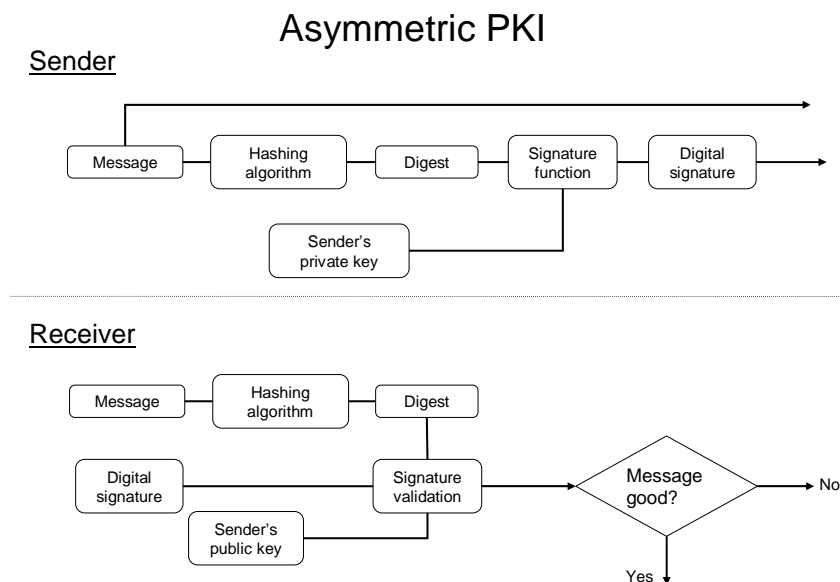


Figure 12-1 Asymmetric PKI Message Security

Both the private key and the public key are obtained from a Certification Authority, a trusted source that can be accessed by both sender and receiver.

12.2. Certification Authority

{Security 1} The certification authority (CA) shall be the GSA. The CA may designate trust anchors that are other subsidiary entities that are entitled to provide certificates.

12.3. Certificate Content

{Security 2} Each certificate shall contain at least four data items:

- The public key of the certificate holder
- The scope of the certificate defining the geographical scope for RSEs and the functions for which the certificate is valid

- Expiry time
- A digital signature

12.4. Digital Signature in RSU

{Security 3} When an RSE is installed it shall be connected to the CA through the VII Message Switch and the initial registration process shall occur. The CA administrator shall interrogate the RSE and keep a record of its public key together with its identity (serial number) and permissions.

{Security 4} The CA shall determine what functions that RSE is to perform.

{Security 5} Each RSE shall then be issued a certificate by the CA that indicates its location and the messages that it is permitted to send.

12.5. Digital Signature in OBUs

{Security 6} The OEMs shall be authorized as trust anchors to install digital certificates in the OBEs.

{Security 7} Each OBE shall have a large number of key pairs.

12.6. Certificate Revocation Lists

{Security 8} Certificate Revocation Lists (CRL) shall be distributed to the RSEs as part of the VII network management function. The RSEs shall download CRLs to the OBUs on an occasional basis.

12.7. OBU Physical Protection

{Security 9} The OBE shall be configured to lose its certificates upon being physically opened.

12.8. RSU Location Checking

{Security 10} The OBU, upon receipt of the GPS time and location, shall perform validity checks on the data for valid proximity and time.

12.9. RSU Data Security

The RSE will provide for verification of message authenticity for those safety messages that are sent to and received from an OBU.

{Security 11} The RSE shall store a valid PKI Certificate for transmission of its digital signature. This shall act as assurance to an OBU that the RSU is a trusted source.

{Security 12} The digital signature shall be sent out by the RSU as a portion of the RSU Service Table Broadcast message to the OBU.

{Security 13} The RSE shall validate messages that have been received from the OBU by use of the OBU's digital signature. The OBU's public key will be received as part of the PKI Certificate that will have been transmitted to the RSU.

13. Appendix A – VII Public Data Items from the Vehicle

VII Public Use Case Data Elements [†]			
	Usage	Range	Comment
Periodic data snapshots			
Vehicle position data	Location, direction and traffic data		
Differential Correction status	Map update process	0..1	Not corrected, Corrected
Year	Wide range of use cases relating relevant variables to	0-255	Offset year 2000
Month		1..12	
Day	Geographic Information Systems	1...31	
Hours		0..23	
Minutes		0..59	
Seconds		0..59	
Latitude zone		0..1	0 =North, 1=South
Latitude degree		0..90	
Latitude minute		0..59	
Latitude sub minute		0..9999	
Longitude zone		2..3	2=East, 3=West
Longitude degree		0..179	
Longitude minute		0..59	
Longitude sub minute		0..9999	
Altitude		-400..+4000	Meters and decimal meters positive and negative relative to sea level
Velocity		0..255	
Direction		0..359	
Vehicle type		1-15	FHWA categories see appendix C
MAC Address	Identifies specific vehicles.		Will not be transmitted beyond the RSU.
Wiper system state	Real-time rain detection; for operations and maintenance	0..5	No wiper, Off, Intermittent, Slow , Fast, Maintenance
Headlights	Indicator of lighting conditions	0..4	Off, Low, High, Flash, High Flash
Hazard signal	Provides potential incident locations or disabled vehicle	0..1	Off, On
Exterior temperature	For use by maintenance divisions to determine ice and snow conditions	"-40..150	Degrees C
Vehicle speed	Traffic data	1bit=0.1kph	Alternate to GPS when signal lacking Note: Not all vehicles will have all devices therefore when possible duplication is desirable.

VII Public Use Case Data Elements [†]			
	Usage	Range	Comment
Rain sensor	Used by maintenance divisions, operations staff and incident detection algorithms	0-255	0 = No rain
Sun sensor	Used by maintenance divisions, operations staff and incident detection algorithms	0-16	Watts/m ²
Fog lamps	Possible by operations staff as fog indicator	0..2	None, Off, On
Brake applied status	Within range of an RSU, can be used for incident and queue detection	1,2 or 3	Off, On, Engaged
Wheel angle	For map generation	0-359	Angle is tangent to map spline
Turn signal	For use in new adaptive traffic control algorithms	0, 1, 2	Off, Right, Left
Travel Time	For use in TOCs		Change in odometer reading and time passed since last RSU with probe AID
Event-driven data		0..59 0..59 1bit=0.1	Minutes Seconds Kilometers Event data will be logged together with GPS information
Traction control state	To provide information on poor road surface locations	1,2 or 3	Off, On, Engaged
Antilock brake system state		1,2 or 3	Off, On, Engaged
Air bag activations	For incident detection	0..1	Not Deployed, Deployed

[†]Data derived from AMI-C Common Message Set v 1.01 2003-03-07

14. Appendix B VII Acronyms and Glossary

AASHTO – American Association of State Highway and Transportation Officials – A nonprofit, nonpartisan association representing highway and transportation departments in the 50 states, the District of Columbia and Puerto Rico.

AID – Application Identification, a designation of an application that is supported by a VII element such as a RSE or OBE. A list of AIDs is included in the PST and UST.

AMI-C – Automotive Multimedia Interface Collaboration; an organization representing many of the world's vehicle producers, coming together to create an open and free standard that will allow in-vehicle electronics to be easily incorporated into vehicles.

ASTM – American Society for Testing and Materials; one of the largest voluntary standards development organizations in the world, a source for technical standards for materials, products, systems, and services.

VSC – Vehicle Safety Communications Project – A partnership of seven automotive company organizations, working in partnership with the USDOT, communications-based vehicle safety applications.

Certification Authority (CA) – A trusted third party that issues digital certificates to entities which are to be used to validate the reliability of the data being transmitted.

Control Channel – A communications channel reserved for managing the allocation of transmissions to the other communications channels associated with an application.

CSP - Content Service Providers A company that is in the business of providing information to VII equipped vehicles on a commercial basis

DGPS – Differential GPS; a service that achieves greater position accuracy than GPS through broadcasts of corrections to GPS signals

DIC – DSRC Prototype team creating the standards and prototypes to verify them

Digital Certificate – A message sent by an entity that will provide information on the sending entity and the entity's public key in order for the receiver to validate that data being received is reliable.

Digital Signature – In order to validate that the sender is valid, this is encrypted information about the sender of the message that may be decrypted using the attached public key.

DOT – Department of Transportation; an organization responsible for transportation services in a political jurisdiction such as a State or city.

DSRC – Dedicated Short Range Communications; a wireless (radio) communications approach that enables short range communications between vehicles and between vehicles and the roadside for a variety of purposes.

DSRCS – Dedicated Short Range Communications Service; a term used by the FCC to describe the applications enabled through a DSRC communications link.

E-911 – Enhanced 911; technologies implemented on wireless telephone systems that enable the determination of a caller's location.

Ethernet - A family of local-area network (LAN) technologies covered by the IEEE 802.3 standard.

FCC – Federal Communications Commission; an independent US government agency, directly responsible to Congress, charged with regulating interstate and international communications by radio, television, wire, satellite, and cable.

FHWA – Federal Highway Administration; an operating administration of the United States Department of Transportation.

FIFO – First In First Out; a method of defining how items in a list are handled.

GIS – Geographic Information System; a map based system that enables display of layers of data for various analysis purposes.

GPS – Global Positioning System; a worldwide radio-navigation system formed from a constellation of 24 satellites and their ground stations. GPS calculates positions accurate to a matter of meters.

GHz – Gigahertz; one billion hertz; a unit of measurement for high frequency DSRC transmissions.

HA-DGPS – High Accuracy Differential GPS that uses the multiple DGPS radio signals to provide centimeter accuracy positioning.

HALL – High Availability Low Latency; a descriptor of a DSRC channel used for safety messages

HMI – Human Machine Interface; a term used to describe the process of human interactions with a system.

IEEE – Institute of Electronic and Electrical Engineers; an organization that promotes the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences for the benefit of humanity and the profession.

IETF – Internet Engineering Task Force; a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IP – Internet Protocol; the world's most popular open-system (nonproprietary) protocol suite used to communicate across any set of interconnected networks.

ISDN – Integrated Services Digital Network; a system of digital phone connections that allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity.

ISM - industrial-scientific-medical frequency band (902-928 MHz, 2400-2483 MHz, 5725-5780 MHz) Industrial Scientific & Medical (unlicensed frequency bands 915 MHz, 2.4 & 5.725 GHz)

ITS – Intelligent Transportation Systems; a broad range of communications-based information, control, and electronics technologies integrated into the transportation system infrastructure, and in vehicles themselves, to help monitor and manage traffic flow, reduce congestion, provide alternate routes to travelers, enhance productivity, and save lives, time, and money.

IVI – Intelligent Vehicle Initiative; a part of the USDOT's ITS program that is aimed at investigating the application of technologies and systems to reduce driver distraction and facilitating the accelerated development and deployment of crash-avoidance systems.

IVSAWS – In-Vehicle Safety Advisory and Warning Systems; a term used to describe in-vehicle information systems that provide drivers with advance, supplemental notification of dangerous road conditions using electronic warning zones with precise areas of coverage.

LAN – Local Area Network; a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area.

Local Safety Systems – Hardware and/or software used to assist in safety applications that are located close to the RSU. The devices may, but are not required to be ITS devices.

Local Users – Safety equipment, ITS equipment, systems and the like that are local to the intersection in which the RSU is located and connected directly to the Input/Output Controller (I/OC).

Mbps – Megabits per second; millions of bits per second; a measure of bandwidth over a communications medium.

MHz – Megahertz; one million hertz; a unit of measurement for medium frequency DSRC transmissions.

MOM – Message oriented middleware.

msec – Millisecond; one thousandth of a second.

Network Users – Public and private users of data received using the VII Network infrastructure.

OBU – On-Board Unit; a collection of electronic equipment within a vehicle that assembles GPS and vehicle sensor data and transmits it via a wireless communications link to roadside infrastructure, other processing sites, and other vehicles.

OVHI – OBU-Vehicle Host Interface where it provides host interface between OBU and Vehicle such as Ethernet connection.

OD – Origin / Destination; a term used in transportation planning; the matrix that describes the location of all trip origins and destinations in a transportation network.

OEM – Original Equipment Manufacturers; a term used to describe those companies that are the original manufacturers of vehicles and equipment.

OSI – Open Systems Interconnection; a program that grew out of the need for international networking standards, designed to facilitate communication among systems despite differences in underlying architectures by implementing a protocol suite that comprises numerous standard protocols based on a standard OSI reference model.

PKI – Public Key Infrastructure; the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

Public Sector – Those institutions such as cities, states, counties, toll authorities, and federal agencies that have a need for the VII data.

Publish – When an entity that has data to distribute receives a subscription request it checks the validity of the request in order to be assured that the subscribing entity is entitled to a copy of the data. Following verification of the subscriber's right to the data the requested information is subsequently sent (published) to the subscriber. New data is sent when received and the transmission continues until the entity leaves the network.

PSAP – Public Safety Answering Point; a site operated by a county, a municipality, or other governmental jurisdiction for the purpose of answering 911 emergency calls placed by the public.

PSRSUs - Public Safety RSUs; RSUs mounted on emergency vehicles, school buses etcetera.

PST – Provider Service Table; a list of information that defines the applications a specific RSU can provide – see UST.

P&S – the combination of Publish and Subscribe

Register – when an entity requires data from another entity it must register its presence. Entities include the VII devices such as Routers and RSUs and also include institutions such as highway authorities, Cities and CSPs. A communication setup process referred to as registration provides information concerning electronic addresses and the identity of the entity requesting information and subscription information.

RF – Radio Frequency; a term used to describe the set of frequencies between normally audible sound waves and the infrared light portion of the spectrum.

RSE – Road Side Equipment; Includes the RSU, processors, and all interfaces that are put on the roadside in order to receive and process OBU data.

RSU – Road Side Unit; a DSRC transceiver that exchanges data with OBUs in its communications zone,.

RSU Service Table Broadcast – the initial broadcast sent out regularly by the RSU that informs the OBU of the RSU's existence and the services that it provides.

SAE – Society of Automotive Engineers; an individual member organization that is a resource for standards development, events, and technical information and expertise used in designing, building, maintaining, and operating self-propelled vehicles.

Service Table – Service Tables identify the services that may be provided between the RSU and the OBU.

Subscribe – As part of the registration process an entity requiring certain data needs to subscribe in order to obtain the data. Subscribing involves sending a request for specific data messages. Once a subscription is accepted the appropriate messages will then be published to the subscriber.

TOC – Transportation Operations Center; a generic term that describes any control center with hardware and software that is used to monitor and manage transportation system operations.

USDOT – United States Department of Transportation; a Cabinet-level Department that exists to serve the United States by ensuring a fast, safe, efficient, accessible, and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future.

UST – User Service Table; a list of information that defines the applications a specific OBU can provide – see PST.

V-V – Vehicle-to-Vehicle; a term used to describe data communications between individual vehicles in a traffic stream.

VII – Vehicle Infrastructure Integration; a cooperative program among State DOTs, OEMs, and the USDOT aimed at making travel safer, more efficient, and more convenient; providing business opportunities; and improving customer relations by enabling communication of sensor data between vehicles and the infrastructure and between vehicles.

VII Message Switch – A device used to distribute VII data to the various users that have subscribed.

VII Network – Includes the RSEs, VII Message Switch, and Network Users, Map Server and CA.

VII Network Operations Entity – This is the organization or institution that will be responsible for the operations and maintenance of the VII System.

VSCC – Vehicle Safety Communications Consortium; consisting of several OEMs, the objective of the Consortium is to facilitate the advancement of vehicle safety through communication technologies and to assess associated communication requirements including vehicle-to-vehicle and vehicle-to-infrastructure communications.

WAAS – Wide Area Augmentation System; signals from additional satellites are beamed to GPS units that provide higher accuracy; designed to assist in aircraft landing.

WiFi – Wireless Fidelity; a wireless technology that enables computers to send and receive data anywhere within the range of a base station. WiFi networks apply IEEE 802.11b or 802.11a standards to provide secure, reliable, fast wireless connectivity.

WSM – Wave Short Message, a DSRC protocol that allows short messages to bypass the queue in order to support low latency safety messages

15. Appendix C FHWA Vehicle Types²⁵

VEHICLE_CLASS refers to the FHWA 13-bin vehicle classification system (table 4). (Note that although the classification system is named 13-bin for historical reasons, it has 15 categories.)

FHWA 13-bin vehicle classification system

Vehicle Class	Description
1	Motorcycles
2	Passenger cars
3	Other 2-axle, 4-tire single-unit vehicles
4	Buses
5	2-axle, 6-tire single-unit trucks
6	3-axle single-unit trucks
7	4- or more axle single-unit trucks
8	4- or less axle single-trailer trucks
9	5-axle single-trailer trucks
10	6- or more axle single-trailer trucks
11	5- or less axle multi-trailer trucks
12	6-axle multi-trailer trucks
13	7- or more axle multi-trailer trucks
14	Unclassifiable
15	Partial vehicles, including offscale or lane-changing vehicles

²⁵ <http://www.tfrc.gov/pavement/ltpa/reports/03088/12.htm>

16. Appendix D. Example Use Case

Use Case name: Infrastructure-Based Curve Warning

Description:	Provide warnings to drivers, through infrastructure signs or in-vehicle driver-vehicle interface devices, that their speed must be reduced to safely traverse the impending curve				
Required devices:	Vehicle On-vehicle processor On-vehicle driver warning interface On-vehicle location device such as GPS On-vehicle transceiver such as DSRC OBU OBU-to-vehicle services interface Infrastructure Roadside controller or processor Roadside vehicle detectors Road surface condition sensor (optional) GPS differential correction sensors Infrastructure data transceiver such as DSRC RSU Roadside advisory signs				
Required services:					
Prior conditions:					
Flow of events					
Vehicle approaches a curve in the roadway					
1. Infrastructure provides carrier phase differential GPS, identifies location and presence of curve, and road surface condition data (optional).					
2. Infrastructure sensors and processor determine vehicle type, and safe speed for the curve and whether the vehicle must reduce speed more quickly for each vehicle type, based upon the vehicle classification detectors, the specific roadway characteristics for the curve, and (optionally) the current road surface condition.					
3. Roadside unit activates dynamic message sign to advise driver of safe speed for the curve and whether the vehicle must decelerate faster to safely traverse the curve.					
4. Roadside unit provides message to vehicle (identified by location) of safe speed to traverse the curve and whether the vehicle must decelerate faster, by vehicle type, and assumed vehicle type.					
5. Vehicle provides current speed, current location, vehicle type, and (optionally) vehicle performance characteristics; uses location of the curve and safe speeds by vehicle type from the infrastructure; and determines the safe speed for the curve and whether the vehicle must decelerate faster.					
6. Vehicle determines need to provide advice to the driver.					
7. The driver is advised of a safe speed to traverse the impending curve and of the need to decelerate, either from the roadside signs or from the in-vehicle interface, and reduces speed accordingly.					
Optional devices:	Road surface condition sensors.				
Actors:	Vehicle System	Occupant		Service Provider	Road Department
		Driver	Passenger		
	X	X			X