



CVISN Guide Series



# CVISN Guide to Safety Information Exchange

POR-99-7191  
Draft Version D.1  
March 2000

**CVISN Guide to  
Safety Information Exchange**

**POR-99-7191  
Draft Version D.1**

March 2000

**Note**

*The Motor Carrier Safety Improvement Act was signed into law on December 9, 1999. This act established a new Federal Motor Carrier Safety Administration (FMCSA) within the US Department of Transportation (DOT), effective January 1, 2000. Prior to that, the motor carrier and highway safety program was administered under the Federal Highway Administration (FHWA).*

*The mission of the FMCSA is to improve truck and commercial passenger carrier safety on our nation's highways through information technology, targeted enforcement, research and technology, outreach, and partnerships. The FMCSA manages the ITS/CVO Program, a voluntary effort involving public and private partnerships that uses information systems, innovative technologies, and business practice reengineering to improve safety, simplify government administrative systems, and provide savings to states and motor carriers. The FMCSA works closely with the FHWA's ITS Joint Program Office (JPO) to ensure the integration and interoperability of ITS/CVO systems with the national ITS program.*

**DRAFT ISSUE**

IT IS IMPORTANT TO NOTE THAT THIS IS A DRAFT DOCUMENT. The document is incomplete and may contain sections that have not been completely reviewed internally. The material presented herein will undergo several iterations of review and comment before a baseline version is published.

This document is disseminated in the interest of information exchange. JHU/APL assumes no liability for its contents or use thereof. This report does not constitute a standard, specification, or regulation. JHU/APL does not endorse products or manufacturers. Trade and manufacturer's names appear in this report only because they are considered essential to the object of this document.

Note: This document and other CVISN-related documentation are available for review and downloading by the ITS/CVO community from the JHU/APL CVISN site on the World Wide Web. The URL for the CVISN site is: <http://www.jhuapl.edu/cvisn/>

Review and comments to this document are welcome. Please send comments to:

Mr. Paul North  
JHU/APL CVISN Project  
11100 Johns Hopkins Road  
Laurel, MD 20723

Phone: 240-228-6627  
Fax: 240-228-6620  
E-Mail: [paul.north@jhuapl.edu](mailto:paul.north@jhuapl.edu)

---

**CVISN GUIDE TO SAFETY INFORMATION EXCHANGE****Table of Contents**

1.	INTRODUCTION.....	1-1
2.	WHAT IS SAFETY INFORMATION EXCHANGE? .....	2-1
3.	WHAT ALREADY EXISTS? .....	3-1
3.1	Products Used By Carriers And Other Third Party Users .....	3-1
3.2	Products Used By States.....	3-1
3.2.1	State Infrastructure Systems .....	3-1
3.3	CVISN Core Infrastructure Systems .....	3-10
3.3.1	Motor Carrier Management Information System .....	3-10
3.3.2	Safety and Fitness Electronic Records System.....	3-12
3.3.3	Commercial Driver License Information System.....	3-16
3.4	Data Interchange Standards .....	3-17
4.	OPERATIONAL CONCEPTS AND SCENARIOS.....	4-1
4.1	Key Operational Concepts.....	4-2
4.2	Operational Scenarios.....	4-4
4.2.1	Example Operational Scenario: Record Inspections Electronically and Report Them to SAFER and MCMIS in 2000 (ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0).....	4-5
5.	CRITICAL DECISIONS.....	5-1
5.1	Design Decisions .....	5-1
5.2	Planning Decisions .....	5-3
5.3	Funding and Contracting Decisions .....	5-5
5.4	Development Decisions.....	5-5
6.	REQUIREMENTS AND DESIGN GUIDANCE.....	6-1
6.1	Safety Information Exchange – Conforming With the Architecture.....	6-1
6.2	Focus on ASPEN or Its Equivalent .....	6-4
6.2.1	Design Options .....	6-5
6.2.2	Data Exchange Formats .....	6-7
6.3	Focus on CVIEW.....	6-8
6.3.1	Design Options .....	6-9
6.3.2	Data Exchange Formats .....	6-10
6.3.3	FMCSA Development and Maintenance Support for CVIEW .....	6-11

6.4	Focus on SAFER .....	6-12
6.4.1	Design Options .....	6-13
6.5	Focus on Communications .....	6-15
6.5.1	SAFER Communications.....	6-15
6.5.2	CVIEW Communications.....	6-16
6.5.3	SAFETYNET Communications .....	6-17
6.5.4	ASPEN, or equivalent, Communications .....	6-17
6.5.5	ROC Communications.....	6-17
7.	RECOMMENDED DEVELOPMENT PROCESS.....	7-1
7.1	Development Process Overview.....	7-1
7.2	Top Level Design Phase .....	7-3
7.3	Program and Project Planning Phase.....	7-6
7.4	Funding and Contracts Phase.....	7-8
7.5	Development Phase "n" .....	7-11
7.6	Requirements Specification.....	7-14
8.	SAFETY INFORMATION EXCHANGE IN THE CVISN MODEL DEPLOYMENT STATES .....	8-1
8.1	California.....	8-1
8.2	Colorado .....	8-2
8.3	Connecticut.....	8-4
8.4	Kentucky.....	8-4
8.5	Maryland.....	8-5
8.6	Michigan.....	8-6
8.7	Minnesota .....	8-9
8.8	Oregon .....	8-9
8.9	Virginia.....	8-10
8.10	Washington.....	8-11
9.	INTEROPERABILITY ISSUES/STATUS .....	9-1
9.1	Issues .....	9-1
9.2	Interoperability Tests.....	9-2

---

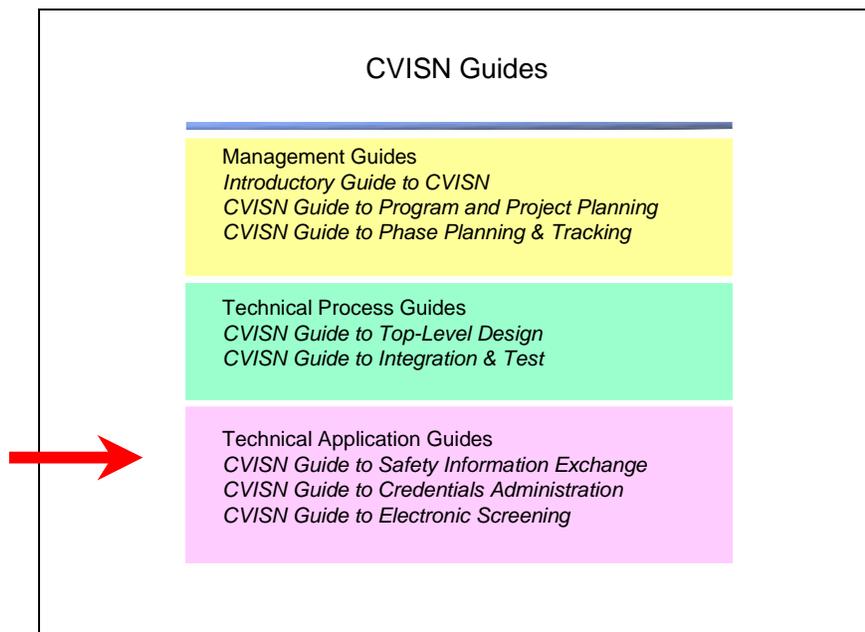
10.	LESSONS LEARNED – SAFETY INFORMATION EXCHANGE.....	10-1
10.1	Lessons Learned – California .....	10-1
10.2	Lessons Learned – Colorado .....	10-2
10.3	Lessons Learned – Connecticut.....	10-2
10.4	Lessons Learned – Kentucky.....	10-2
10.5	Lessons Learned – Maryland.....	10-2
10.6	Lessons Learned – Michigan.....	10-2
10.7	Lessons Learned – Minnesota .....	10-2
10.8	Lessons Learned – Oregon .....	10-2
10.9	Lessons Learned – Virginia.....	10-3
10.10	Lessons Learned – Washington.....	10-3
	APPENDIX A. REFERENCES .....	A-1
	APPENDIX B. PRISM AND CVISN – EXPLAINING THE RELATIONSHIP .....	B-1
	APPENDIX C. OPERATIONAL SCENARIOS AND FUNCTIONAL THREAD DIAGRAMS .....	C-1

This Page Intentionally Blank

# 1. INTRODUCTION

Safety Information Exchange is one of the three key program areas in Commercial Vehicle Information Systems and Networks (CVISN) Level 1. The CVISN Guide to Safety Information Exchange provides reference information and offers advice about implementing safety information exchange functions in CVISN.

This is one in a series of guides. The other guides are available from the CVISN web site (<http://www.jhuapl.edu/cvo/>). The list of CVISN Guides is shown in Figure 1-1.



**Figure 1-1. CVISN Guides**

## Factors to Consider in Safety Information Exchange

Some factors that should be considered when working in the safety information exchange area are:

- One of the more critical decisions a state needs to make is how to integrate inter- and intrastate safety information and provide it to the roadside to facilitate electronic screening and inspection operations, i.e., what approach will a state use building and deploying a Commercial Vehicle Information Exchange Window (CVIEW) system or its equivalent.
- The development process for CVIEW or its equivalent will need to accommodate the characteristics of legacy systems that currently process safety and supporting credential data. If these systems are commercial-off-the-shelf (COTS) products (as opposed to custom state systems), close cooperation with the product vendors is essential to success.

Procurement and subcontract management will be very important components of a successful safety information exchange program.

- It is important for states to establish the habit of monitoring external events as their project proceeds. The CVISN Deployment Workshops are intended to provide a snapshot of the "CVISN world status", but time marches on and things change. The project manager should identify useful Web sites and points of contact to monitor key external factors that may benefit (or harm) the project. Some examples of these are:
  - Status of EDI standards and implementation guides
  - IRP and IFTA Clearinghouse status
  - Status of safety information exchange products, e.g., ASPEN, SAFER, CVIEW, SAFETYNET
  - Development of new technologies such as the eXtensible Markup Language (XML)
  - Progress of safety information exchange efforts in other states
  - Activities of state associations such as CVSA, AAMVA, AASHTO, IFTA, Inc. and IRP, Inc.

## 2. WHAT IS SAFETY INFORMATION EXCHANGE?

Safety Information Exchange is the electronic exchange of safety data, and supporting credential information, regarding carriers, vehicles, and drivers involved in commercial vehicle operations. This information is used by the enforcement community and other related agencies and organizations, e.g., state administrative offices, to make better-informed decisions regarding who to inspect at roadside sites, who to grant credentials and permits to, etc., based on historical safety performance information.

The Safety Information Exchange capability area includes:

- Automated collection of information about safety performance
- Augmentation of safety information with the automated collection of supporting credentials information
- Improved access to carrier, vehicle, and (future) driver safety and credentials information
- Proactive updates of carrier, vehicle, and (future) driver snapshot information
- Support for programs that identify and encourage unsafe operators to improve their performance

Expected benefits from this capability area are:

- Improved safety performance
- Focusing government resources on high risk operators
- Providing carriers with better information to manage their safety programs

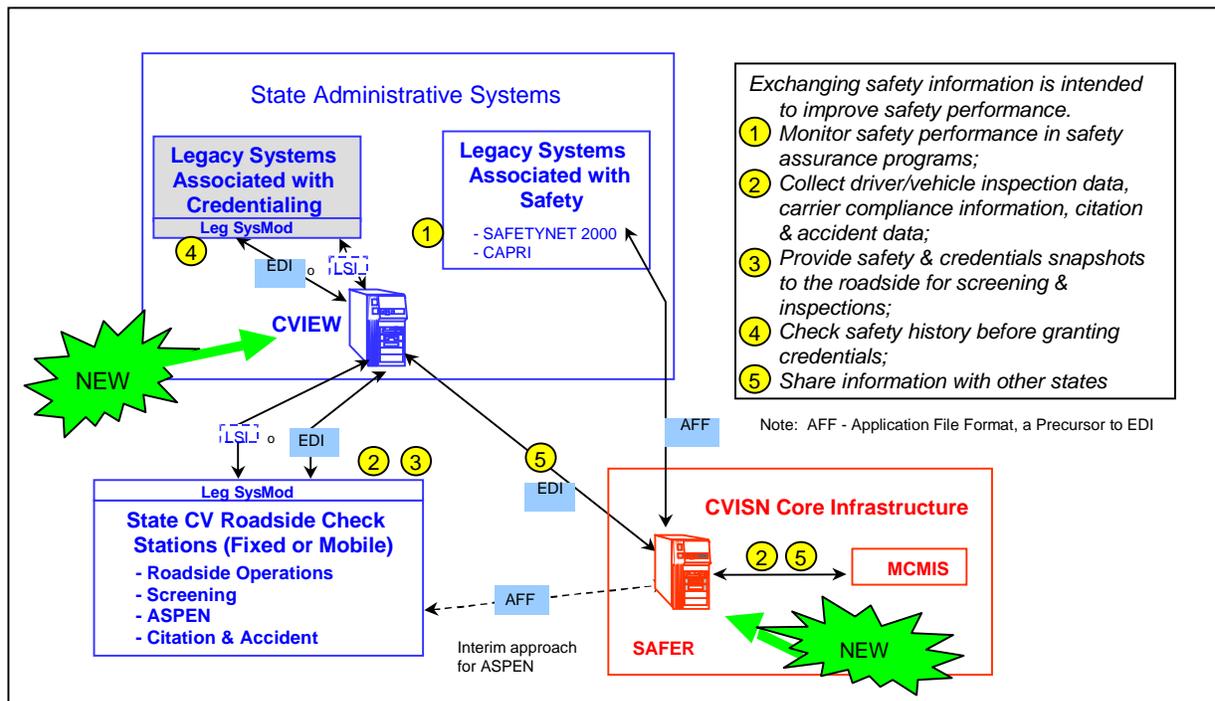


Figure 2-1. Safety Information Exchange

The electronic exchange of safety information and supporting credentials data is used to facilitate the uniform application of safety assurance policies throughout the U.S. Safety assurance is concerned with improving safety in the operation of commercial vehicles. Safety assurance includes collecting information about safety performance, analyzing that information, and implementing regulations, training, and procedures geared towards improving safety. A key element in safety assurance is the exchange of safety information.

Traditional approaches to improving safety have focused on the commercial driver and enforcement of roadway, compliance, and credentialing statutes. There are federal motor carrier statutes intended to assure safe operations. In 1986, the U.S. Department of Transportation adopted the Commercial Motor Vehicle Safety Act. This act defined new national standards for commercial drivers, the equipment and maintenance of vehicles, and the fitness of operating companies. The standards were incorporated in the Code of Federal Regulations, Title 49. The Federal Motor Carrier Safety Administration (FMCSA) is responsible for the issuance, administration, and enforcement of the Federal Motor Carrier Safety Regulations.

As part of their strategic planning in 1997, the FMCSA set a goal to reduce the number of commercial vehicle accidents. To meet that goal, the FMCSA defined several objectives: reducing the risk of crash occurrence, reducing the risk of hazardous materials incidents and environmental damage, enhancing the safety of passenger carriers, and improving the consistency and effectiveness of enforcement and compliance programs. Safety performance is monitored through a program of roadside inspections and carrier compliance reviews.

Federal policy encourages states to enforce the regulations uniformly for both interstate and intrastate drivers and carriers. Federal regulations tend to focus on interstate transportation. Intrastate regulation is largely a state and local responsibility. To assure safe commercial vehicle operations, enforcement and inspection efforts must be consistently applied to both interstate and interstate operators.

### 3. WHAT ALREADY EXISTS?

Key components already exist for carrier, state and CVISN core infrastructure systems. These include state legacy systems that process intrastate safety and supporting credential data, communications systems to exchange information, Internet capabilities, and Web sites and client applications, e.g., ASPEN, to distribute information. In addition, there are commercially available products that support CVISN in terms of data mapping and translation between systems. The following sections provide a summary of products used by carriers, states, and the CVISN core infrastructure, plus a summary of the data interchange standards that are the backbone of the CVISN architecture.

#### 3.1 Products Used By Carriers And Other Third Party Users

With the development of the Internet, carriers have access to electronic information via e-mail and various other communications protocols. With the establishment of the Safety and Fitness Electronic Records (SAFER) Web site, interstate carriers have access to their own safety records that are stored in the Motor Carrier Management Information System (MCMIS) and updated weekly on the SAFER system. The SAFER Web site also provides access to Licensing and Insurance information for those carriers required to obtain insurance and federal operating authority.

#### 3.2 Products Used By States

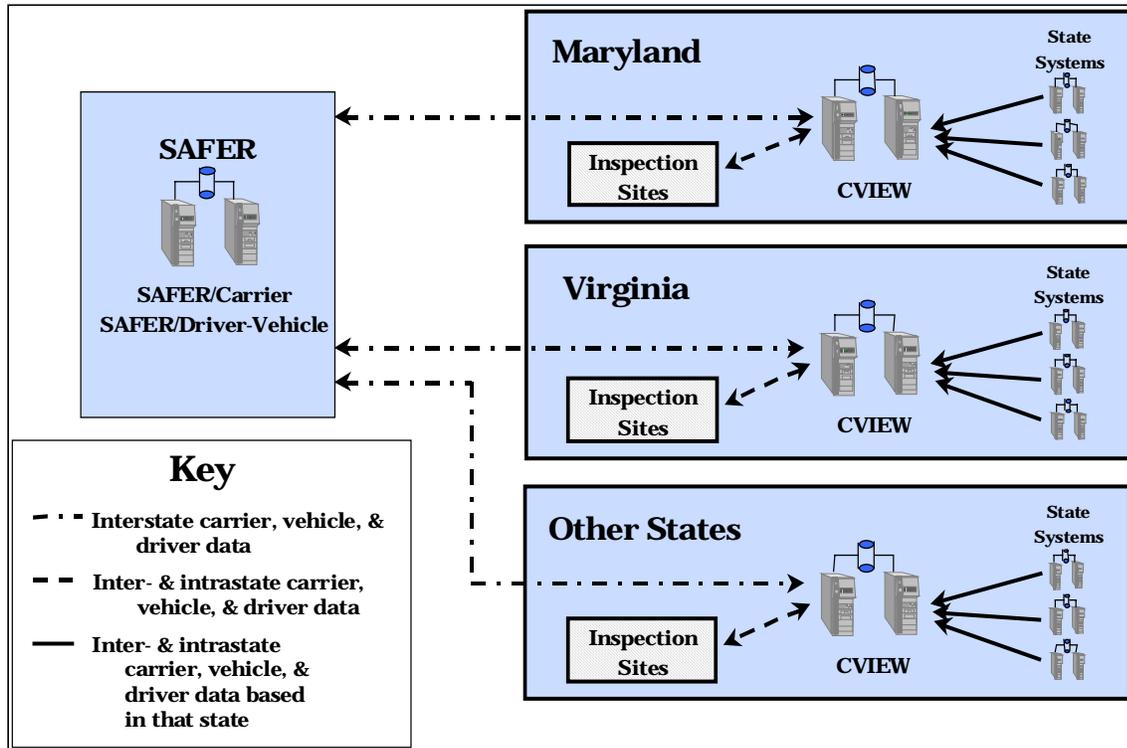
Many states today use a variety of software applications for exchanging safety information electronically. These are divided into state infrastructure systems, which include the Commercial Vehicle Information Exchange Window (CVIEW) and SAFETYNET systems; state roadside systems, which include ASPEN, the Past Inspection Query (PIQ), the Inspection Selection System (ISS) and the Roadside Operations Computer (ROC); and other applications that fall into neither category such as the Carrier Automated Performance Review Information (CAPRI) application. A more detailed description of each application/system is provided below.

##### 3.2.1 State Infrastructure Systems

###### 3.2.1.1 Commercial Vehicle Information Exchange Window (CVIEW)

###### 3.2.1.1.1 Description

CVIEW, or its equivalent, is a state system that collects information from the commercial vehicle (CV) credentialing and tax systems to formulate segments of the interstate carrier, vehicle, and (future) driver snapshots and reports for exchange within the state (e.g., to roadside sites) and with the SAFER system. Each state is responsible for maintaining the credential segments of the snapshots for interstate carriers and for vehicles based within the state. CVIEW is also responsible for assembling and storing complete snapshots for intrastate carriers and vehicles and making that data available to the roadside and other state agencies. The flow of information between SAFER, CVIEW, and a state's legacy systems is depicted in the Figure 3-1.



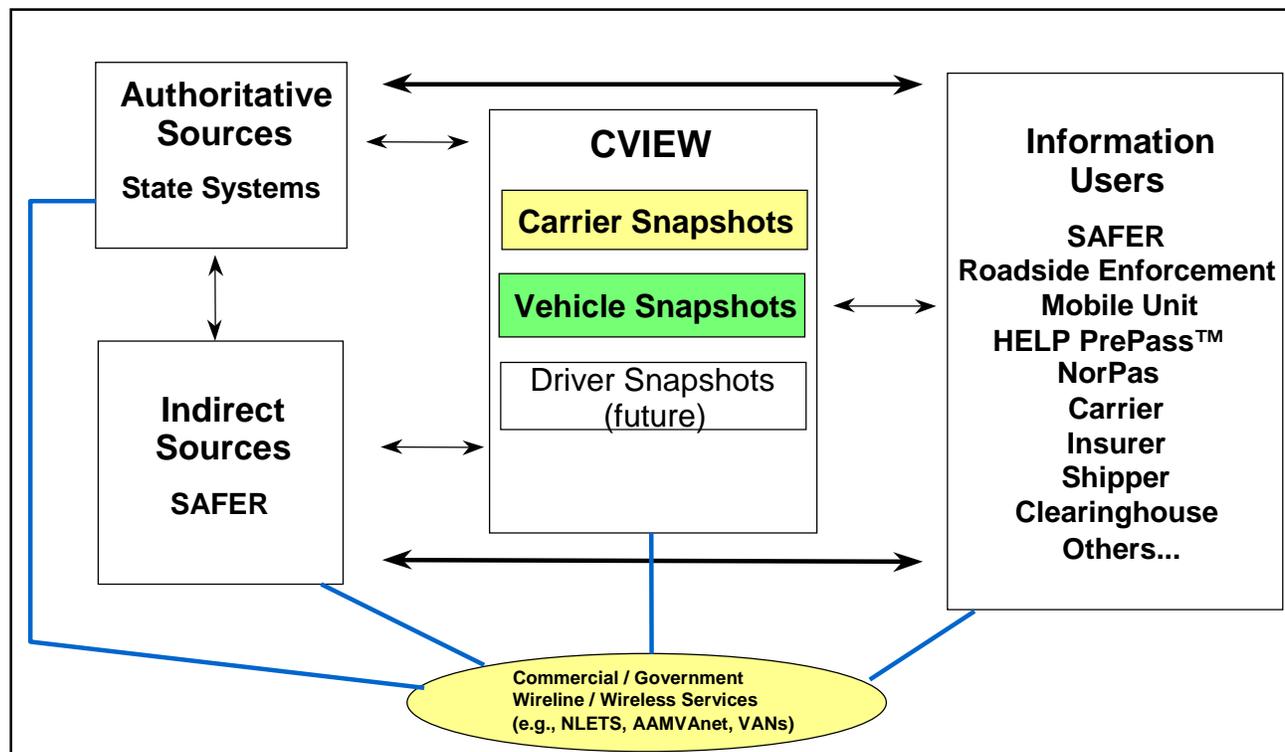
**Figure 3-1. Safety Information Exchange Among SAFER, CVIEW and State Legacy Systems**

In addition to snapshot-related functions, CVIEW, or its equivalent, is expected to serve as the single interface system for ASPEN units in the field. ASPEN will upload and retrieve inspection reports to/from SAFER via CVIEW. CVIEW has similar Data Mailbox facilities as SAFER to facilitate the exchange of information among state users within the state agencies.

In CVISN Level 1, there is a requirement to implement CVIEW or its equivalent for snapshot exchange within the state. CVIEW is a distributed version of the FMCSA-developed SAFER system. It is owned by and located in a state. The functions that CVIEW, or its equivalent, will perform are listed below.

- Provide for the electronic exchange of state-based interstate carrier and vehicle credential data between state source/legacy systems, users, and SAFER
- Provide for the electronic exchange of intrastate carrier and vehicle snapshot data between state source systems and users
- Serve as the repository for a state-selected subset of interstate carrier and vehicle safety and credential data
- Serve as the repository for a state-selected subset of intrastate carrier and vehicle safety and credential data
- Provide inter- and intrastate carrier and vehicle safety and credential data to the roadside to support electronic screening and other roadside operations

The storage of snapshot data in CVIEW and the flow of snapshot information among users and systems via wide-area network communications is depicted in Figure 3-2.



**Figure 3-2. CVIEW Design Overview**

### 3.2.1.1.2 Information Flow

CVIEW does on a State level what SAFER does nationally. It has the potential to consolidate safety, registration, taxation and permit information for intrastate carriers from state “legacy” systems that house these data and make it available electronically to roadside locations. The CVIEW software is essentially a “clone” of the SAFER software except that it runs at the State level and it supports custom interfaces to communicate with each of the state’s legacy systems using legacy system interfaces (LSIs) in cases where EDI data exchange is not available.

CVIEW can send and retrieve safety and credentials data to/from SAFER. It can subscribe to SAFER on behalf of the entire state, receive carrier, driver (future), and vehicle snapshot updates from SAFER on a periodic basis, and forward that data to each user (e.g., each ASPEN system) in the state. To support data exchange functions, CVIEW incorporates a data mailbox system similar to the one used by SAFER, referred to as the CVIEW Data Mailbox (CDM). CVIEW can also (optionally) send interstate registration, taxation and permitting data to SAFER. The flow of information through CVIEW is depicted in the figures below. The bolded or blue highlighted text, if this document is printed in color, denotes the relevant data flows in the figures.

In Figure 3-3, **Flow 1** represents the transmission of registration and fuel tax information from state legacy systems, via legacy system interfaces (LSIs), to the state's CVIEW system. This flow is essential for intrastate data and may be optionally used for interstate data instead of the clearinghouse route. Via the subscription process, CVIEW sends SAFER interstate credential data received from the state (**Flow 2**). CVIEW also receives interstate credentials data (obtained from the Clearinghouses and the Licensing and Insurance system) from SAFER and sends inter- and intrastate credential data to the roadside, **Flows 3 and 4**, respectively.

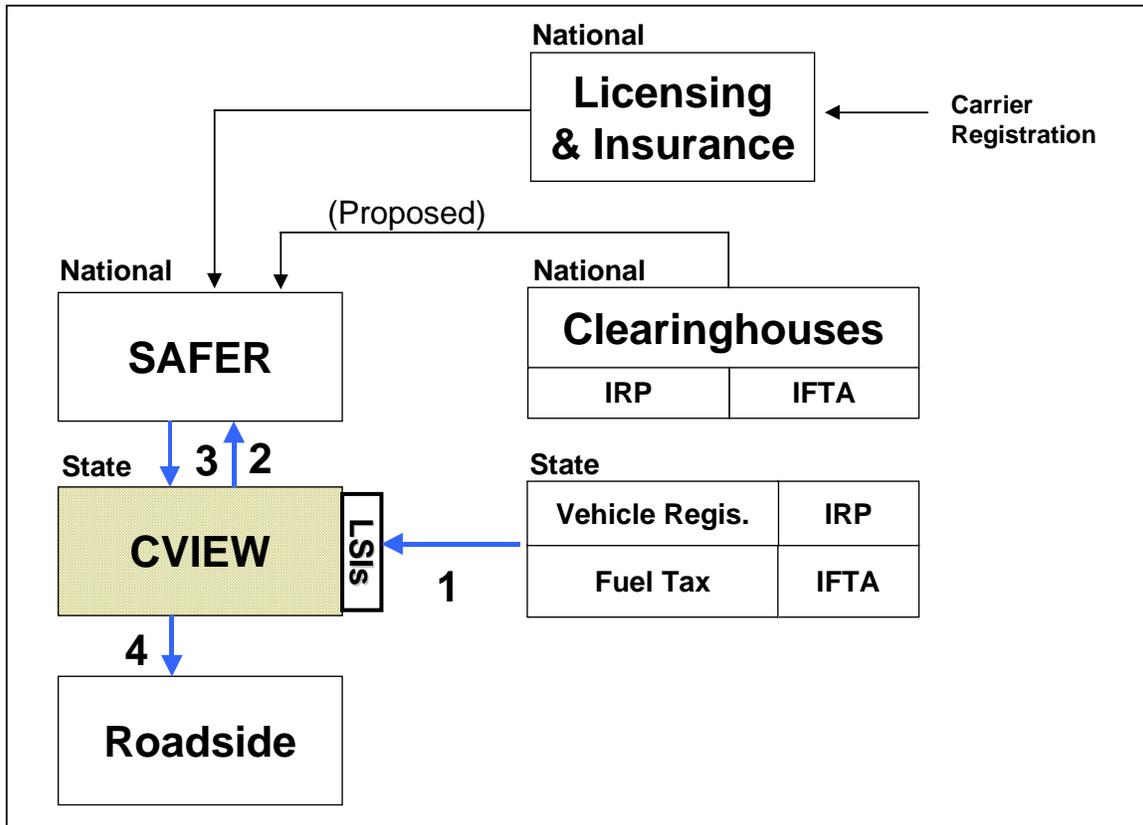


Figure 3-3. CVIEW Credential Information Flow

In Figure 3-4, **Flow 1** represents the transmission of vehicle and/or driver inspection data from the roadside, via the ASPEN client or equivalent, to a state's CVIEW system. CVIEW doesn't store the inspection data but rather passes it through to SAFER (**Flow 2**), where it is stored for a forty-five day period. **Flows 3 and 4** represent the return of one or more inspection reports from SAFER through CVIEW to the roadside in response to a query from a user via the Past Inspection Query application (PIQ). **Note, Flows 1, 2, 3 and 4 are future CVIEW capabilities that will be incorporated in Version 3.0 of the software.** Today, inspection reports are sent to and stored in SAFER (Flow 5) and retrieved from SAFER via PIQ (Flow 6). SAFER sends inspection data to MCMIS and the state's SAFETYNET system via the SAFER Data Mailbox (SDM) in Flows 7 and 8, respectively. Compliance Review data, crash data, enforcement data, and manually generated inspection reports are sent to SAFETYNET from other sources within the state (Flow 9) and transmitted to MCMIS via the SAFER Data Mailbox system (Flows 10 and 11). Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a concise collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis (Flow 12). Via the subscription process, SAFER transmits safety and credential snapshot data to CVIEW, which in turn, is sent by CVIEW to the roadside operations computer (ROC) (**Flows 13 and 14**, respectively). Based on current configurations, SAFER sends weekly updates of safety data to the ISS clients via the subscription process (Flow 15). Although CVIEW is capable of performing this function, no CVIEW systems are currently configured to perform that operation.

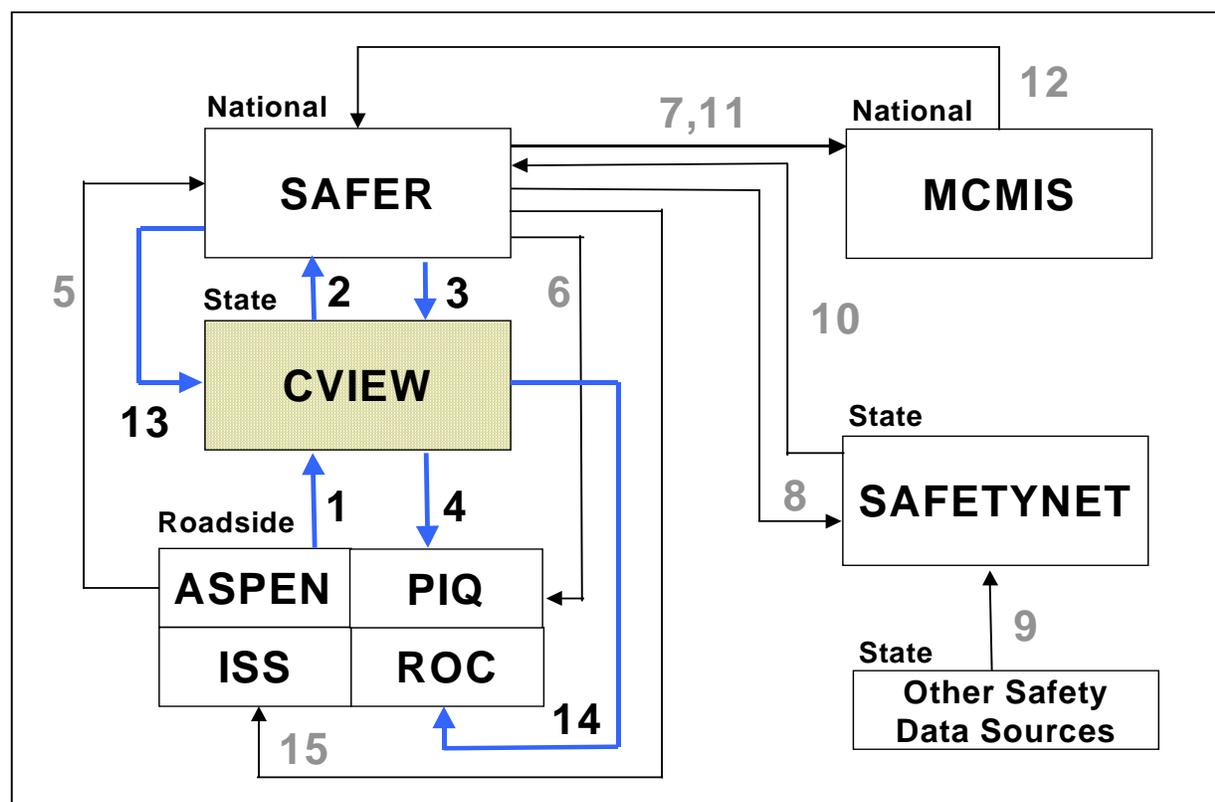


Figure 3-4. CVIEW Safety Information Flow

### 3.2.1.2 SAFETYNET

#### 3.2.1.2.1 Description

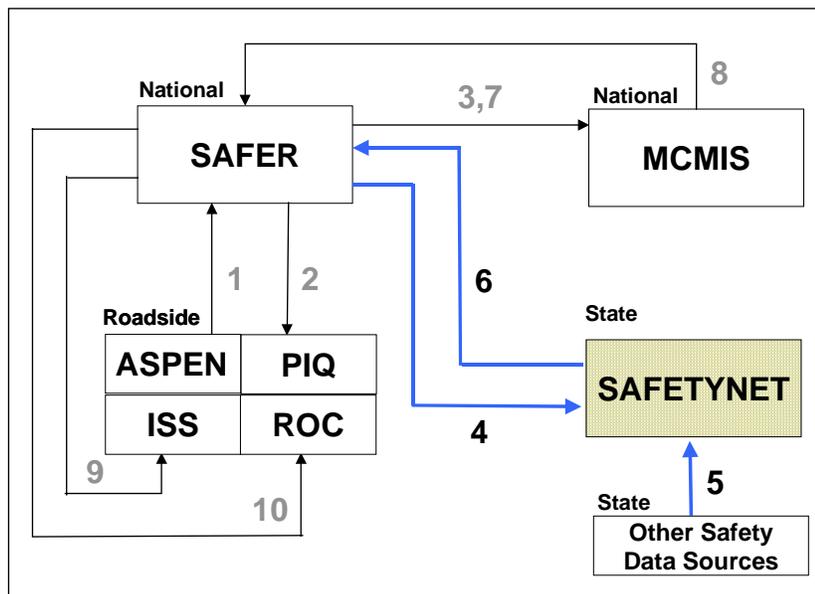
SAFETYNET is a cooperative effort to share motor carrier information among States and the FMCSA. The SAFETYNET system consists of software located in state and federal offices, a communications component, which provides for the electronic transmission of data from these offices to the FMCSA mainframe computer in Washington, D.C., and software which resides on the FMCSA mainframe computer to process the data and load it into the Motor Carrier Management Information System (MCMIS).

The SAFETYNET software is an automated information management system designed to assist motor carrier safety offices in monitoring the safety performance of interstate and intrastate commercial motor carriers. In 1998, the FMCSA released SAFETYNET Version 9.0a, which integrated separate state and federal office functions into a single application. Prior to that, the SAFETYNET system was primarily used by only state offices.

The newest version of SAFETYNET, SAFETYNET 2000, is expected to be released in CY 2000. It is being re-written as a 32-bit Windows-based application that will use the SAFER system, i.e., the SAFER Data Mailbox, to send and retrieve information to/from the Motor Carrier Management Information System (MCMIS).

#### 3.2.1.2.2 Information Flow

The flow of information through SAFETYNET is depicted in Figure 3-5. The bolded or blue highlighted text, if this document is printed in color, denotes the relevant data flows in the figure.



**Figure 3-5. SAFETYNET Safety Information Flow**

In Figure 3-5, Flow 1 represents the transmission of vehicle and/or driver inspection data from the ASPEN client or equivalent, to SAFER via the SAFER Data Mailbox where it is stored for a forty-five day period. Previously stored inspections can be retrieved from SAFER via the Past Inspection Query (PIQ) application, which also interacts with SAFER via the SDM (Flow 2). SAFER sends inspection data to MCMIS and the state's SAFETYNET system via the SAFER Data Mailbox (SDM) in **Flows 3 and 4**, respectively. Compliance Review data, electronically recorded using CAPRI, crash data, enforcement data, and manually generated inspection reports are sent to SAFETYNET from other sources within the state (**Flow 5**) and transmitted to MCMIS via the SAFER Data Mailbox system (**Flows 6 and 7**). Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a concise collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis (Flow 8). Via the subscription process, SAFER transmits safety snapshot data to the ISS (Flow 9). SAFER could send snapshot data to the ROC (Flow 10); however, there are no ROC subscriptions currently defined on the SAFER system.

### 3.2.1.3 State Roadside System

#### 3.2.1.3.1 Description

##### 3.2.1.3.1.1 ASPEN

The FMCSA has developed and is deploying pen- and laptop-based computer software and communications for the conduct of roadside driver/vehicle inspections. This system, called ASPEN, is designed to improve the accuracy of inspection information and the availability of electronic inspection data to users.

Over 2,000 state highway officers in 40 states including the U.S. commonwealth islands use ASPEN. It has been in use since 1995 and has undergone several progressive development phases to stay current with new advances in technology and the increasing sophistication of state and national information systems. ASPEN executes on both portable pen-computers and police cruiser mounted laptops known as Mobile Data Terminals (MDT).

ASPEN facilitates the electronic collection and transmittal of inspection data to state data management systems (SAFETYNET) and from there into the national Motor Carrier Management Information System (MCMIS). This is accomplished through either direct communications with SAFETYNET or via the use of the SAFER Data Mailbox, a component of the SAFER system (see Figure 3-4, to see the relationship between ASPEN and SAFER when a CVIEW system is involved). Inspection data sent to SAFER is stored for a 45 day period during which any stored inspection can be retrieved via the Past Inspection Query (PIQ) application, described below.

Inspection data is used in the process of generating carrier snapshots and carrier profiles. Inspections, along with accident data, provide the basis for carrier safety performance measures, which are computed via the SafeStat algorithm. This safety performance data is fed back to the Inspection Selection System in ASPEN to provide an effective mechanism to ensure greater levels of safety on the nation's highways.

### 3.2.1.3.1.2 *Inspection Selection System (ISS)*

A critical feature of ASPEN is the Inspection Selection System (ISS), an algorithm which helps target problem carriers while helping inspectors avoid performing repetitive inspections of carriers with good safety performance records. The system quickly accesses identification and safety statistics on any of the nation's 450,000 + motor carriers based on the USDOT number found on the side of commercial vehicles. It also provides officers with tips on likely safety problems based on previous inspections of the carrier.

Carrier census and safety data needed by the ISS algorithm is stored locally on the pen or laptop client computer. If the client machine has the ability to communicate with SAFER, it receives weekly updates of that information from SAFER via the SAFER Data Mailbox. This function could also be performed by having the client interact with CVIEW via the CDM.

### 3.2.1.3.1.3 *Past Inspection Query (PIQ)*

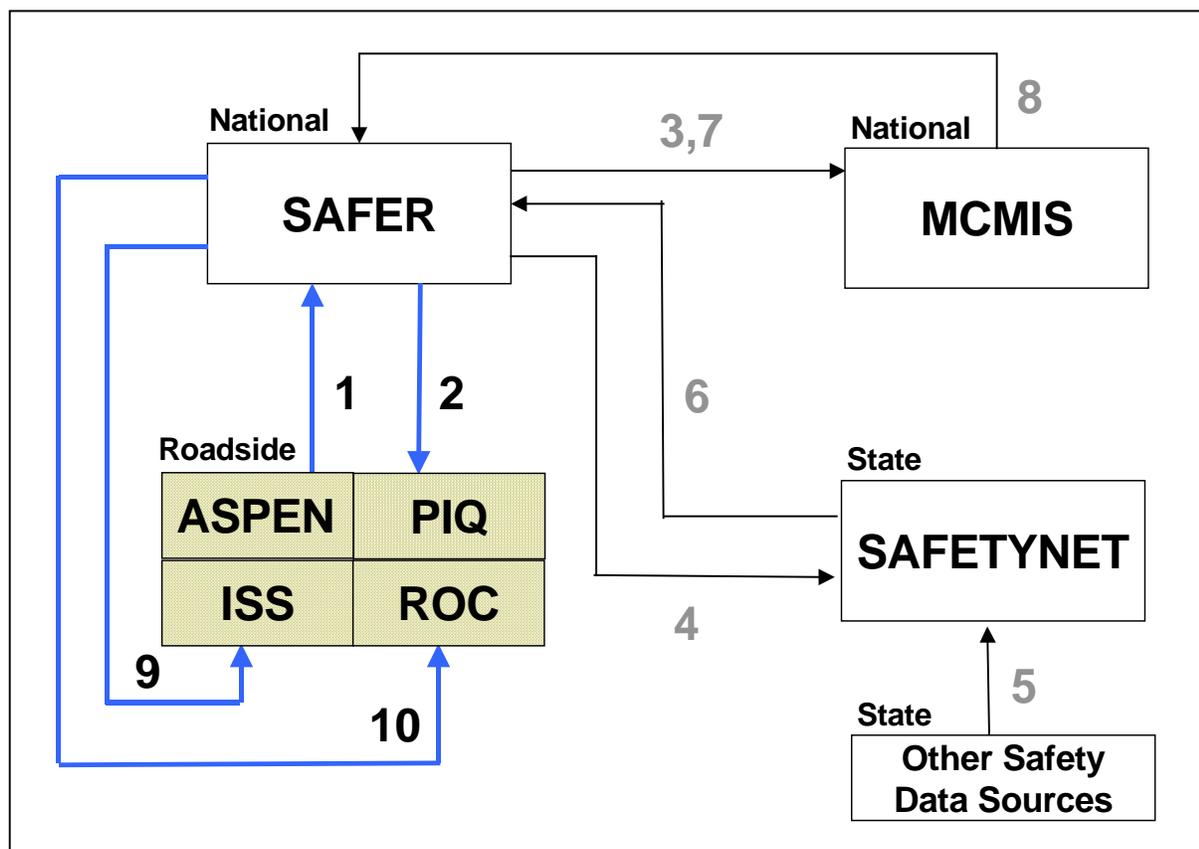
PIQ is an information retrieval application that allows federal and state law enforcement personnel to quickly obtain recent past vehicle safety inspections on any vehicle regardless of where the inspection was performed.

PIQ executes on roadside desktop, laptop, and pen computers. It links to the SAFER system, via the SAFER Data Mailbox, to query and retrieve past inspections based on power unit plate number and state ID. These “past” inspections are saved in SAFER for a 45 day period. Using PIQ, inspection reports can be queried and retrieved at the roadside within seconds of a user’s request (see Figure 3-4, to see the relationship between PIQ and SAFER when a CVIEW system is involved).

### 3.2.1.3.1.4 *Roadside Operations Computer (ROC)*

The Roadside Operations Computer (ROC) is designed to perform the roadside electronic screening functions proposed in *the Commercial Vehicle Information Systems and Networks (CVISN)* architecture. The purpose of the system is to make more efficient use of inspection resources by automatically signaling illegal or high-risk vehicles to pull in for inspection and generally allowing safe and legal vehicles to bypass. Pull-in rates for vehicles are calculated based on screening criteria set at the ROC, using safety and credential snapshot data obtained from either SAFER (see Figure 3-6), CVIEW, or its equivalent (see Figure 3-4).

The flow of information from SAFER through ASPEN, PIQ, ISS, and the ROC is depicted in Figure 3-6 below. The bolded (or blue highlighted text if this document is printed in color) denotes the relevant data flows in the figure.



**Figure 3-6. ASPEN, PIQ, ISS, ROC Safety Information Flow**

In Figure 3-6, **Flow 1** represents the transmission of vehicle and/or driver inspection data from the ASPEN client or equivalent, to SAFER via the SAFER Data Mailbox where it is stored for a forty-five day period. Previously stored inspections can be retrieved from SAFER via the Past Inspection Query (PIQ) application, which also interacts with SAFER via the SDM (**Flow 2**). SAFER sends inspection data to MCMIS and the state's SAFETYNET system via the SAFER Data Mailbox (SDM) in Flows 3 and 4, respectively. Compliance Review data, crash data, enforcement data, and manually generated inspection reports are sent to SAFETYNET from other sources within the state (Flow 5) and transmitted to MCMIS via the SAFER Data Mailbox system (Flows 6 and 7). Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a concise collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis (Flow 8). Via the subscription process, SAFER transmits safety snapshot data to the ISS (**Flow 9**). SAFER could send snapshot data to the ROC (**Flow 10**); however, there are no ROC subscriptions currently defined on the SAFER system.

### 3.2.1.4 Other State Systems

#### 3.2.1.4.1 Carrier Automated Performance Review Information (CAPRI)

The FMCSA has implemented software to conduct Compliance Reviews (CRs) on laptop computers by all Federal and most State investigators. CRs are on-site reviews of carriers and hazardous material shippers that cover compliance with critical parts of the Federal Motor Carrier Safety Regulations.

The software that supports the electronic capture of CR data is called Carrier Automated Performance Review Information (CAPRI). Currently, CAPRI transmits completed CRs to SAFETYNET via floppy disk transfer, or, if in a local area network environment, by storing a completed CR on a designated disk drive that SAFETYNET accesses directly. Future plans include being able to transfer CRs from CAPRI to SAFETYNET via the SAFER Data Mailbox.

## 3.3 CVISN Core Infrastructure Systems

### 3.3.1 Motor Carrier Management Information System

#### 3.3.1.1 Description

The Motor Carrier Management Information System (MCMIS) is the national system that consolidates and processes motor carrier safety data from sources throughout the U.S. It operates on a mainframe computer at the Transportation Computer Center at DOT Headquarters in Washington, D.C. The system contains safety records in excess of 450,000 active interstate motor carriers, over 150,000 safety and compliance reviews, and supports the addition of approximately 2 million roadside inspection records and 100,000 crash records annually.

All interstate motor carriers (private and for hire) are required to identify themselves to the FMCSA using the MCS-150 form. It provides basic carrier identification information and data on the type and size of their operations. After the registration process is completed, a USDOT number is issued to the carrier, which the carrier must post on all of its vehicles.

MCMIS provides many types of consolidated data and reports back to State and Federal SAFETYNET systems, mostly by electronic means. Carrier profiles and prioritizations based on algorithms that consider all of a carrier's safety data are principal examples. Carriers, for which Compliance Reviews have been conducted, are also given a Safety Fitness Rating. Much of this information is available to industry and the public via written request, a toll-free phone number, or the Internet.

MCMIS, via the SAFER system, supplies carrier ID and historical safety data for each interstate carrier to the ASPEN ISS (Inspection Selection System) which is an algorithm to prioritize vehicles for inspection at the roadside. SAFER obtains that information from MCMIS on a weekly basis. The weekly update to SAFER contains all records on MCMIS that have had census and/or safety changes during the previous week. It includes, for each interstate carrier, ID information such as USDOT and ICC number, name and address, and summarized safety data from past inspections, compliance reviews, crashes, and enforcement activities.

The flow of information through MCMIS is depicted in the figure below. The bolded or blue highlighted text, if this document is printed in color, denotes the relevant data flows in the figure.

### 3.3.1.2 MCMIS Safety Information Flow

In Figure 3-7, Flow 1 represents the transmission of vehicle and/or driver inspection data from the ASPEN client or equivalent, to SAFER via the SAFER Data Mailbox where it is stored for a forty-five day period. Previously stored inspections can be retrieved from SAFER via the Past Inspection Query (PIQ) application, which also interacts with SAFER via the SDM (Flow 2). SAFER sends inspection data to MCMIS and the state's SAFETYNET system via the SAFER Data Mailbox (SDM) in **Flows 3** and 4, respectively. Compliance Review data, crash data, enforcement data, and manually generated inspection reports are sent to SAFETYNET from other sources within the state (Flow 5) and transmitted to MCMIS via the SAFER Data Mailbox system (**Flows 6** and **7**). Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a concise collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis (**Flow 8**). Via the subscription process, SAFER transmits safety snapshot data to the ISS (Flow 9). SAFER could send snapshot data to the ROC (Flow 10); however, there are no ROC subscriptions currently defined on the SAFER system.

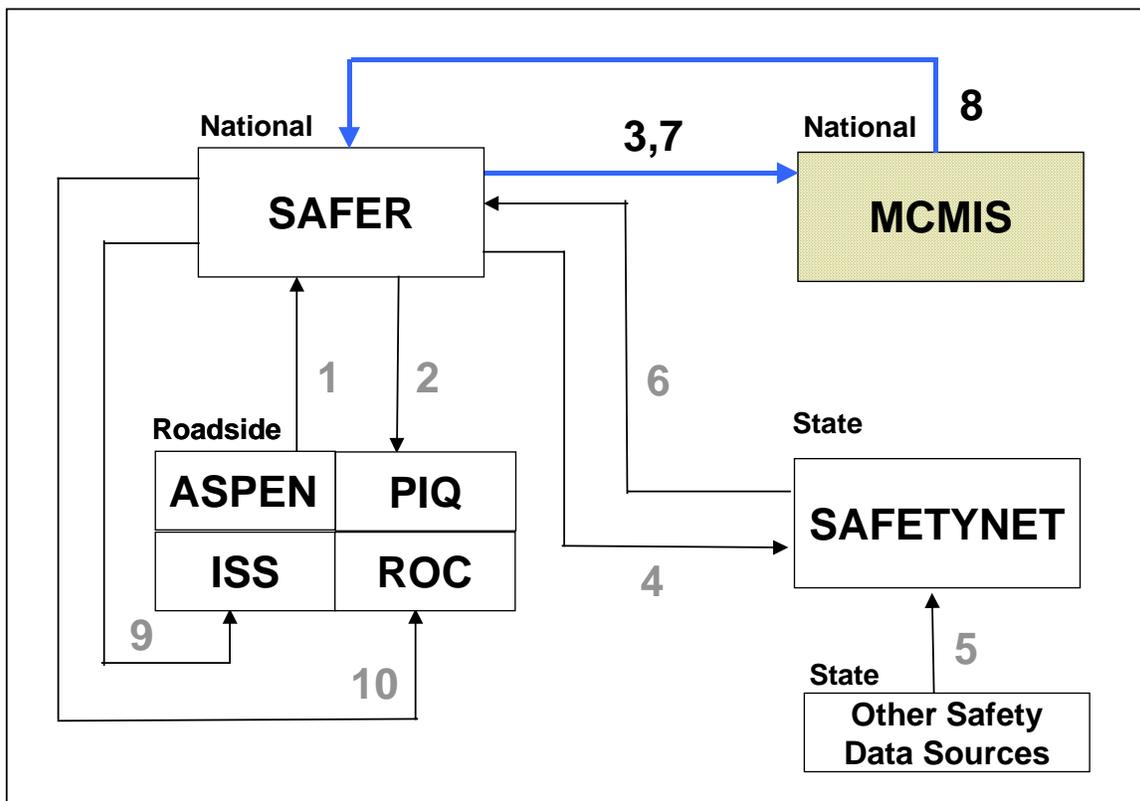


Figure 3-7. MCMIS Safety Information Flow

## **Planned Next Steps**

The MCMIS application is currently being re-designed based on a client-server paradigm and a relational data model. The most significant impact of this re-design effort on users will be the shift towards the use of web-based communications as opposed to the mainframe-based methods used today. Also, it is expected that the new system will be capable of processing both inter- and intrastate carrier safety information, which is currently limited to only interstate data. More information on this development effort will be available as the design progresses.

### **3.3.2 Safety and Fitness Electronic Records System**

#### *3.3.2.1 Description*

SAFER is a federal system that provides standardized carrier, vehicle, and driver (future) datasets (snapshots and reports) containing safety and credentials information to authorized users within a few seconds of a user's request. The SAFER Data Mailbox component facilitates the exchange of information between roadside sites and administrative centers by acting as a temporary repository for data files and messages.

The primary function of SAFER is to provide users timely, electronic access to safety and credential data via one or more wide area network (WAN) communication links (see figure below). This information includes identity data about carriers, vehicles, and drivers, summaries of past safety performance histories (inspections, accidents, and other data) and supporting credential information needed to support electronic screening activities at the roadside, e.g., electronic cab card data, and summary IRP and IFTA data.

SAFER provides users with either a summary safety record (“snapshot”), or a more detailed report. Two such reports are the carrier profile and vehicle/driver inspection reports. SAFER supports on-line query and response for snapshot and report information.

One of SAFER’s primary objectives is to increase the efficiency and effectiveness of the inspection process at the roadside. The SAFER system currently provides carrier, vehicle, and driver safety and credentials information to fixed and mobile roadside inspection stations. This allows roadside inspectors to focus their efforts on high-risk areas; i.e., selecting vehicles and/or drivers for inspection based on the number of prior carrier inspections and its safety and credential history.

SAFER allows users to request, via subscriptions, that specific snapshots are sent to them automatically when substantial change in the data occurs. Users can also specify the types of change that triggers transmission of subscription requests. To utilize these system functions, users will require, at a minimum, a computer system, a user account, and the ability to connect to one of the several WANs supported by SAFER.

An overview of the SAFER design is shown in Figure 3-8. The flow of information through SAFER is depicted in Figures 3-9 and 3-10, below. The bolded (or blue highlighted text if this document is printed in color) denotes the relevant data flows in the figures.

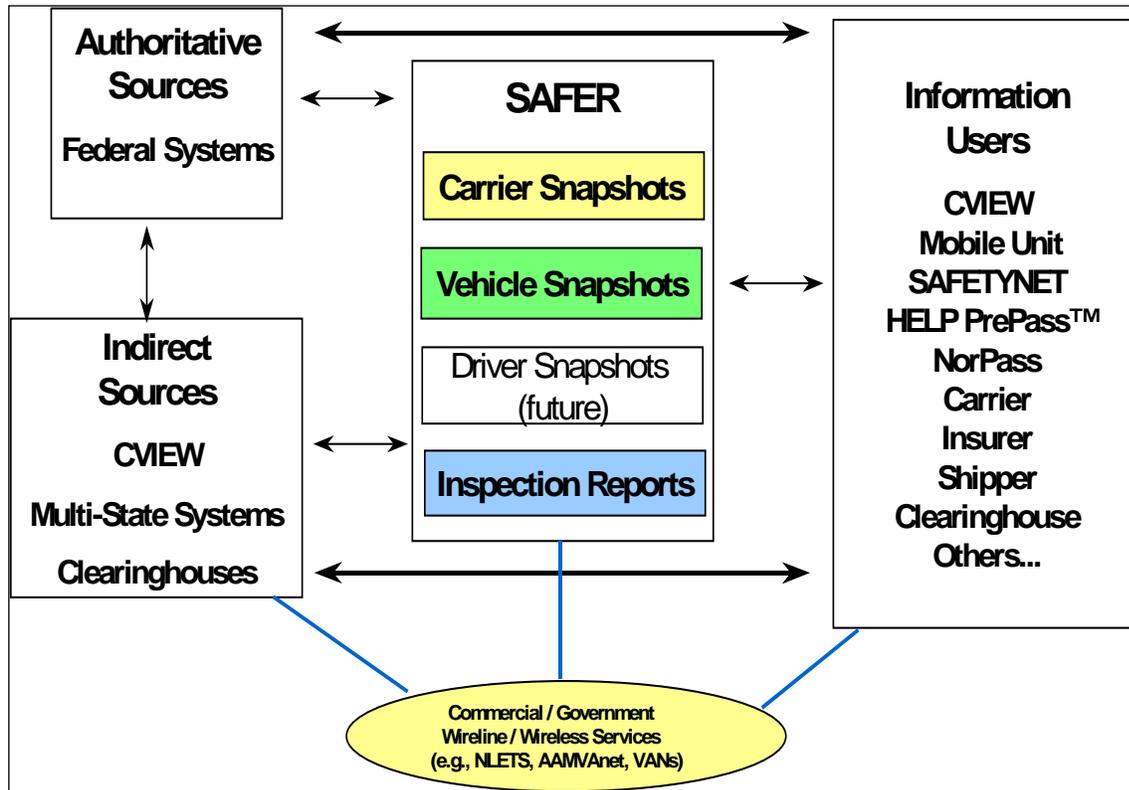


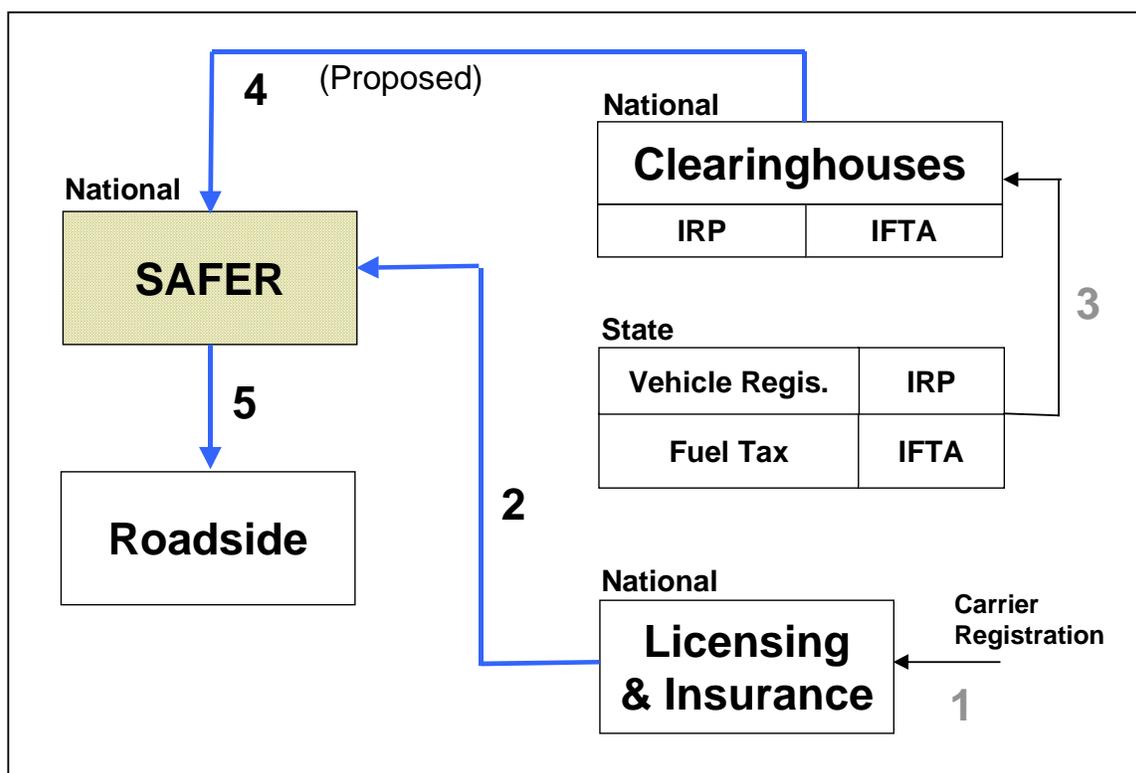
Figure 3-8. SAFER Design Overview

### 3.3.2.2 Information Flow

#### 3.3.2.2.1 SAFER Credential Information Flow

All States support systems for the administration of the International Registration Plan (IRP) for commercial vehicles and the International Fuel Tax Agreement (IFTA) for interstate operations. IRP and IFTA Clearinghouses, national information systems designed to assemble in one database certain information about the registration and fuel taxation of interstate carriers and vehicles, respectively, have been developed.

The carrier licensing (“authority”) and insurance certification required by the former Interstate Commerce Commission (ICC) remain in effect for most for-hire carriers (about 85,000 carriers). In Figure 3-9, the Licensing and Insurance (L & I) system registers these carriers (Flow 1), tracks their insurance, and sends a summary of that information to SAFER for display on the SAFER Web and for incorporation into carrier snapshots (Flow 2).



**Figure 3-9. SAFER Credentials Information Flow**

In Flow 3, State IRP/IFTA systems send certain data to the national clearinghouses. It is not decided yet if this will be just demographic data or will include tax status information. It is envisioned that national clearinghouses will send updates of vehicle registration and fuel taxation data to SAFER for distribution (**Flow 4**).

SAFER includes IRP, IFTA and insurance (for hire) credential data in the snapshot for interstate carriers and vehicles and “pushes” this information to ASPEN and other roadside users (**Flow 5**). Figure 3-3, illustrates the relationship between credentials data exchange and SAFER when a CVIEW system is involved.

The delivery of **interstate** safety, registration and taxation information to the roadside may be handled by interstate clearinghouses such as MCMIS, IRP, and IFTA and distributed via SAFER. However, states will be participating to varying levels in the IRP and IFTA Clearinghouses for interstate data. Additionally, some method is needed to deliver similar **intrastate** data to roadside locations within a State. These data are not processed in the clearinghouses and are not uniform from State to State. In most cases, there is no roadside access to intrastate vehicle registration, fuel taxation and permit data within a State. An underlying problem is there was no uniform way of identifying intrastate carriers, as there was

with the USDOT registration for interstate carriers. Some States have intrastate carrier registration and carrier numbers, however, many do not.

The solution recommended for CVISN Level 1 is that states implement CVIEW or an equivalent system to handle information exchange about intrastate carriers and vehicles. CVIEW can also be used to provide credentials to SAFER for interstate carriers and vehicles based in that state.

### 3.3.2.2.2 SAFER Safety Information Flow

In Figure 3-10, **Flow 1** represents the transmission of vehicle and/or driver inspection data from the ASPEN client or equivalent, to SAFER via the SAFER Data Mailbox where it is stored for a forty-five day period. Previously stored inspections can be retrieved from SAFER via the Past Inspection Query (PIQ) application, which also interacts with SAFER via the SDM (**Flow 2**). SAFER sends inspection data to MCMIS and the state's SAFETYNET system via the SAFER Data Mailbox (SDM) in **Flows 3 and 4**, respectively. Compliance Review data, crash data, enforcement data, and manually generated inspection reports are sent to SAFETYNET from other sources within the state (Flow 5) and transmitted to MCMIS via the SAFER Data Mailbox system (**Flows 6 and 7**). Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a concise collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis (**Flow 8**). Via the subscription process, SAFER transmits safety snapshot data to the ISS (**Flow 9**). SAFER could send snapshot data to the ROC (**Flow 10**); however, there are no ROC subscriptions currently defined on the SAFER system.

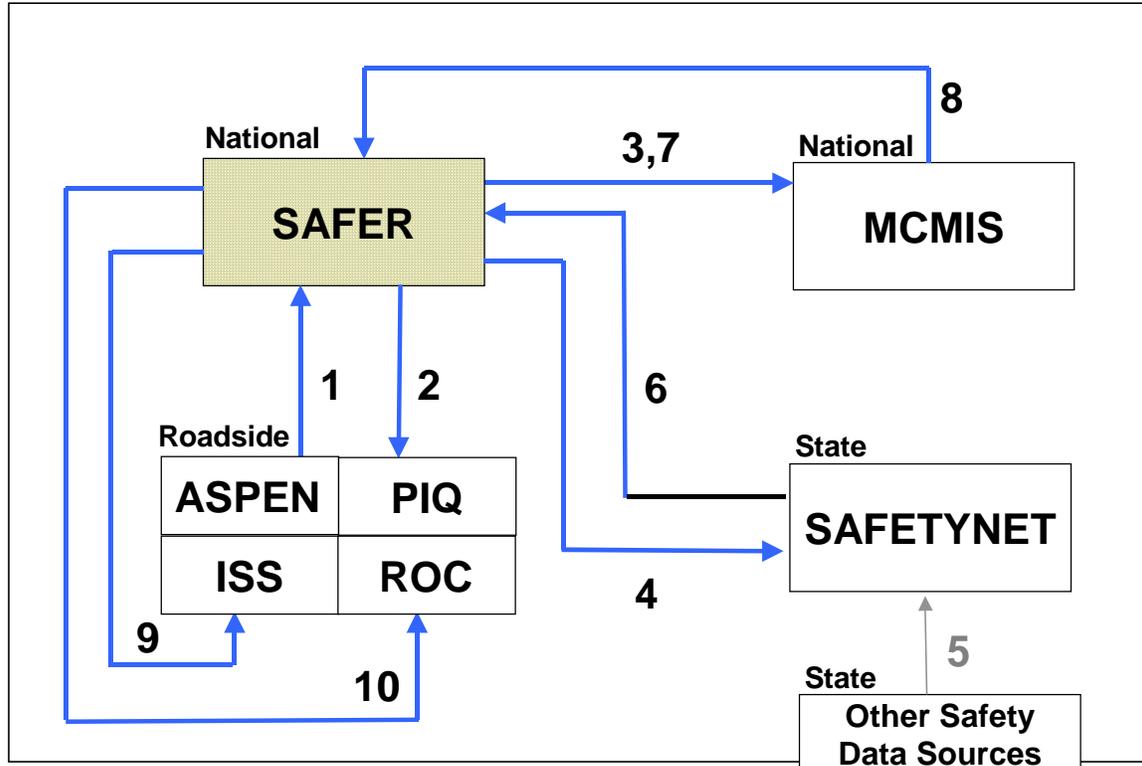


Figure 3-10. SAFER Safety Information Flow

### 3.3.3 Commercial Driver License Information System

#### 3.3.3.1 Description

The Commercial Driver's License Information System (CDLIS) was developed to support the commercial driver's licensing process performed by the states. CDLIS is a transaction routing (or "pointer") system that permits states to share CDL information. CDLIS has been operational since 1992.

The flow of information through CDLIS is depicted in the Figure 3-11. The bolded or blue highlighted text, if this document is printed in color, denotes the relevant data flows in the figure.

#### 3.3.3.2 CDLIS Credential Information Flow

In Figure 3-11, **Flow 1** represents both a query and its response to/from ASPEN via direct dial-up communications to TML, an authorized, independent communications company with access rights to CDLIS, to obtain either summary or detailed information regarding a commercial driver's license from the CDLIS system. TML uses the CDLIS Pointer system (**Flow 2**) to determine which state Department of Motor Vehicles (DMV) contains the requested information. The query is forwarded to the appropriate state's DMV. It returns the requested information to ASPEN via the TML link (**Flows 3, 2 and 1** respectively).

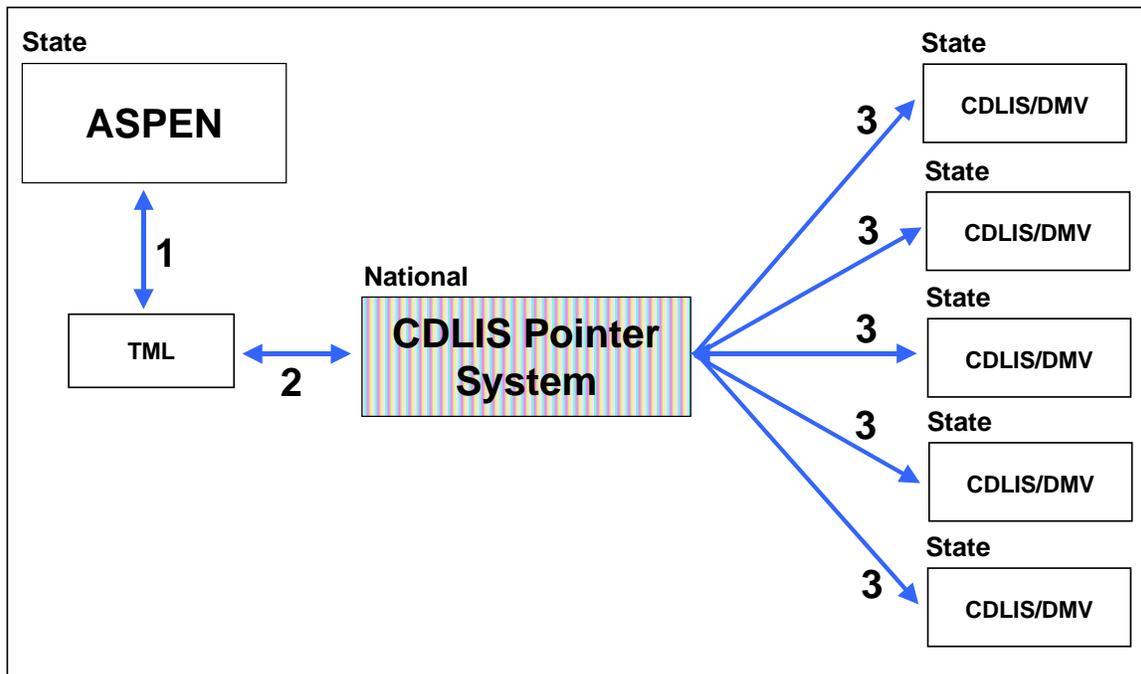


Figure 3-11. CDLIS Credential Information Flow

In the future, users connecting directly to SAFER will be able to establish a web-based link to CDLIS via a TML Web server. For example, an ASPEN user, having connected wirelessly to SAFER via a Bell Atlantic CDPD method, would be able to query CDLIS via an onboard web browser over the existing CDPD link to SAFER. Linkage from SAFER to TML will be accomplished via the FTS2000 WAN. SAFER will handle the routing from one network to another on behalf of the user, e.g., Bell Atlantic to FTS2000. Note, this network routing approach still needs to be prototyped and tested.

### 3.4 Data Interchange Standards

Use of ANSI ASC X12 EDI transaction sets is part of the CVISN architecture. The SAFER and CVIEW systems use transaction set (TS) 285 for processing safety and supporting credential data. TS 997 and TS 824 are used to acknowledge that a transaction is received. TS 284 will support the exchange of various types of safety reports, e.g., inspection reports. The following transaction sets support safety data exchange:

TS 285	CV Safety & Credentials Information Exchange (snapshots)
TS 284	Commercial Vehicle Safety Reports
TS 824	Application Advice
TS 997	Functional Acknowledgement

Commercial products are available that map standard data formats to and from the format required by the standard, if necessary.

Implementation Guides (see the CVISN Web Site at <http://www.jhuapl.edu/cvisn>) are available for the transaction sets currently used in CVISN.

This Page Intentionally Blank

## 4. OPERATIONAL CONCEPTS AND SCENARIOS

The term “operational concept” generally means “how a system is used in various operational scenarios”. “System” is used here in a broad sense to include people and manual processes as well as automated information, sensor and control systems. New operational concepts are adopted in order to solve a problem in the current operations or to take advantage of new knowledge or technology that enables improvements in current operations.

The operational concepts are related to the guiding principles developed by the stakeholder community. The concepts were derived by first analyzing the user services that discuss how to improve commercial vehicle operations, then interpreting the stakeholder-developed guiding principles, and finally applying knowledge about the state of existing and emerging technologies. The combination of the desired commercial vehicle operations improvements, guiding principles about making those improvements, and the reality of technological advances are reflected in the operational concepts.

CVISN objectives for safety information exchange are listed below:

- Collect, store, and provide access to safety information
- Pro-actively identify unsafe operators
- Improve safety assurance program efficiency & effectiveness
- Provide safety compliance statistics to support policy decisions, rule making, and program development
- Implement programs to encourage unsafe operators to improve their performance or to remove them from the highways

Key to the safety information the exchange concepts are “snapshots” – a collection of carrier, vehicle, and (future) driver information assembled from authoritative or indirect sources. Snapshots reflect the state of those data when the information was provided to the systems that manage snapshots, the national Safety and Fitness Electronic Records (SAFER) system and the state Commercial Vehicle Information Exchange Window (CVIEW) systems. SAFER and CVIEW assemble snapshots for inter- and intrastate carriers and vehicles, respectively. Driver snapshots are not presently available. Snapshot data *are stored* in SAFER and CVIEW. Generally, the assembly and transmission are accomplished using ANSI EDI ASC X12 transaction set (TS) 285.

## 4.1 Key Operational Concepts

The *CVISN Operational and Architectural Compatibility Handbook (COACH) Part 1, Operational Concept and Top-Level Design Checklists* (Reference 2), provides a comprehensive checklist of key operational concepts relating to Safety Information Exchange. The operational concepts should be used to guide the state design process. The safety information exchange operational concepts stated in the COACH Part 1 are repeated and further explained here.

- Data are collected to quantify the primary measures of effectiveness related to safety of CVO (accidents and fatalities). Accidents (rates and/or numbers) and fatalities have been identified as the primary measures of effectiveness of the safety improvement initiatives. The safety information exchange processes collect data to measure these parameters and assess changes.

- Electronic carrier and vehicle safety records (snapshots) are made available to the roadside via SAFER and CVIEW to aid inspectors and other enforcement personnel. The carrier snapshots provide details on the components of the carrier safety risk rating and credentials information. Vehicle snapshots contain information on vehicle safety records and credentials. (Driver snapshots that could provide details on driver safety performance and credentials have not been endorsed by the CVO community and are not planned for near-term implementation.) Vehicle snapshots contain information equivalent to an electronic Commercial Vehicle Safety Alliance decal and electronic Out-Of-Service status. From the vehicle itself, one or more identifiers will be provided. This basic information will allow roadside systems to link the vehicle to the snapshot and other infrastructure-provided data. For more information about snapshots, please see Reference 11.

### Key ITS/CVO Operational Concepts for Safety Information Exchange

- Measures of effectiveness: accidents and fatalities
- Electronic safety records at roadside
- Automated collection of inspection results
- National electronic access to interstate safety information
- Controlled access to data
- Able to correct errors
- Determining safety risk ratings
- Standard inspection selection criteria
- Comprehensive safety policy (deskside and roadside) implemented to improve safety
- Base state for each carrier (safety record and credentials)
- Compliance reviews and electronic access to participating carrier's records

- Inspectors use computer applications to capture, verify, and submit intrastate and interstate inspection data at the point of inspection. Automated support for collecting and reporting inspection data increases the consistency in inspection reporting, removes the need to forward a paper copy for subsequent data entry, and reduces inspection time. This may include collecting information from on-board safety monitoring systems, as well as using

advanced technology such as automated brake testing equipment to support the inspection process.

- Safety data are made available electronically to qualified stakeholders. Providing safety data electronically to shippers, insurance companies, vehicle leasing companies, and the general public allows them to use timely information in making their business decisions. Providing the information to carriers helps them analyze and improve their own safety performance.
- User access to data is controlled (restricted and/or monitored) where necessary. Information sharing within a single jurisdiction and across jurisdictions using electronic networks is a cornerstone of the Intelligent Transportation Systems (ITS)/CVO initiative. Information systems are only as good as the quality of the data they use. Data must be accurate, current, and safe from tampering or unauthorized disclosure. Authoritative sources are the official repositories for the data. Some information will be sensitive and not all stakeholders will be granted access to sensitive data. The systems must include techniques for controlling access to information so that inappropriate disclosure does not take place.
- Mechanisms are made available for operators to dispute safety records held by government systems. If errors exist in government-held records pertaining to safety, standard procedures must be available to note and correct the error.
- Safety risk ratings are determined according to uniform guidelines. As part of the ongoing Performance and Registration Information Systems Management (PRISM) project, the Motor Carrier Safety Status (SafeStat) algorithm was developed as a safety status indicator in the Motor Carrier Safety Improvement Program (MCSIP). (Reference 12)
- Jurisdictions support a standard set of criteria for inspection selection. The ASPEN inspection support system includes an algorithm called the Inspection Selection System (ISS). This algorithm uses carrier safety performance and inspection history data to rank carriers according to the relative value of conducting a vehicle inspection. The objective is to increase inspections for carriers with poor safety performance records (accidents, out-of-service defects and other safety problems) and for those for which little or no safety information is available. (Reference 34).
- A comprehensive safety policy, including roadside and deskside activities, is implemented to improve safety. In the long term, supporting automation of part or all of a vehicle inspection (e.g., electronic connection to brake testing systems) or driver inspection (e.g., alertness testing) improves inspection accuracy, reduces inspection time and improves the inspector's work environment. Electronic access from the roadside to on-board vehicle and driver safety monitoring systems shifts the focus of the inspection from assessing the condition of the vehicle or driver to verifying the on-board systems are functioning properly.

- Carriers are associated with a base state for safety information record storage and credentialing. The base state processes credential applications for the carrier, using safety information to judge whether or not to grant the credential. The base state makes safety data available to other jurisdictions via snapshots and reports exchanged via SAFER.
- Compliance reviews are supported through electronic access to carrier-held records. Electronic access to carrier records and automated support for collecting and reporting compliance review data increases consistency, removes the need for handling paper, and speeds the auditing process.

## 4.2 Operational Scenarios

The expected benefits resulting from applying the safety information exchange concepts are improved safety assurance program efficiency and effectiveness through increased focus on at-risk operators.

A state must develop or otherwise acquire new systems and modify some existing systems to implement the CVISN Level 1 capabilities. There are many ways to do this and still be in conformance with the architecture and standards.

Regardless of the design approach chosen, all states need to model their intended business processes in a way that is easy for all stakeholders to review and understand. The functional thread diagram is the tool recommended to illustrate operational scenarios.

This section depicts an example functional thread diagram. The scenario chosen is one of the CVISN Level 1 capabilities. **The high-level CVISN Level 1 operational scenarios related to Safety Information Exchange functions are listed below:**

- Record inspections electronically and report them to SAFER and MCMIS
- Query for a past inspection report
- Maintain carrier and vehicle snapshots for intrastate operators
- Query for a snapshot

The operational scenarios related to filling snapshots with credential data are included in the CVISN Guide to Credentials Administration, Reference 9.

The example operational scenario illustrates the first operational scenario in the list: Record inspections electronically and report them to SAFER and MCMIS. The method used to demonstrate the scenario is called a “functional thread diagram.” The activities in the scenario are listed as steps. To differentiate between different time schedules, numbers are used to show the conduct and reporting of the inspection. Letters are used to show the manual review of the inspection, and the subsequent submission to MCMIS.

A diagram corresponding to the steps listed is presented in Figure 4-1 for a graphical view of the scenario. The lines represent data flow between products, with arrows indicating the direction of flow. Each line is labeled with a number or letter. The complete set of lines constitutes a thread

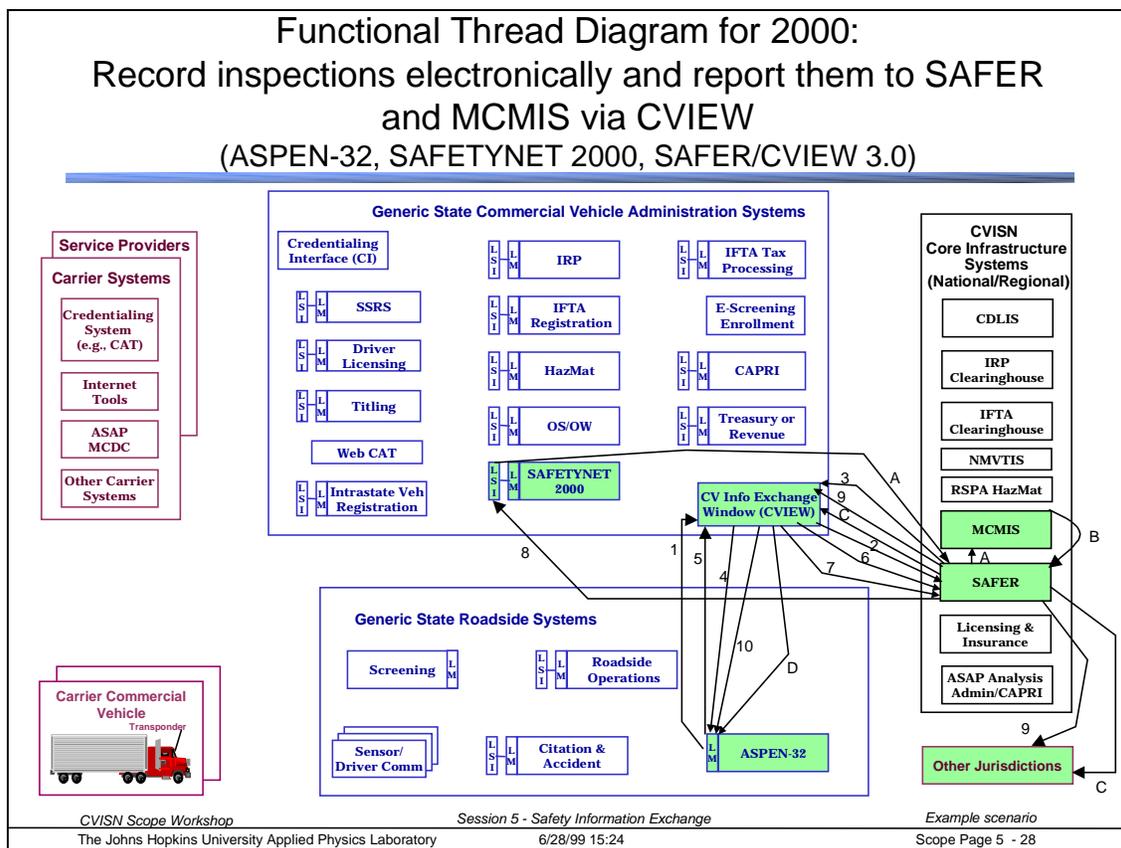
of activities that accomplish a function. Hence, the diagram is called a “functional thread diagram.”

The scenario included in this chapter reflects the steps that states will follow once the year 2000 versions of SAFER, ASPEN, and SAFETYNET are implemented. In this example, the state has a CVIEW that serves as the within-state interface to SAFER and ASPEN.

#### **4.2.1 Example Operational Scenario: Record Inspections Electronically and Report Them to SAFER and MCMIS in 2000 (ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)**

1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to CVIEW’s input mailbox in the CVIEW Data Mailbox (CDM), for all inspection reports relating to a particular carrier. The PIQ receives inspection reports in Application File Format (AFF), a precursor to EDI translation.
2. CVIEW passes the query to SAFER, via a Remote Procedure Call (RPC).  
Note: All queries are passed to SAFER where Interstate and Intrastate Inspection Reports are stored for 45-day period.
3. SAFER receives the query, processes the request, and then retrieves the inspection report from data storage. SAFER sends all inspection reports matching the query to CVIEW, via RPC.
4. CVIEW passes the inspection reports to the ASPEN client via its query mailbox in the CDM, in AFF format. The PIQ detects and processes the report for display on the ASPEN client. The past inspections show that this carrier’s vehicles often have brake problems.
5. The enforcement officer conducts the inspection and finds that the brakes are not functioning properly. He completes the inspection and places the vehicle Out-Of-Service (OOS). ASPEN sends the inspection report to CVIEW’s input mailbox in the CDM, in AFF.
6. CVIEW passes the inspection report to SAFER, via RPC.
7. CVIEW sends the inspection report to SAFETYNET 2000’s input mailbox in the SDM in AFF.
8. SAFETYNET retrieves the inspection report from its SDM mailbox.
9. SAFER updates the vehicle snapshot segment with inspection information, e.g., OOS status, Inspection history. SAFER forwards snapshots to subscribers, including CVIEW systems, via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
10. CVIEW forwards vehicle snapshots to ASPEN clients via their subscription mailboxes in the CDM in AFF. The vehicle snapshots contain OOS information based on the previously submitted inspection reports.

- A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the SDM.
- B. MCMIS receives the inspection report and updates carrier summary information and computes carrier safety statistics, e.g., carrier safety ratings and history, inspection summaries. Weekly, MCMIS sends SAFER updated carrier snapshot segments via flat file.
- C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshots to subscribers, including CVIEW systems, via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
- D. CVIEW forwards carrier snapshots to ASPEN clients to support the ISS via their subscription mailboxes in the CDM in AFF.



**Figure 4-1. Functional Thread Diagram: Record Inspections**

NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. The results of processing an incoming TS 285 are reported via TS 824.

Additional examples of operational scenarios and functional thread diagrams are in Appendix C. They are included for reference, and as starting points for states that plan to implement similar processes.

A list of scenarios geared to interoperability testing CVISN Level 1 capabilities is shown in Table 4-1. The list shows details such as different kinds of snapshot queries. Error handling scenarios are not included in the table, but must be addressed as part of the design process. A state may need to add scenarios to address additional functions.

**Table 4-1. Safety Information Exchange Scenarios for Interoperability Testing**

<b>Scenario</b>
<i>Report inspection via SAFER DM (AFF)</i>
<i>Report inspection via CVIEW DM (AFF)</i>
<i>Report inspection via SAFER DM (EDI)</i>
<i>Report inspection via CVIEW DM (EDI)</i>
<i>Report inspection via SAFER DM (CIA)</i>
<i>Process request for inspection report via SAFER (AFF)</i>
<i>Process request for inspection report via CVIEW (AFF)</i>
<i>Process request for inspection report via SAFER (EDI)</i>
<i>Process request for inspection report via CVIEW (EDI)</i>
<i>Process request for inspection report via SAFER (CIA)</i>
<i>Maintain intrastate snapshots (detailed tests TBD)</i>
<i>Process request for snapshot via SAFER</i>
SAFER process vehicle snapshot request from legacy credential product
SAFER process carrier snapshot request from legacy credential product
SAFER process vehicle snapshot request from Roadside Operations
SAFER process carrier snapshot request from Roadside Operations
SAFER process carrier snapshot request from ASPEN
<i>Process request for snapshot via CVIEW</i>
CVIEW process vehicle snapshot request from legacy credential product
CVIEW process carrier snapshot request from legacy credential product
CVIEW process vehicle snapshot request from Roadside Operations
CVIEW process carrier snapshot request from Roadside Operations
CVIEW process carrier snapshot request from ASPEN

Notes:

- AFF stands for application file format, a precursor to EDI.
- CIA stands for custom interface agreement, referring to non-AFF, non-EDI exchanges.
- The development of standard interoperability tests is not necessarily planned for all scenarios listed. Please see the interoperability testing documents (References 33, 6, 19-21) for more information.

This Page Intentionally Blank

## 5. CRITICAL DECISIONS

In this chapter, we identify some of the decisions that are critical to successful implementation of Commercial Vehicle Information Systems and Networks (CVISN) Level 1 Safety Information Exchange. The chapter is intended to serve as a checklist to remind states about some of the major planning and design issues they should settle as early in the process as possible. Other decisions may be just as critical for a given state.

### 5.1 Design Decisions

The decisions listed below are categorized as “design” because they have a significant impact on the design approach. They all impact planning as well.

**Will the state implement a CVIEW (or equivalent) system?** CVIEW is a distributed version of the OMCS-developed SAFER system. It is owned by and located in a state that chooses to use CVIEW as a data exchange mechanism. A state would implement and deploy a CVIEW (or equivalent) system to:

- Provide for the electronic exchange of state-based interstate carrier and vehicle safety and credential data between state source/legacy systems, users, and SAFER
- Provide for the electronic exchange of intrastate carrier and vehicle safety and credential data between state source systems and users
- Serve as the repository for a state-selected subset of interstate carrier and vehicle safety and credential data
- Serve as the repository for a state-selected subset of intrastate carrier and vehicle safety and credential data
- Provide inter- and intrastate carrier and vehicle safety and credential data to the roadside to support electronic screening and other roadside operations

Could a state perform some or all of these functions by exchanging data with SAFER alone? Since SAFER functions to exchange carrier, vehicle, and driver information across jurisdictional boundaries, i.e., is involved with the exchange of interstate data, a state choosing not to implement CVIEW could only provide interstate data to its internal systems, including the roadside, that directly subscribed to SAFER. The exchange of intrastate data within the state would have to be handled in a different way. CVIEW, or its equivalent, is one method for providing that service.

**Will the state build a CVIEW (or equivalent) from scratch or start with the generic FMCSA-developed model?** The FMCSA-developed model has benefited from the design and implementation of the SAFER system since CVIEW shares a large number of common functions with SAFER and is in fact, a distributed version of that system. The main difference between the two systems is that CVIEW, via legacy system interface (LSI) modules, can be customized to interface with state-specific systems; SAFER does not support customization for individual states. A state choosing to use the generic model has the advantage of leveraging off an existing functional system that, by definition, is designed to interface with SAFER and other client systems, such as ASPEN. To develop CVIEW from “scratch” would likely involve the investment of several millions of dollars of state funds to complete the work. See the JHU/APL CVISN Web site at <http://www.jhuapl.edu/cvisn> for available CVIEW documentation.

**What functions will the CVIEW (or equivalent) system perform?** A state’s CVIEW, or equivalent system, should be capable of performing the following functions:

- Provide for the electronic exchange of state-based interstate carrier and vehicle safety and credential data between state source/legacy systems, users, and SAFER
- Provide for the electronic exchange of intrastate carrier and vehicle safety and credential data between state source systems and users
- Serve as the repository for a state-selected subset of interstate carrier and vehicle safety and credential data
- Serve as the repository for a state-selected subset of intrastate carrier and vehicle safety and credential data
- Provide inter- and intrastate carrier and vehicle safety and credential data to the roadside to support electronic screening and other roadside operations

A state may choose to implement other state-specific functions in CVIEW or implement some of the functions listed above in other state systems.

**Does the state use or intend to use ASPEN for inspections?** ASPEN is a client system deployed in over forty states throughout the U.S. that allows roadside inspectors to record and store inspection results electronically and forward that information to SAFER and/or CVIEW, SAFETYNET, and MCMIS. A supplementary application referred to as the Past Inspection Query (PIQ), allows any inspector throughout the country to retrieve inspections previously stored in the SAFER system for the most recent forty-five day period. If a state chooses not to deploy ASPEN, the state must be prepared to develop, either directly via internal staff or indirectly via an independent vendor, an equivalent set of applications to perform analogous functions.

**Will CVIEW (or equivalent) act as the single snapshot and inspection report interface system for ASPEN units in the field?** Today, ASPEN clients interface to SAFER to download weekly updates of carrier snapshot data that are used by the ISS algorithm and to upload electronically-captured inspection reports. Although CVIEW Version 1.5 supports the former function, the latter function along with inspection retrieval capability via PIQ will not be supported until Version 3.0, which is expected to be available in June 2000. With Version 3.0,

ASPEN clients could interface exclusively with their state's CVIEW system to perform all of the functions it now performs via its link to SAFER.

**What systems in the state will provide snapshot segment updates?** This decision will be based on the types of information your state will be capable of providing and willing to provide as segment updates to the snapshot data stored in your CVIEW or equivalent system. It will also depend on what information will be required at roadside sites within your state to support electronic screening, inspections, and other enforcement activities. For example, the state of Maryland made the design and implementation decision to initially provide IRP data to their CVIEW system via an IRP vehicle snapshot segment update. IRP data is transferred to an internal Maryland IRP workstation and then transmitted to and stored in their CVIEW system via a Legacy System Interface (LSI) using a flat file data exchange method. Upon receiving the data via the IRP LSI, CVIEW is configured to update the appropriate IRP segment in the vehicle snapshot without adversely affecting any other data elements.

Each state will have to decide which types of data are to be supplied to and stored in their CVIEW or equivalent system.

**Will the state maintain intrastate snapshots?** Your state needs to decide if the exchange of intrastate data, in the form of snapshots, is required in your state. Such information could be used at roadside sites to facilitate electronic screening and inspection of intrastate carriers, vehicles, and drivers or, in desk-side operations, to support grant or denial decisions for credential applicants. Should this be a requirement, your CVIEW or equivalent system would be used to facilitate the exchange of intrastate data within your state. Alternatively, a state could choose to exchange only interstate data within the state; however, most states would find that an unacceptable alternative.

**What snapshot views will be used where?** A view is a collection of all or a portion of the data elements within a particular type of snapshot. For example, an IRP view of the vehicle snapshot is comprised of only those data elements related to IRP in the vehicle snapshot. The types of data your state chooses to exchange within the state will determine the views that are needed to support that exchange. For example, ASPEN users that use the Inspection Selection System (ISS) would require data to be sent to them using the ISS View. The ISS View supplies ASPEN clients only those data elements that are needed by the ISS algorithm.

## 5.2 Planning Decisions

The decisions listed in this category usually do not impact design as much as they impact the preparation of task lists, assignments, schedules, and budget considerations.

**Build vs. Buy?** One of the most important decisions the project team must make is the "build-vs.-buy" decision. What should you buy and what should you get off the shelf? This question needs to be addressed for each safety system or subsystem, e.g., CVIEW or equivalent, ASPEN or equivalent, communication components, etc. As the decisions are made, keep in mind license considerations for commercial-off-the-shelf (COTS) products.

**Will the state update current legacy systems or re-compete/re-develop?** Sometimes a major project like implementing CVISN is the catalyst to re-evaluate existing systems and address lingering problems. As the design options are considered, legacy systems in place today and other possible substitutes should be examined. The decisions to build a new product or modify an existing one using either in-state resources or outside vendors should take into account the risks associated with each option, the available resources, existing contractual arrangements, and the state's experiences with the current products.

**Will the state participate in PRISM?** Some PRISM funding may be available. Please see Reference 12 for contact information. In addition, the PRISM processes should be considered as the top-level CVISN design for the state is established.

**What are the priorities and sequence for implementing capabilities?** For every state, some priorities and sequences for implementation make more sense than others. Both design and cost factors should be considered when establishing the baseline schedules. The relationship of CVISN activities to other state activities must also be considered. For example, many states were forced to divert CVISN personnel resources to address the Y2K problem. The process of incremental deliveries and testing may be new to some stakeholders. Defining the priorities and development sequence helps everyone understand when each capability will be ready, and what kinds of tests must be executed to verify the delivered components.

**Who is the system integrator?** A decision closely related to the build-vs.-buy decision is who will provide the system integration function. System integration refers to the process of integrating each system or subsystem into the whole, testing the interfaces, testing the functionality, testing the overall flow, and testing for interoperability, performance and reliability. Some alternatives are:

- The state builds everything in-house and does the system integration with in-house staff.
- The state buys some products, builds some in-house, and integrates them with in-house staff.
- The state hires a system integrator to integrate all the purchased and in-house systems in the safety information area.
- The state contracts with a system integrator to serve as prime contractor and deliver a complete working system.

**Should the state have an independent verification and validation (V&V) agent?** Some states have policies that encourage them to hire an independent verification and validation agent to provide independent technical assessment and guidance as the project proceeds. If the agent has experience from other similar projects, they can be very helpful. They may serve as an acceptance test conductor or witness to ensure independence in the test process.

**Sole Source or Competitive Contracting?** Sole source contracting is sometimes selected if the state believes that a particular vendor is uniquely qualified to perform a particular portion of the work. In some cases, sole source contracts can be put in place more quickly than contracts established through a competitive bidding cycle. Sole source contracting may not be an option since most states require competition whenever possible.

### 5.3 Funding and Contracting Decisions

These are issues that must be faced during the funding and contracting phase of the project. They are not unique to the area of safety information exchange.

- How much funding is required to complete the project?
- Where will the funding be obtained?
- What type of procurement should be used for each product or service?
- What can be done to expedite procurements?
- What type of incentives and remedial mechanisms should be included in the contracts?
- What software rights should be included in the contracts?
- How can the RFPs be written to assure architectural conformance and interoperability?

### 5.4 Development Decisions

These are issues that must be faced during the development phase of the project. They are not unique to area of safety information exchange.

- How should the initial design be modified based on the experience gained in each phase?
- How should the initial phase plan be modified based on progress actually made in each phase?

This Page Intentionally Blank

## 6. REQUIREMENTS AND DESIGN GUIDANCE

According to the Transportation Equity Act for the 21<sup>st</sup> century (TEA-21), states using federal funds (Highway Trust Funds) must conform with the National Intelligent Transportation System (ITS) architecture and standards, which include the Commercial Vehicle Information Systems and Networks (CVISN) and International Border Clearance (IBC) architecture and standards. References 23 and 24 contain initial draft guidance from the United States Department of Transportation related to conformance. Rulemaking related to architecture conformance is expected in CY 2000. Broadly stated, for safety information exchange, “conforming with the architecture,” means:

- Agreeing with the principles and following the guidance in the CVISN Operational and Architectural Compatibility Handbook (COACH) Part 1 (Reference 2),
- Using the electronic data interchange (EDI) standards and common identifiers as explained in the COACH Part 4 (Reference 5), and
- Conducting interoperability tests to demonstrate the criteria defined in the COACH Part 5 (Reference 6).

The CVISN System Design Description (Reference 7) illustrates the top-level requirements for Safety Information Exchange, and shows the generic CVISN state design approach. The COACH Part 3 (Reference 4) takes the COACH Part 1 state safety information exchange-related requirements and allocates them to components of the generic CVISN state design, providing a model for states to tailor.

Recall the high-level definition of CVISN Level 1 as stated in Reference 8:

- ASPEN (or equivalent) at all major inspection sites.
- Connection to the Safety and Fitness Electronic Records (SAFER) system to provide exchange of interstate carrier and vehicle snapshots among states.
- Implementation of the Commercial Vehicle Information Exchange Window (CVIEW) (or equivalent) system for exchange of intrastate and interstate snapshots within the state and connection to SAFER for exchange of interstate snapshots.

### 6.1 Safety Information Exchange – Conforming With the Architecture

In this section, we illustrate various approaches to safety information exchange. Some are marked as explicitly conforming to the architecture. Others do not meet the architecture requirements, but are acceptable alternatives as long as some other approach to safety information exchange that does conform to the architecture is also implemented.

Since the use of open standards is a key architectural concept, it is important that states support the use of the identified EDI X12 transactions, where applicable. In particular, data exchange operations from SAFER to CVIEW, or its equivalent, and the ROC, should employ the use of EDI X12 transactions. An exception to this requirement has been made for ASPEN and SAFETYNET at the direction of the FMCSA to avoid the cost of EDI translators. This is an

acceptable solution because the FMCSA maintains direct control over data exchange operations between SAFER and these systems.

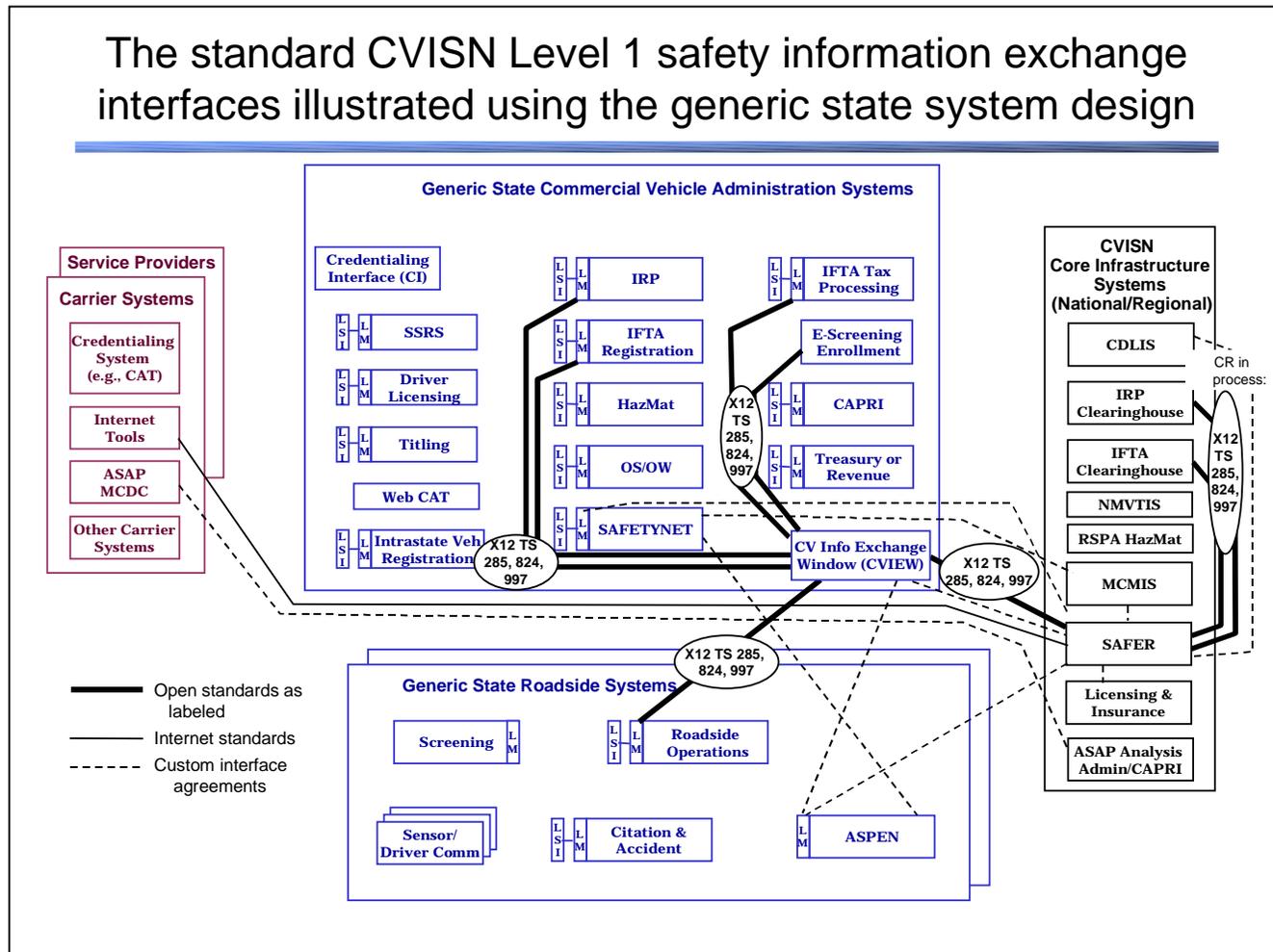
Several design options are depicted on following pages. The examples do not exhaust the possibilities, but do represent a variety of choices that have been considered by early implementers.

The architecture may be updated to include use of additional standards, if recommended by a consensus of the stakeholder community. These may include one or more electronic methods of credit card payment for data products or services, and the use alternate data formatting standards such as the Extensible Markup Language (XML).

Support of the standards identified in the architecture (shown in Figure 6-1 and below) is necessary for architecture conformance. The EDI transaction sets (TSs) associated with safety information exchange are:

- TS 285 Commercial Vehicle Safety & Credentials Information Exchange
- TS 284 Commercial Vehicle Safety Reports
- TS 824 Application Advice
- TS 997 Functional Acknowledgement

Figure 6-1 and the following list summarizes the EDI requirements related to safety information exchange from the COACH Part 4 (Reference 5).



**Figure 6-1. CVISN Level 1 Interfaces Related to Safety Information Exchange**

- If a state chooses to use EDI internally to update snapshots, the state legacy credentialing system(s) or state Credentialing Interface (CI) should be capable of requesting, updating and receiving carrier and vehicle safety and credential information to/from CVIEW, or its equivalent, via EDI X12 standard transactions (285, 824, 997). Alternatively, a state-specific flat file/LSI method could be used.
- To conform with the architecture, a state's CVIEW, or equivalent, should be capable of requesting, updating and receiving carrier and vehicle safety and credential information to/from SAFER via EDI X12 standard transactions (285, 824, 997) or via the existing CIA.
- If a state chooses to use EDI internally to send snapshots to the roadside, a state's roadside system, e.g., the Roadside Operations Computer (ROC), should be capable of requesting and receiving carrier and vehicle safety information to/from CVIEW, or its

equivalent, via EDI X12 standard transactions (285, 824, 997). Alternatively, a state-specific flat file/LSI method could be used.

- To conform with the architecture, ASPEN inspection systems should be capable of submitting, requesting, and receiving inspection reports to/from CVIEW, its equivalent, or SAFER via the existing Custom Interface Agreement (CIA).
- To conform with the architecture, non-ASPEN inspection systems should be capable of submitting, requesting, and receiving inspection reports to/from CVIEW, its equivalent, or SAFER via EDI X12 standard transactions (284, 824, 997).
- To conform with the architecture, CVIEW or its equivalent, should be capable of submitting, requesting, and receiving inspection reports to/from SAFER via EDI X12 standard transactions (284, 824, 997) or the existing CIA.

## 6.2 Focus on ASPEN or Its Equivalent

Your state will have to decide whether to use the ASPEN client, developed by the FMCSA, or some equivalent system developed by internal state staff or outside vendors. The term “ASPEN client” refers collectively to the software applications that reside on the client for recording and transmitting inspections electronically (ASPEN), for supporting the ISS algorithm (ISS), and for retrieving previously stored inspections (PIQ). The functions that need to be supported include:

- Recording inspection data electronically
- Electronic transmission of inspection reports to SAFER, either directly or via CVIEW or its equivalent
- Electronic retrievals of inspection reports from SAFER, either directly or via CVIEW or its equivalent
- Download of carrier snapshots via subscription processing to support the ISS

The choice of whether to use the existing ASPEN client or build an equivalent product depends on:

- The level of state funding available to support new development efforts
- Assuming the work will be done in-house, the expertise of your state’s information systems (IS) staff in the areas of client/server software, relational database design and development, data formatting strategies, such as the use of X12 EDI, and TCP/IP network communications
- The lag time your state is willing to tolerate before a client is available to support the functions mentioned above

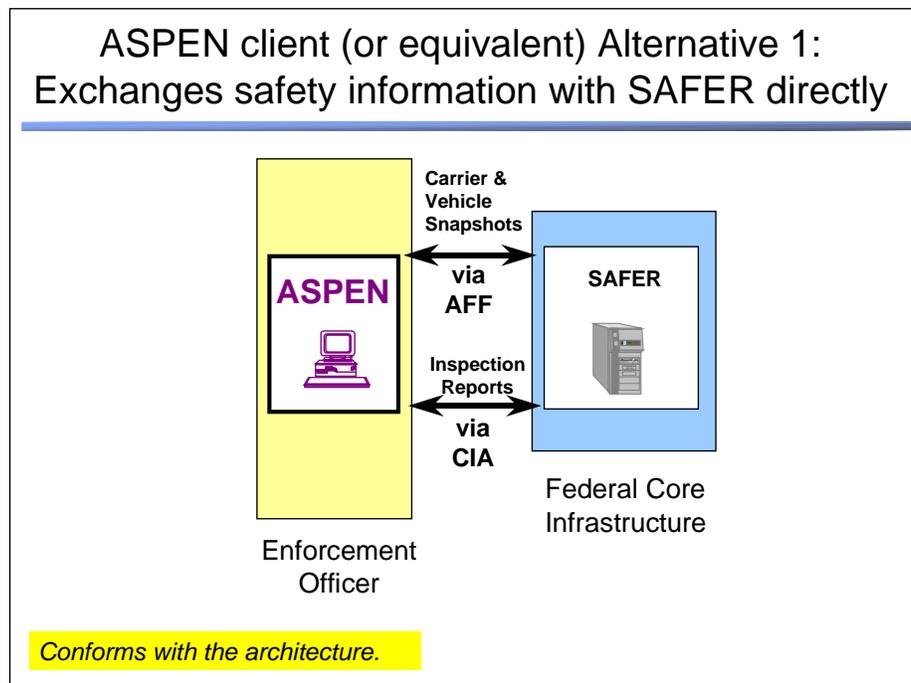
## 6.2.1 Design Options

In the diagrams below, the focus is on the choices the state will need to make regarding how the ASPEN client, or its equivalent, will exchange safety information with SAFER. Basically, the state has three choices:

- The ASPEN client communicates directly with SAFER
- The ASPEN client communicates with SAFER via the state's CVIEW system, or equivalent
- The ASPEN client communicates with SAFER via the state's SAFETYNET system

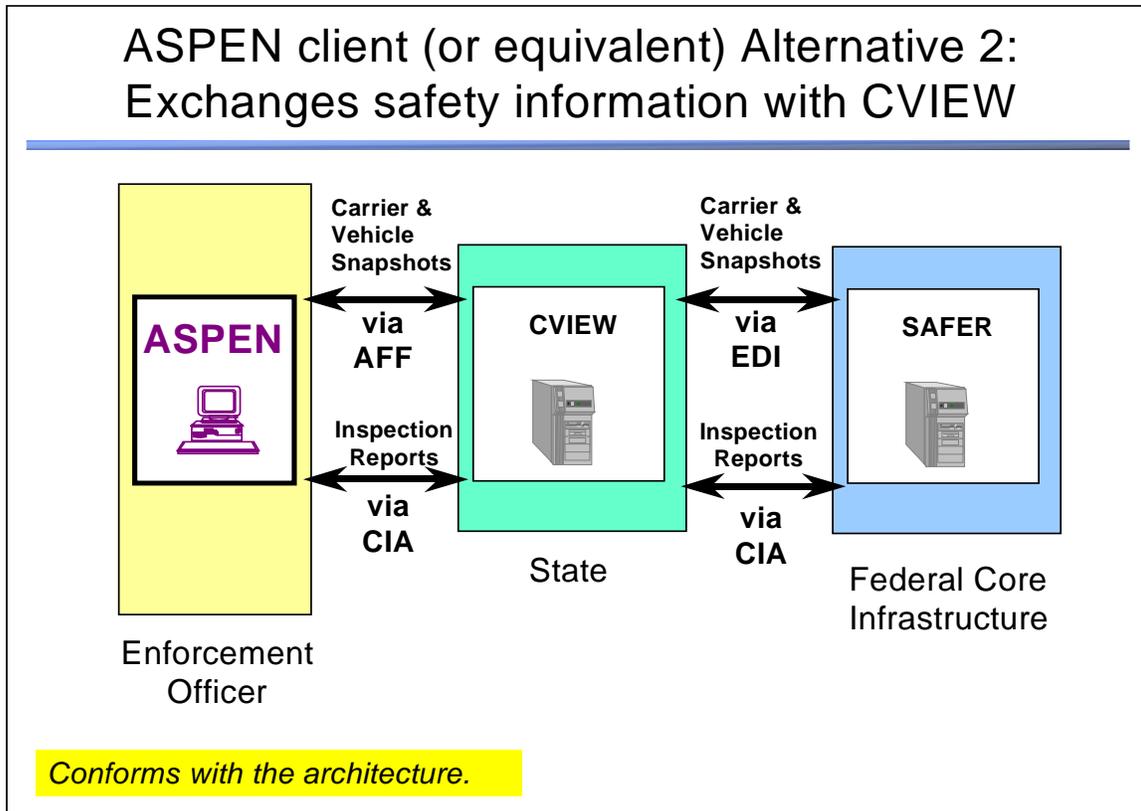
In Figure 6-2, an enforcement officer sends and retrieves inspection reports and downloads carrier ISS subscription data to/from the ASPEN client, or its equivalent, via direct communications with the SAFER system. The inspection report and ISS subscription transactions are performed using customized interface agreement (CIA), and AFF data formatting methods, respectively. This approach is most suitable where

- A state elects not to develop a CVIEW system, or its equivalent, but wants to support ASPEN data exchange or
- CVIEW will be developed or is in the process of being developed but is not yet ready to provide data exchange support within the state.



**Figure 6-2. ASPEN Client Communicates Directly With SAFER**

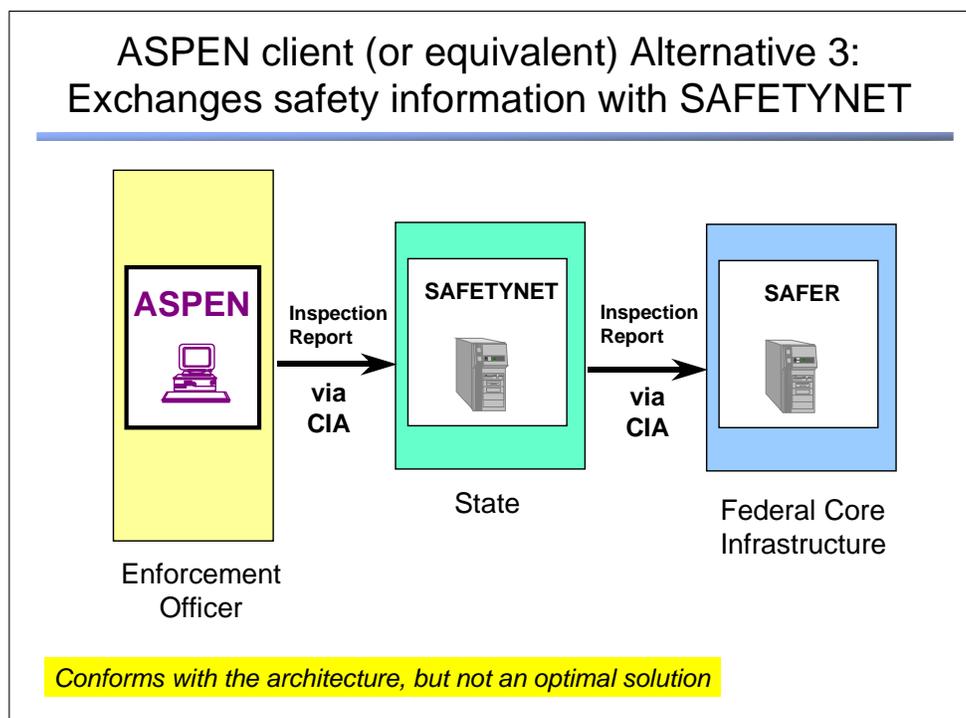
In Figure 6-3, an enforcement officer sends and retrieves inspection reports and downloads carrier ISS subscription data to/from the ASPEN client, or its equivalent, via direct communications with the state's CVIEW system, which in turn, communicates with SAFER on behalf of the client. Between ASPEN and CVIEW, inspection report uploads and queries and ISS subscription downloads are performed using customized interface agreement (CIA), and AFF data formatting methods, respectively. Between CVIEW and SAFER, inspection reports uploads and queries and carrier and vehicle subscription data are exchanged using the existing customized interface agreement (CIA), and EDI formatting methods, respectively.



**Figure 6-3. ASPEN Communicates With SAFER via CVIEW**

The exchange of safety information between ASPEN and SAFER via CVIEW will be supported with the release of Version 3.0 of the SAFER and CVIEW software, which is planned for the fourth quarter of CY 2000. If a state chooses to deploy a CVIEW system, Figure 6-3 represents the preferred architectural approach for uploading and downloading safety information from/to ASPEN or its equivalent.

In Figure 6-4, an enforcement officer, using ASPEN, or its equivalent, sends inspection reports to the state's SAFETYNET system, which in turn uploads that information to SAFER via the SAFER Data Mailbox using the existing CIA. Although this method allows inspectors to send inspection reports to SAFER, it does not provide them the ability to download ISS data from SAFER nor query SAFER for previously stored inspection reports. Although this approach is considered to conform with the CVISN architecture, it is not an optimal solution for the reasons stated above.



**Figure 6-4. ASPEN Communicates With SAFER via SAFETYNET**

## 6.2.2 Data Exchange Formats

ASPEN does not currently support safety data exchange via the use of Electronic Data Interchange (EDI). The primary reason for that decision was the cost of equipping each ASPEN client with an EDI translator, i.e., the software component responsible for translating EDI-formatted data into a format that is expected by the receiving application. To exchange data with SAFER and CVIEW, or its equivalent, the ASPEN client has incorporated a set of software tools, referred to as the SAFER and CVIEW Application Programming Interface (SCAPI) that performs all of the data formatting and communication functions needed by the client to communicate with the SAFER and CVIEW systems. See Reference 35 for a detailed description of the SCAPI.

### 6.3 Focus on CVIEW

Your state will have to decide whether to use the FMCSA-developed CVIEW system, or some equivalent system developed by internal state staff or outside vendors. The functions that need to be supported include:

- For the ASPEN client, or its equivalent, subscription download and online query of carrier snapshots to support the ISS algorithm via AFF and the upload and retrieval of inspection reports via the existing CIA
- For the Roadside Operations Computer (ROC), subscription download and online query of carrier and vehicle snapshots to support electronic screening operations via EDI X12 standard transactions (285, 824, 997) or a state-specific flat file/LSI method
- For state systems, subscription download of carrier and vehicle snapshots and the upload of carrier and vehicle safety information, and supporting credential data, in the form of snapshot segments updates via either EDI X12 standard transactions (285, 824, 997) or legacy system interfaces (LSIs)
- Electronic upload and retrieval of inspection reports to/from SAFER via either EDI X12 standard transactions (284, 824, 997) or existing CIAs, e.g., ASPEN-formatted inspection reports
- Subscription download of carrier and vehicle snapshots from SAFER via EDI X12 standard transactions (285, 824, 997).

The choice of whether to use the existing FMCSA-developed CVIEW system or build an equivalent product depends on:

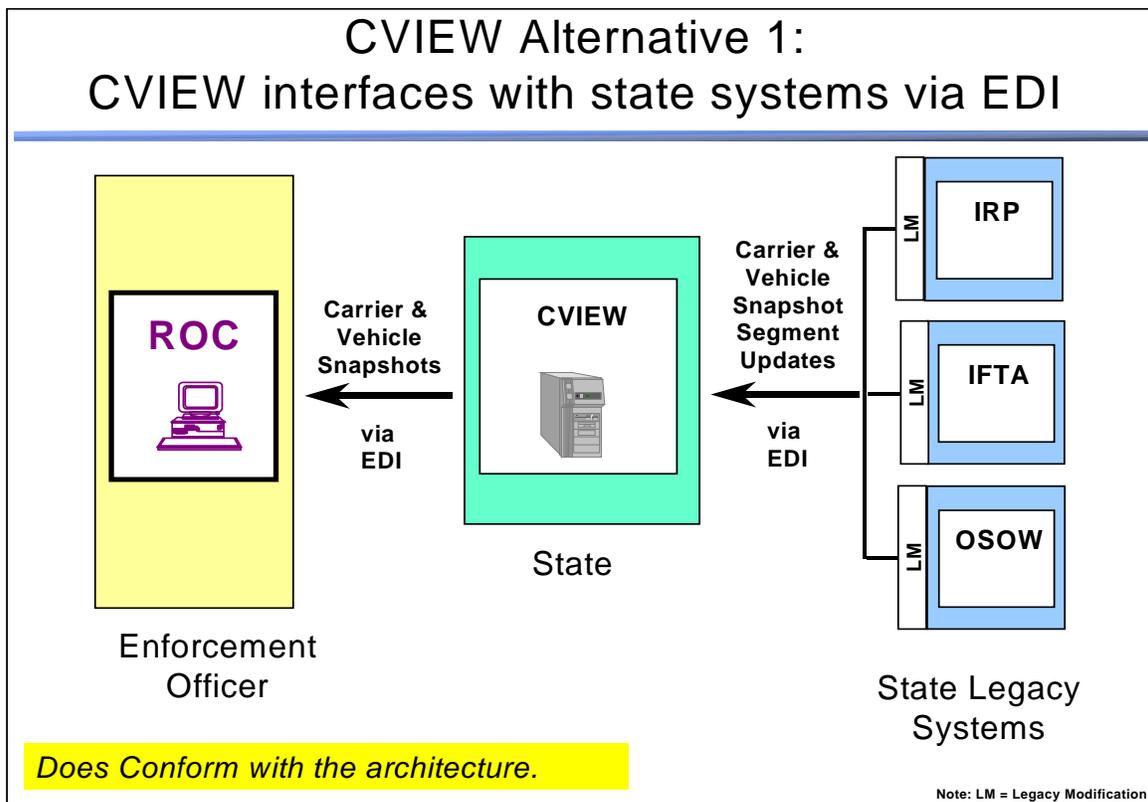
- The extent of state-specific requirements that are not satisfied by the FMCSA-developed CVIEW system
- The level of state funding available to support new development efforts
- Assuming the work will be done in-house, the expertise of your state's information systems (IS) staff in the areas of client/server software, relational database design and development, data formatting strategies, such as the use of X12 EDI, and TCP/IP network communications
- The lag time your state is willing to tolerate before a CVIEW system is available to support the functions mentioned above

### 6.3.1 Design Options

In the diagrams below, the focus is on the choices the state will need to make regarding how its CVIEW system, or equivalent, will exchange safety information with SAFER and other systems within the state. Aside from the issue of supporting all of the functions mentioned above, there are two additional design choices the state must make:

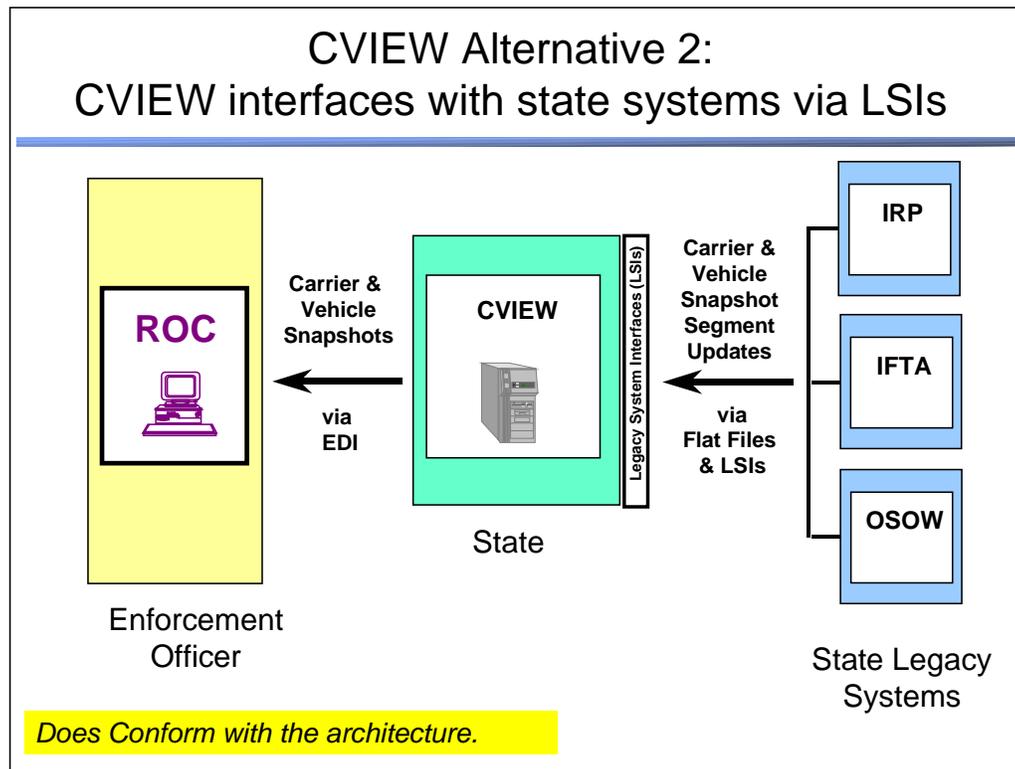
- How to interface CVIEW with existing or new state systems, i.e., should CVIEW interfaces with state systems via EDI or the use of flat files via Legacy System Interfaces (LSIs)
- Whether or not the state should send its IRP and IFTA data directly to its CVIEW system, or equivalent, for upload to SAFER and download to its roadside systems or send it directly to the IRP and IFTA Clearinghouses

In Figure 6-5, legacy systems within the state send CVIEW, or its equivalent, carrier and/or vehicle updates from each of their respective systems via EDI X12 standard transactions (285, 824, 997). In many cases, this requires a modification to the state's legacy system(s) (shown as LM box). CVIEW, or its equivalent, updates its internal snapshot database and provides that information to any client systems, e.g., a ROC, that have requested that data via the subscription process using EDI X12 standard transactions (285, 824, 997). The use of EDI to standardize data exchange among state systems is not required by the CVISN architecture and therefore, is considered an optional approach.



**Figure 6-5. CVIEW Communicates With State Systems via EDI**

In Figure 6-6, legacy systems within the state send CVIEW, or its equivalent, carrier and/or vehicle updates from each of their respective systems via flat files and legacy system interfaces (LSIs), a software toolkit that is designed to interpret and manipulate data received in flat file format. CVIEW, or its equivalent, updates its internal snapshot database and provides that information to any client systems, e.g., a ROC, that have requested that data via the subscription process using EDI X12 standard transactions (285, 824, 997). This approach is most suitable when a state wants to minimize changes to existing legacy systems, e.g., incorporation of EDI capabilities, and take advantage of existing flat files to support data exchange operations.



**Figure 6-6. CVIEW Communicates With State Systems via LSIs**

### 6.3.2 Data Exchange Formats

The FMCSA-developed CVIEW system supports safety data exchange via the use of Electronic Data Interchange (EDI) and legacy system interfaces (LSIs). Again, the choice using one vs. the other or a combination of both, e.g., EDI with some systems and LSIs with others, is a decision the state must make. Development of unique LSIs is usually required.

### 6.3.3 FMCSA Development and Maintenance Support for CVIEW

The FMCSA has sponsored and funded the development of CVIEW to facilitate state-level exchange of inter- and intrastate carrier, vehicle, and driver safety and credential data to support electronic screening operations and to allow states greater control and flexibility for establishing interfaces with internal state legacy systems.

The FMCSA will continue to fund development and maintenance support of CVIEW through Version 3.0, which includes all of the capabilities required for CVISN Level 1 compatibility. Due to delays associated with supporting SAFETYNET 2000 data exchange requirements in SAFER/CVIEW Version 2.0 and the accelerated schedule for migrating the SAFER System to the DOT Volpe Center, **CVIEW Version 3.0 will not be released until the fourth quarter of CY 2000.** Maintenance support for Version 3.0 will continue through December 2000. **As of January 2001, the FMCSA support for CVIEW development and maintenance activities will be discontinued due to funding limitations.** States that elected to develop a CVIEW system based on the FMCSA-sponsored model will be required, at that time, to assume responsibility for CVIEW enhancement and maintenance operations.

In CY 2003, the FMCSA plans to allow states to use MCMIS and SAFER to support the exchange of intrastate safety data and credential flags. CVIEW or its equivalent, e.g., a custom state system, will fill this role until then. When intrastate data services are operational in 2003, each state will have at least three options to choose from for exchanging this type of information. They may use the federally supported SAFER system, they may continue to use and maintain CVIEW or they may use a custom state system.

In the 2003 time frame, SAFER communications will support Internet-based methods for exchanging snapshots, profiles, crash reports, inspection reports, compliance review reports, and all safety reports provided on interstate and intrastate carriers.

Configuration control of carrier, vehicle, and driver snapshots that are used by SAFER and CVIEW, or its equivalent, will be maintained by JHU/APL. This is important because if changes are made to SAFER snapshots, CVIEW (or equivalent, systems that provide or use snapshot data) may also require modification. The formal definition of the snapshot data elements are documented in Reference 38, which is available via the CVISN Web site at <http://www.jhuapl.edu/cvisn/downdocs/index.html#post-scope>. Any planned changes to those definitions will be posted via the Web site including a method for providing comments to JHU/APL prior to change implementation.

A similar approach for posting other types of planned changes, e.g., communication enhancements, to the SAFER system that may have potential impacts on fielded CVIEW (or equivalent) systems will also be provided via the CVISN Web site.

## 6.4 Focus on SAFER

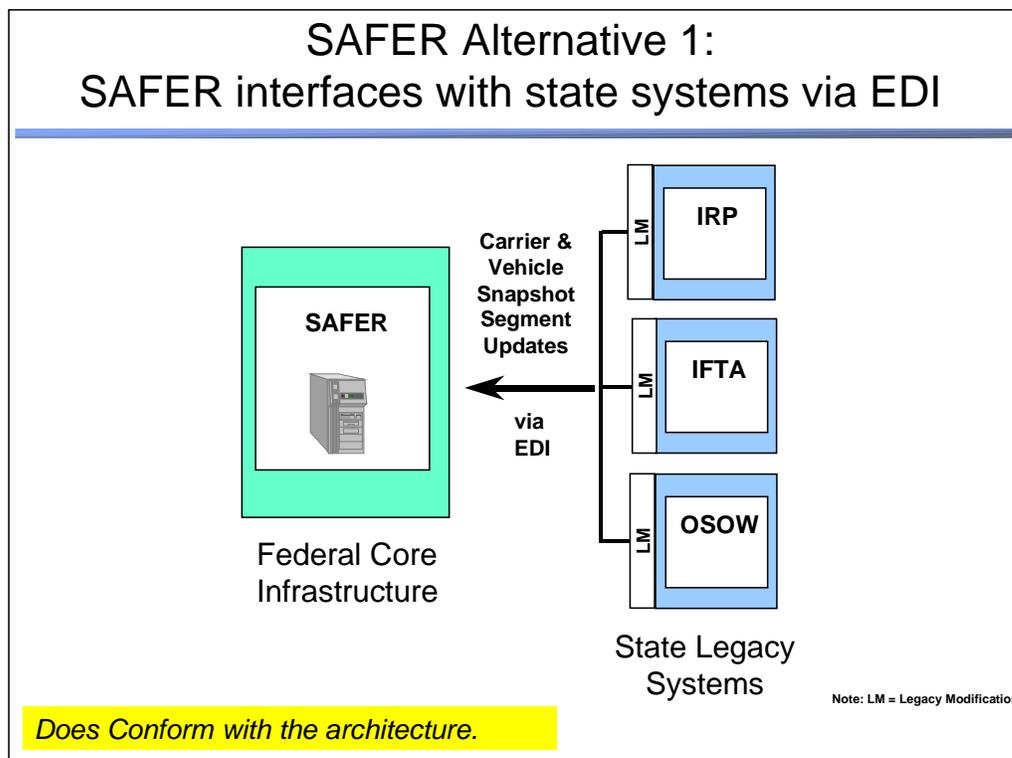
Your state will have to decide whether to perform most safety data exchange via CVIEW (or its equivalent) or to perform some of those activities directly with SAFER. For example, SAFETYNET 2000 is already designed to interface only to SAFER. The functions that SAFER supports include:

- For ASPEN clients, or equivalent, subscription download and online query of carrier snapshots to support the ISS algorithm via AFF and the upload and retrieval of inspection reports via the existing CIA
- For SAFETYNET clients, subscription download of carrier snapshots and uploads of inspection reports via AFF, upload of compliance reviews, crash and enforcement data via CIAs, and online queries for carrier profiles, crash and inspection report facsimiles via a combination of AFF and CIAs
- For the Roadside Operations Computer (ROC), subscription download and online query of carrier and vehicle snapshots to support electronic screening operations via EDI X12 standard transactions (285, 824, 997)
- For state legacy systems, subscription download of carrier and vehicle snapshots and the upload of carrier and vehicle safety information, and supporting credential data, in the form of snapshot segments updates via EDI X12 standard transactions (285, 824, 997); **Note: unlike CVIEW, SAFER does not support legacy system interfaces with state systems**
- Electronic upload and download of inspection reports from/to CVIEW via either EDI X12 standard transactions (284, 824, 997) or existing CIAs, e.g., ASPEN-formatted inspection reports
- Subscription upload of carrier and vehicle snapshot segments from CVIEW via EDI X12 standard transactions (285, 824, 997).

### 6.4.1 Design Options

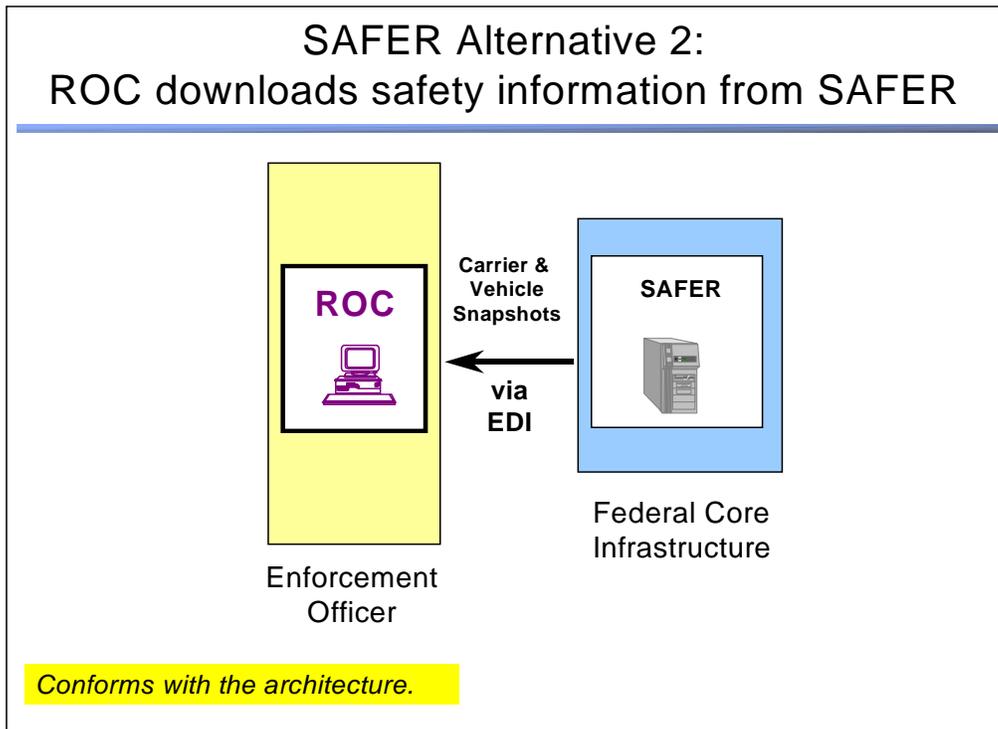
In the diagrams below, the focus is on the choices the state will need to make regarding what types of data exchange operations, in addition to SAFETYNET exchange, will be performed directly with the SAFER system. Although connecting state systems to SAFER via CVIEW is the recommended approach (see Figure 6-3 as an example) a direct linkage between multiple roadside and administrative state systems and SAFER is a supported option. Two example design options are provided below.

In Figure 6-7, legacy systems within the state send SAFER carrier and/or vehicle updates from each of their respective systems via EDI X12 standard transactions (285, 824, 997). SAFER updates its internal snapshot database and provides that information to any client systems, e.g., a ROC, that have requested that data via the subscription process using EDI X12 standard transactions (285, 824, 997). **Note: unlike CVIEW, SAFER does not support legacy system interfaces with state systems.** This approach is most suitable when state legacy systems are already EDI capable.



**Figure 6-7. SAFER Communicates With State Systems via EDI**

In Figure 6-8 below, the Roadside Operations Computer (ROC), performs subscription download functions and online queries of carrier and vehicle snapshots to support electronic screening operations via EDI X12 standard transactions (285, 824, 997). This approach is most suitable if a state chooses to interface some or all of its roadside systems to SAFER directly.



**Figure 6-8. SAFER Communicates With State Systems via EDI**

## 6.5 Focus on Communications

Your state will have to determine the types of support needed for communications between the following systems:

- ASPEN client (or equivalent) and the SAFER and/or CVIEW systems
- SAFETYNET and SAFER systems
- CVIEW and SAFER systems

### 6.5.1 SAFER Communications

The SAFER system currently supports the following TCP/IP-based wide area network (WAN) link options (See Reference 39):

1. Internet
2. AAMVAnet frame-relay
3. FTS2000 frame-relay
4. Bell Atlantic
- 5.

In addition, a digital modem bank employing 800 number, toll-free access provides standard public service telephone network (PSTN) and analog, circuit-switched cellular dial-up support to users.

#### 6.5.1.1 *Internet Communications*

SAFER supports Internet access to the SAFER home page, which allows users to query the SAFER database to obtain carrier and shipper census, safety, and licensing and insurance credential information.

SAFER also supports Internet access for non-Web-based data exchange operations. An Internet service provider (ISP) could provide access to SAFER for both types of operations. Use of an ISP is a low cost communications solution; however, it is only as reliable as is the Internet in general. In addition, access via the Internet requires establishing a point-to-point tunneling protocol (PPTP) link to SAFER that provides communications security between SAFER and the client by forcing the password and subsequent data transmissions to be encrypted. The State of Kentucky currently uses this approach to facilitate communications between its CVIEW system and SAFER.

### 6.5.1.2 AAMVAnet Frame-relay

SAFER supports communications over the AAMVAnet, Inc., frame-relay WAN. This is a private network that offers greater reliability and trouble-shooting diagnostics than the Internet solution but at a substantially higher cost. The CVISN Prototype States of Maryland and Virginia use the AAMVAnet WAN to provide communications between their CVIEW systems and SAFER. AAMVAnet also supports local PSTN and 800# dial-up services for users/organizations not wanting to expend the funds needed to support a leased line approach. For more information on the types of communication lines offered, their costs, and supporting network services, please contact AAMVAnet, Inc. directly.

### 6.5.1.3 FTS2000

FTS2000 is a frame-relay WAN that supports communications among federal systems. In the near-future, SAFER will use this WAN to communicate with the Motor Carrier Management Information System (MCMIS) for the exchange of weekly carrier census and safety information. Currently, this is being accomplished via the Internet. It is envisioned the next version of FTS2000, i.e., FTS2001, will support communications among both federal and state systems. FTS2000 also supports local PSTN and 800# dial-up services for users/organizations not wanting to expend the funds needed to support a leased line approach. For more information on the types of communication lines offered, their costs, and supporting network services, please contact the FMCSA, directly.

### 6.5.1.4 Bell Atlantic

SAFER supports a connection to the Bell Atlantic WAN to facilitate wireless Cellular Digital Packet Data (CDPD) communications. The CDPD approach allows enforcement officers in mobile units to communicate with SAFER and perform the same data exchange functions as officers in fixed roadside sites. For more information on the types of communication lines offered, their costs, and supporting network services, please contact Bell Atlantic, directly.

## 6.5.2 CVIEW Communications

A state that chooses to use CVIEW as a data exchange mechanism will have to decide how that system will communicate with state legacy systems, state roadside systems, e.g., ASPEN, or equivalent, and SAFER. Issues to be resolved include:

- What WAN communications links currently exist within the state and can one or more of those links be used to facilitate communications between CVIEW and other state systems?
- Do any of the links needed to support communications between the state's CVIEW system and SAFER correspond to the WAN providers identified in section 6.5.1? If not, the state needs to either: 1) add an existing SAFER communications link to their CVIEW system or 2) request the FMCSA to add an additional communications link to SAFER to support their state's communication requirements.

### **6.5.3 SAFETYNET Communications**

The current CVISN architecture specifies that SAFETYNET will not communicate with a state's CVIEW system. Rather, it will communicate with SAFER directly, i.e., all inter-and intrastate inspection reports, compliance reviews, enforcement and crash data will be sent to SAFER from SAFETYNET via the SAFER Data Mailbox system. Communications between SAFER and a state's SAFETYNET sites can be accomplished via the communication mechanisms identified in section 6.5.1, options 1-3. Option 4, wireless communications, would not typically be required as a SAFETYNET communications option.

### **6.5.4 ASPEN, or equivalent, Communications**

The ASPEN client, which, in addition to the ASPEN application, includes the Inspection Selection System (ISS), and Past Inspection Query (PIQ) applications, needs to communicate with the either SAFER or the state's CVIEW system. If a state elects to have ASPEN clients communicate directly with SAFER, options 1,2 and 4, specified in section 6.5.1, would support ASPEN to SAFER communications. If a state requires ASPEN clients to communicate with SAFER via CVIEW, then some combinations of options 1-4, specified in section 6.5.1, could be used to facilitate communications among these systems.

### **6.5.5 ROC Communications**

The ROC client needs to communicate with either SAFER or the state's CVIEW system. If a state elects to have ROC clients communicate directly with SAFER, options 1,2 and 3, specified in section 6.5.1, would support ROC to SAFER communications. If a state requires ROC clients to communicate with SAFER via CVIEW, then some combinations of options 1-3, specified in section 6.5.1, could be used to facilitate communications among these systems. The available combinations will depend on what communication links are supported by the state's CVIEW system.

This Page Intentionally Blank

## 7. RECOMMENDED DEVELOPMENT PROCESS

The *CVISN Guide to Top-Level Design* (Reference 18) and the *CVISN Guide to Program and Project Planning* (Reference 40) describe fundamental principles and generic processes. This chapter applies and tailors this guidance to the safety information exchange area. Some states may already have a well-documented methodology for information system development. If so, the state should follow that process, possibly making some adjustments to incorporate any ideas included here that aren't reflected in the state's standard procedures.

The first section in this chapter provides an overview of the entire process. Subsequent sections address each successive phase of the process, including these topics:

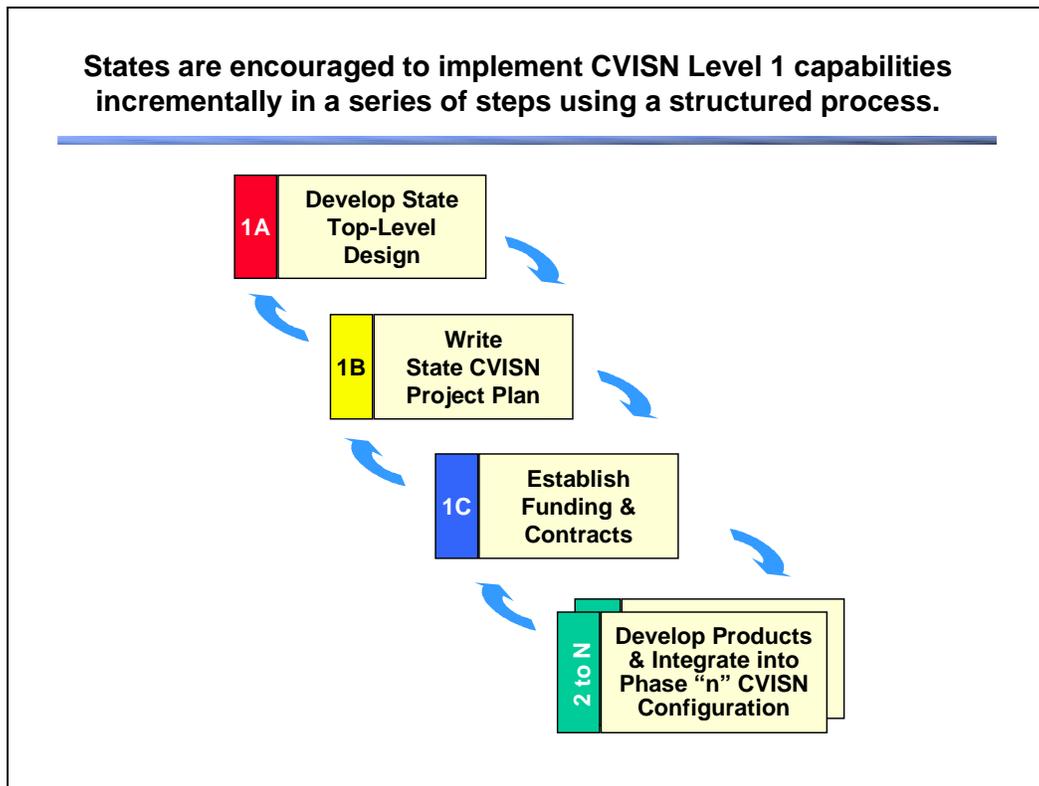
- Phase Process
- Phase Products
- Factors to Consider
- List of Key Decisions (refer to Chapter 5 for a description of each)
- Advice and Lessons Learned

A final section addresses requirements specification, a topic that impacts all phases.

### 7.1 Development Process Overview

The *Introductory Guide to CVISN* outlined a model development process for implementing CVISN capabilities. Figure 7-1 is repeated from that document as a reminder of the model.

Deploying CVISN Level 1 capabilities is a major undertaking that typically takes several years. In order to reduce risk, it is strongly recommended that states use an incremental deployment approach. It is critical that this large project be broken into a series of 3-6 month time periods called project phases. Specific results or products are defined for each phase. These are defined in detail for each phase just before it begins, and more broadly for subsequent phases. The use of phases allows taking a big job and breaking it into small, manageable pieces. If a state completes the first couple development phases on time and meets all the objectives, this provides assurance that the plan is realistic. If not, it allows the state to revise the plan and take other corrective actions prior to committing extensive resources to a project that is not properly structured for success. Incremental development and measurable milestones ensure stakeholder participation and feedback and real visibility into project progress.



**Figure 7-1. Overview of CVISN Deployment Process**

The figure shows that the first phase is devoted to developing the state top-level design, preparing the State CVISN Project Plan, establishing full funding for the project, and issuing major contracts for products and technical services. Each subsequent phase is a development phase that results in some type of demonstration or operational capability. More information on phases is provided in the *CVISN Guide to Program and Project Planning* (Reference 40) and the *CVISN Guide to Phase Planning and Tracking* (Reference 41).

This *CVISN Guide to Safety Information Exchange* has been prepared with the experience of early CVISN deployments in mind. It assumes that states will have to do considerable requirements analysis and state-specific planning. As time goes on and CVISN moves into the mainstream, this will be less the case. Some of the aspects of CVISN will become routine. This may be true for your state even now.

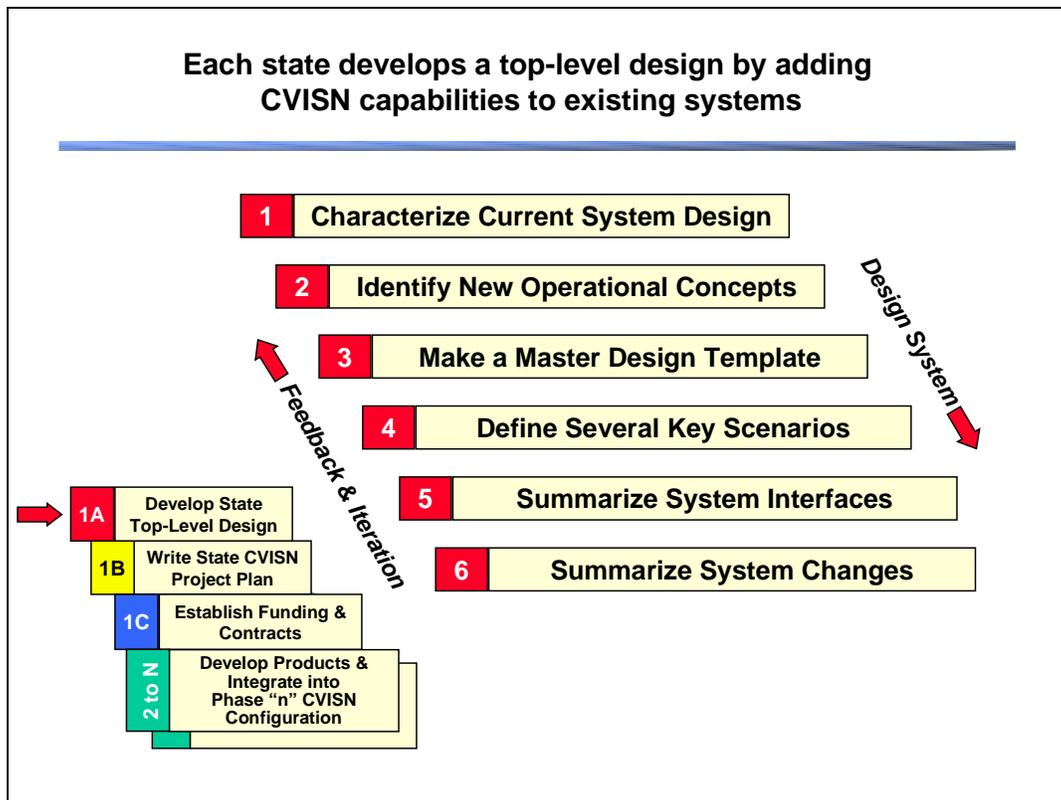
For example, if your state uses ASPEN and SAFETYNET today and plans to continue using them, you already have two key elements in place. If you assign US DOT numbers both interstate and intrastate carriers and use the generic CVIEW developed for other states, you can meet the CVISN Level 1 requirements with a relatively modest effort.

The approach defined herein assumes that your state is providing some level of system integration. If you decide to subcontract the role of system integrator, you may not follow the detailed steps outlined herein. Most likely, your system integrator will propose an approach based on their methodology. Nevertheless, the material herein can help you to understand what they must accomplish.

## 7.2 Top Level Design Phase

### Top-Level Design Phase Process

The CVISN Guide to Top Level Design (Reference 18) describes the general process for developing a top-level design. Figure 7-2 describing this process is repeated below as a reminder.



**Figure 7-2. Top-Level Design Process**

Even though the steps are shown as sequential, the process actually involves a great deal of feedback and iteration. Throughout the process, identify issues, actions and decisions. At the end of this process, your state will have decided what products it wants to develop or acquire, what modifications it wants to make to existing systems, and how it wants to interface systems to each other. This phase establishes the technical framework for everything that follows.

## Top-Level Design Phase Products

- A *State CVISN Top-level Design Description* that shows how safety information exchange fits into the statewide CVISN design. It should include:
  - System Requirements
    - State-specific goals
    - CVISN Operational and Architectural Compatibility Handbook (COACH) Part 1 tables from chapters 2, 3, 4, 5, 6
    - COACH Part 4 tables
    - Other state requirements
  - System Design
    - Allocation of requirements to system components
      - ▶ COACH Part 3 tables, tailored as needed
      - ▶ Description of functions for each new component
    - System Interface Summaries
    - Top-Level Physical System Design
  - System Change Summary
  - Operational Scenarios
  - Issues
- In addition to the State CVISN Top-level Design Description, your state may want to prepare a separate, more detailed specification for CVIEW and each other new system, if any.

## Factors to Consider in the Top-Level Design Phase

- The credentialing area of CVISN Level 1 focuses on interstate carriers in the IRP and IFTA programs. The safety area also includes intrastate carriers and vehicles. Designs must accommodate intrastate data. This is one of the primary reasons for having a CVIEW (or equivalent) in a state.
- As part of the system design process, the state needs to deliberately assess the expected transaction volume and what that implies for computer, storage, and networking needs. This assessment should be updated periodically as the project proceeds.

## Key Decisions

- Will the state implement a CVIEW (or equivalent) system?
- What functions will the CVIEW (or equivalent) system perform?
- Will the state build a CVIEW (or equivalent) from scratch or start with the generic FMCSA-developed model?
- Does the state use or intend to use ASPEN for inspections?
- Will CVIEW (or equivalent) act as the single snapshot and inspection report interface system for ASPEN units in the field?
- Will credentials snapshot inputs come directly from legacy systems and snapshot go to legacy systems? Or from/to the legacy systems via the Credentialing Interface? In EDI format or some custom interface format?

- What systems in the state will provide snapshot segment updates?
- Will the state assign USDOT numbers to intrastate carriers? If not, what identification scheme will be used?
- Will the state maintain intrastate snapshots?
- What snapshot views will be used where?
- Does the state need to add any state-specific fields to the snapshots to support their unique business rules? As an alternative, can the rules be changed to minimize system changes?
- How will requirements be specified?
- What communications services and protocols will be used to provide connections among the systems involved in safety information exchange?

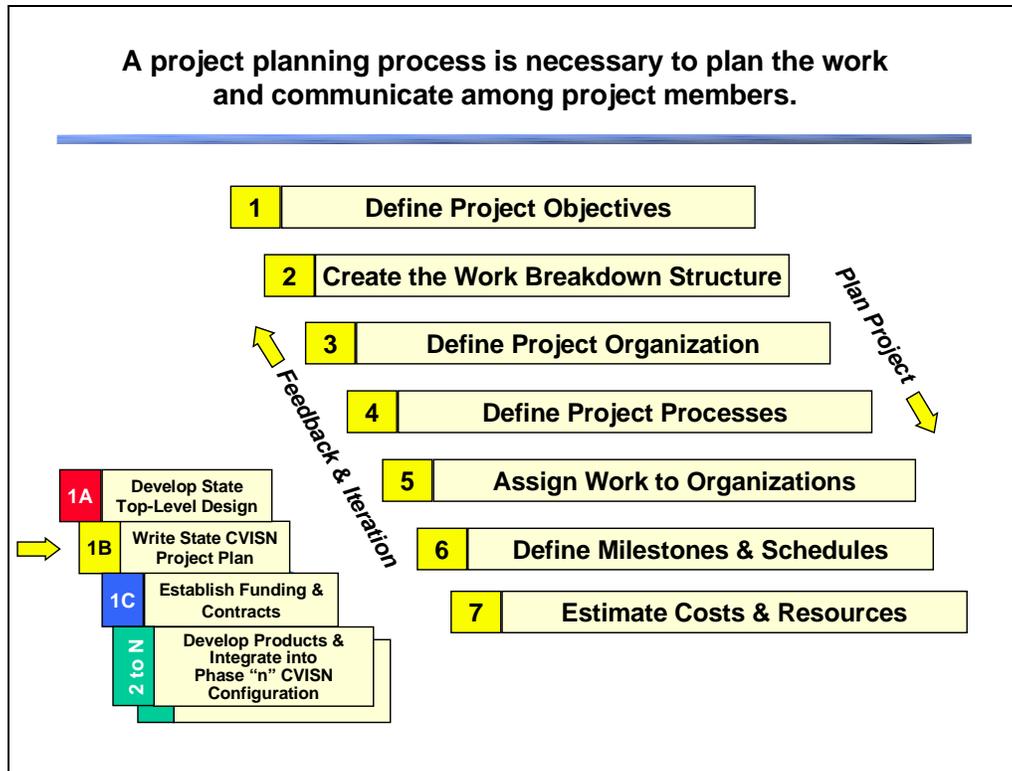
### **Advice and Lessons Learned**

- Develop requirements in multiple levels of detail. Use clear, concise top-level, testable, requirements as the basis for procurements and contracts. Develop more detailed business process descriptions as required by each phase as the work proceeds. (Please see section 7.6 Requirements Specification for more discussion.)
- The use of a CVIEW to serve as a single interface node within the state between sources of snapshots and users of snapshots has proven to be a useful approach. It allows a state to control and standardize interfaces among its internal systems. The state can isolate internal changes from external systems by developing custom legacy system interfaces (LSIs).

## 7.3 Program and Project Planning Phase

### Program and Project Planning Phase Process

The *CVISN Guide to Program and Project Planning* (Reference 40) describes the general process for developing a project plan and organizing the project. Figure 7-3 that portrays this process is repeated below as a reminder.



**Figure 7-3. Program and Project Planning Process**

### Planning Phase Products

- A completed plan that reflects the results of all the decisions made in this step. The top-level plan for safety information exchange should be reflected in the State CVISN Program Plan.
- Documents necessary to support acquisition of full project funding. The plan should support this, but other proposals and state-specific documents may be required.
- Preliminary Phase Schedule for safety information exchange systems and capabilities.

## Factors to be Considered in the Project Planning Phase

- What other projects are going on in your state that may impact the CVISN project. For several of the pilot states, Y2K efforts had such a high priority that resources were not available for CVISN tasks. Are there any major projects ongoing in your state that will compete for resources? Are major upgrades already taking place in the systems that support safety information exchange? Are major upgrades planned in the hardware and communications systems that will support the safety applications?
- If you are modifying existing systems in-house, will state staff be able to dedicate sufficient time to accomplish the modifications? Does this project have sufficient priority among all the on-going efforts? Does the management structure support the project?
- What policies does your state have on the use of the Web? Is there a program in your state to actively promote "electronic government" and deliver more services over the Web and the Internet? Can you leverage on these programs?
- What type of internal methodology has your state used in the past for information system development in the safety information exchange area? Is the process outlined in the CVISN guide series compatible with that approach? Are there any special requirements for feasibility studies or cost/benefit analysis studies?
- What is the typical procurement cycle in your state? What steps are required? How long does it take? What can be done to expedite this?
- What have other nearby states done towards implementing CVISN? Can you leverage what they have done, learn from them or partner with them in some way?

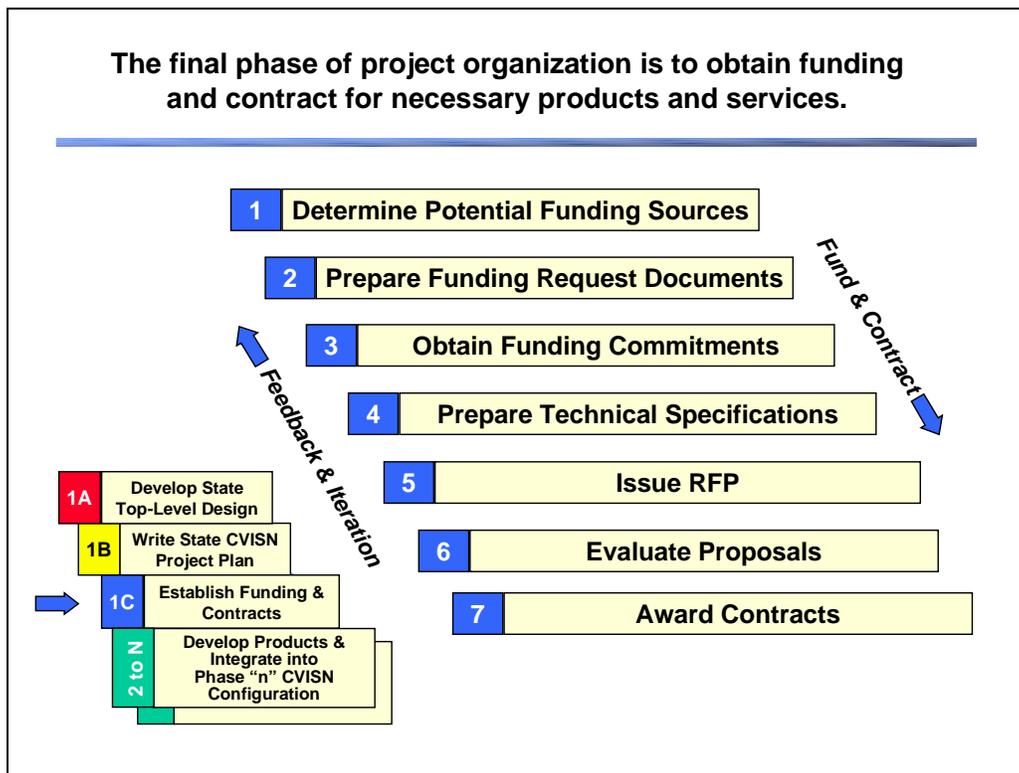
## Key Decisions

- Should the state build, buy, or use a government furnished item for each subsystem?
- Will the state update current legacy systems or re-compete/re-develop?
- When will the state connect to SAFER?
- Will the state participate in the Performance and Registration Information Systems Management (PRISM) program?
- What are the priorities and sequence for implementing capabilities?
- Who is the system integrator?
- Should the state use sole source or competitive contracting?

## 7.4 Funding and Contracts Phase

### Funding and Contracts Phase Process

The CVISN Guide to Program and Project Planning (Reference 40) describes the general process for the funding and contracting phase. Figure 7-4, which portrays this process, is repeated below as a reminder. The process for this phase is very dependent on state specific details. The figure is intended to give a conceptual framework and starting point. You should develop a specific process that meets the needs of your state.



**Figure 7-4. Funding and Contracts Phase Process**

## Funding and Contracts Phase Products

- Documents needed (public relations material, feasibility studies, cost/benefit studies, grant applications or proposals) to obtain funding
- Commitments for funding from state, federal and private sources on a schedule that meets project cash flow requirements.
- Procurement documents (e.g., request for proposal (RFP), evaluation plan, feasibility study, and sole source justification) to acquire hardware and software products as well as software development, system integration, communication, and verification and validation services.
- Flexible contract mechanisms are in place to support a team of contractors as required to complete all aspects of the project.

## Factors to be Considered in the Funding and Contracts Phase

- The safety information exchange area is usually the most straightforward of the CVISN capability areas. Many states already have ASPEN systems in place and these already interface to SAFER. Likewise, nearly all states use SAFETYNET. The FMCSA is already incorporating features in these systems to allow them to conform to the CVISN architecture. A generic version of CVIEW is available at nominal cost that can be used as a starting point (although customization and operations and maintenance support will be required.)
- The state needs contractual vehicles that allow work to be defined and costs estimated at a high level before all the details are known. The contractual mechanism must also have the flexibility to define detailed process and system design as the work proceeds.
- Be sure to include measurements of performance and remedies for non-performance in contracts.
- Be sure to account for operations and maintenance in the budget estimates.
- *If the state is pursuing a mostly custom development approach:* The requirements analysis approach is critical. The requirements will guide the activities of the contractors. Consider including a proof-of-concept phase in which the state can judge the contractor's commitment and ability to meet the technical and schedule requirements.
- *If the state is using mostly commercial-off-the-shelf (COTS) packages:* The requirements analysis approach is required, but not as critical as with custom development. Basically, you are buying what vendors already have. You want an opportunity to "try before you buy". Consider including a preliminary demonstration phase in your contract that allows your state personnel to see the basic (unmodified) package they are getting before making the final commitment to it.

## Key Decisions

- How much funding is required to complete the project?
- Where will the funding be obtained?
- What type of procurement should be used for each product or service?
- What can be done to expedite procurements?
- What type of incentives and remedial mechanisms should be included in the contracts?
- What terms and conditions related to software rights should be included in the contracts?
- How can the RFPs be written to assure architectural conformance and interoperability?

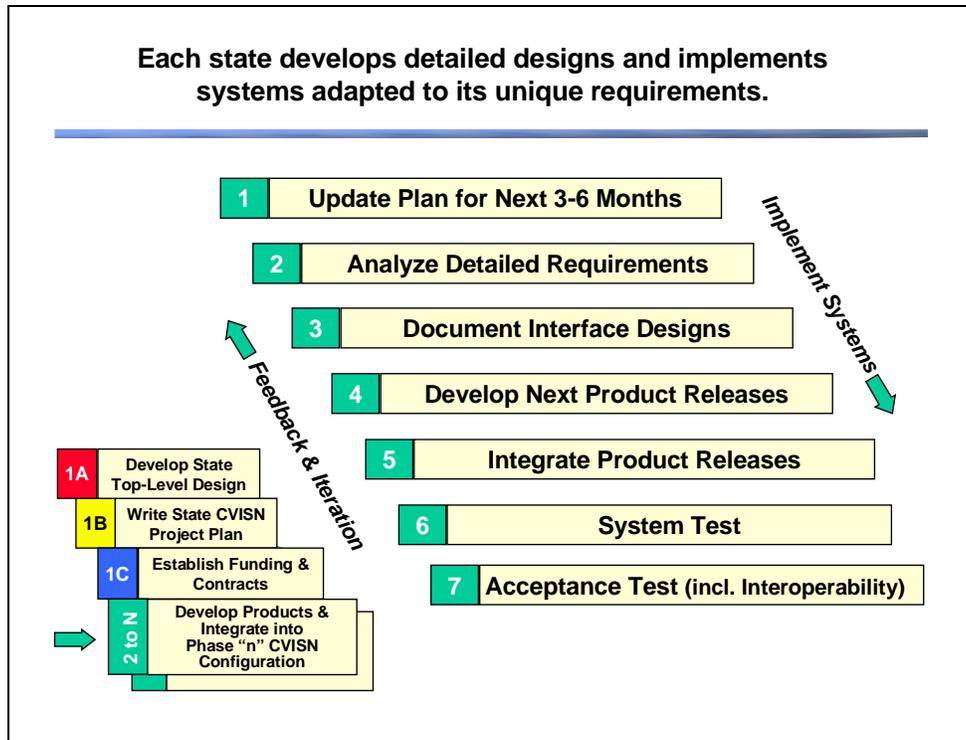
## Advice and Lessons Learned

- If possible, set up some type of indefinite delivery/indefinite quantity (ID/IQ) contract vehicle with your systems integration agent and software services vendors. This allows you to define specific task orders as the work proceeds. It lessens the need to have a "frozen" set of requirements up front. It allows the team a lot more flexibility in solving problems. It allows adapting to changes in technology as the project proceeds.
- To assure architecture conformance, be sure to require that vendors prove that their deliverables conform to the architecture through the execution and analysis of interoperability tests. Also require design reviews so that the state's Conformance Assessment Team can check the design for conformance.
- When states decide to do a mostly COTS approach, they expect the costs to be very small. This expectation is often not met. For example, if your state purchases an existing CVIEW, it is likely to require substantial modification and customization to fit in your environment. It may need custom legacy system interfaces. Your state may have slightly different processes than other states using the product. You may require additional data fields. The result is that the COTS product may still cost hundreds of thousands of dollars. Nevertheless, it is still cost effective because a development from scratch may cost millions of dollars.

## 7.5 Development Phase "n"

### Development Phase "n" Process

The CVISN Guide to Phase Planning and Tracking (Reference 41) describes the general process for developing and maintaining a Phase Plan and tracking progress as the phase proceeds. Figure 7-5, which portrays this process, is repeated below as a reminder.



**Figure 7-5. Development Phase "n" Process**

### Development Phase "n" Products

- Working products (e.g., ASPEN, CVIEW, LSIs, legacy modifications (LMs))
- Products integrated into the operational environment
- Test documentation showing proof that products worked as required
- Operation and maintenance documentation
- Net result: New operational capabilities

## Factors to be Considered in Development Phase "n"

- You need to be able to incrementally define details. Allow time in the schedule to define more scenarios and to document the state specific EDI interface requirements at the beginning of each phase. The state-specific EDI requirements should be published in a *State of \_\_\_ Motor Carrier Safety Information Exchange EDI Interface Control Document* that is made available on a state Web site.
- As components are developed, tests should be executed to verify that the components meet the design. As components are integrated, interoperability tests should be executed to verify that the standard interfaces were implemented correctly, and that the components and products work together correctly.
- Configuration management becomes very important when integrating products from multiple vendors. A change management process must be in place. As changes are made to interface designs, everyone must be kept informed of changes and planned updates. Updates to systems on each end of the interface must be synchronized. Version numbers must be systematically assigned to all products and version description documents prepared to coordinate updates and make sure that compatible versions are installed together.

## Key Decisions

- How should the initial design be modified based on the experience gained in each phase?
- How should the initial phase plan be modified based on progress actually made in each phase?

## Advice and Lessons Learned

- Incremental deliveries reduce the risk for both the state and the vendor. Use them.
- Assuming that you are doing incremental development, allow time at the beginning of each phase for a “mini-business process reengineering (BPR)” study of just the processes for that phase. For example, maybe the next step focuses on the vehicle snapshot delivery to the roadside. Allow a few days to define detailed processes. Also, refine the interface specifications at this time. Finalize any state specific details related to EDI interface maps (the software that converts legacy system data from or to EDI) at this time. This “just-in-time” analysis will present topics to the development team when they are ready to handle them and need the results. It will avoid “warehousing” a thick specification on a shelf to gather dust.
- An early delivery that shows tangible progress is critical to building the team, establishing forward momentum, establishing credibility, and securing funding. For example, Maryland deployed a number of ASPEN units and connected them to SAFER prior to having an operational CVIEW. This was a good first step because it established the critical SAFER interface and provided immediate benefit to the enforcement officers using the new ASPEN systems.

- Schedule management is especially important in the safety information exchange area because of the need to coordinate multiple vendors. The state needs an integrated schedule that has top level milestones and any external dependencies among the various vendors and organizations involved. The system architect needs to have clear authority to adjust the schedule details in response to technical issues. However, everyone must make a firm commitment to meet major milestones.
- The safety information exchange area will probably require close coordination among several parties including the state, the FMCSA and one or more vendors. All participants will be dependent on each other for achieving their goals. These external dependencies need to be identified and carefully managed. When problems come up (as they always will, even in the best programs) there will be a tendency for everyone to blame the problem on someone else. You need a strong system integrator and problem resolution process to deal with this.
- An early indicator of a vendor's ability to perform is to check the level of effort being applied. There is no substitute for a visit to the vendor's development facility. Ask to meet the people working on your system. Ask what other assignments they are working on. Step back and perform a "sanity check" on staffing levels. Ask yourself if it is realistic to expect the work you want with the effort that is being applied.
- Hopefully, careful planning will allow things to go well with your vendors. But be sure to have contractual remedies in place just in case they don't. These can include progress payments based on performance, incremental funding, and cancellation clauses.
- Test data can be time consuming to prepare. Build on existing test data (e.g., the CVISN interoperability test suite package) when possible. Lack of test data can cause insufficient test and allow problems to go undetected until systems are put into production.
- Changes in requirements can kill project schedules and cause cost overruns. An effective configuration management (CM) process is necessary to ensure that changes are only made when the impacts on cost and schedule are understood and approved. For more information about CM, please see Reference 31.

## 7.6 Requirements Specification

Development of accurate requirements specifications that are detailed enough (but not too detailed) is a critical success factor in a safety information exchange project. It is discussed here as a separate topic because it is a consideration that has impact on all phases of the development process, from top-level design through final acceptance testing. Several alternatives to specifying requirements are discussed below.

### **Alternative A: Simplified Requirements Specification Document.**

If your state is not experienced in using detailed requirements specifications effectively, a simplified approach may be a better choice. Consider not writing a very detailed safety information exchange requirements specification up-front. Some folks think that a thick, detailed requirements document will ensure that the contractor will produce what you want. Experience has shown that this is not necessarily the case. Instead, a concise requirements document that states the end results and leaves the details to be developed as part of the phased development process is more likely to succeed. Remember that your objective is to produce a top-level requirements specification that limits the project scope and is concise, testable, and provides a basis for establishing and managing a contract.

One suggested approach is to use your *State CVISN System Design Description* as the basic source of requirements for your safety information exchange subsystems. The design description should include the completed sections of the various parts of the COACH:

- COACH Part 1, Operational Concept and Top-Level Design Checklists
- COACH Part 3, Detailed System Checklists
- COACH Part 4, Interface Specification Checklists

Review and edit these, filling them out and customizing them as required to meet the needs of your state.

Your request for proposal (RFP) should refer to specific sections of the design description relevant to the item or items being procured. It can also reference these guides and any other state specific documentation (e.g., strategic plans) that provide background or describe your concept of operations. The RFP should require that the product pass the interoperability tests. Please see the COACH Part 5 (Reference 6) and the CVISN Interoperability Test Suite Package (References 19-21) for further information. The RFP should require that as part of the project, the vendor perform systems analysis and develop more detailed process descriptions and related requirements with operations personnel during each phase of the project. These process descriptions may be done in joint application development (JAD) sessions using participant flows or some equivalent method and diagramming technique. When evaluating proposals, pay particular attention to the vendors' experience and proposed approaches to working with your team to develop these detailed process designs.

## Alternative B: Delta Requirements

If your state is using a largely COTS approach, you may want to consider a variation on Alternative A. Do the simplified requirements specification based on your State System Design Description and COACH as described above. Then ask the contractor to install their COTS products for a trial period of 1-3 months. During this time, ask the contractor to develop a “delta” (i.e., difference) requirements specification that just describes what changes you want to make to their product. The contractor may use checklists, JAD sessions, focus groups, interviews and other techniques to collect these delta requirements.

Preparation of the delta requirements is in lieu of a detailed description of each scenario or business process. If you are basically satisfied with the process as it exists, there is no need to spend a lot of effort documenting it.

## Alternative C: Comprehensive Requirements Specification Document

Traditional software life cycle models advise having comprehensive, detailed, requirements nailed down before the project starts. Problems with this approach, include:

- Developing the document is costly and time consuming
- Processes change and the document quickly becomes obsolete
- If the people developing the document aren't the ones developing the system, much of the investment remains locked in the heads of the analysts who wrote the specs and is not transferred to the developers. The developers will likely want to redo this work themselves and get the users' perspective first hand.
- User personnel often don't have time to invest in really studying requirements documents and making sure the documents reflect their needs
- It is very difficult for user personnel to review the documents and actually understand what they are getting. When they finally see the system, they will realize that there were lots of things they wanted that didn't occur to them when reviewing the specs.

However, if your state has worked successfully with comprehensive, detailed requirements specifications before and this is what you want on this project, consider issuing a partial draft of the requirements specification as part of your RFP. Then have the successful bidder complete the draft as part of their contract, finalizing sections with each phase of the project as it proceeds.

In Maryland and Virginia, comprehensive Credentials Administration Requirements Specifications (CARS) (References 36 and 37) were prepared up front. These documents provided a description of how transactions flow end-to-end through all the systems supporting credentials administration. They also allocated requirements to each subsystem, legacy system interface and legacy modification and defined interfaces between those elements. Because the prototype states were the first to initiate the credentialing project, it was felt that a comprehensive document like the CARS was needed. In retrospect, the CARS documents provided a wealth of information and were useful to the projects. In particular, the participant flows (in CARS Chapter 3, Business Processes) were very useful for gaining an understanding of how the users wanted the final system to work. However, the more technical sections of the

CARS (Chapter 4, Systems Business Processes and Chapter 5, System Functional Requirements) were less useful and are not recommended for future efforts because of the time and cost of preparation.

## 8. SAFETY INFORMATION EXCHANGE IN THE CVISN MODEL DEPLOYMENT STATES

Several of the CVISN Model Deployment States provided information about how they are implementing safety information exchange functions (see subsequent sections in this chapter). This information is included in this section as written by the states, with minimal editing. All information is as of April 1999 unless otherwise noted. It is subject to change and is provided as background only.

### 8.1 California

Figure 8-1 shows the California CVISN System.

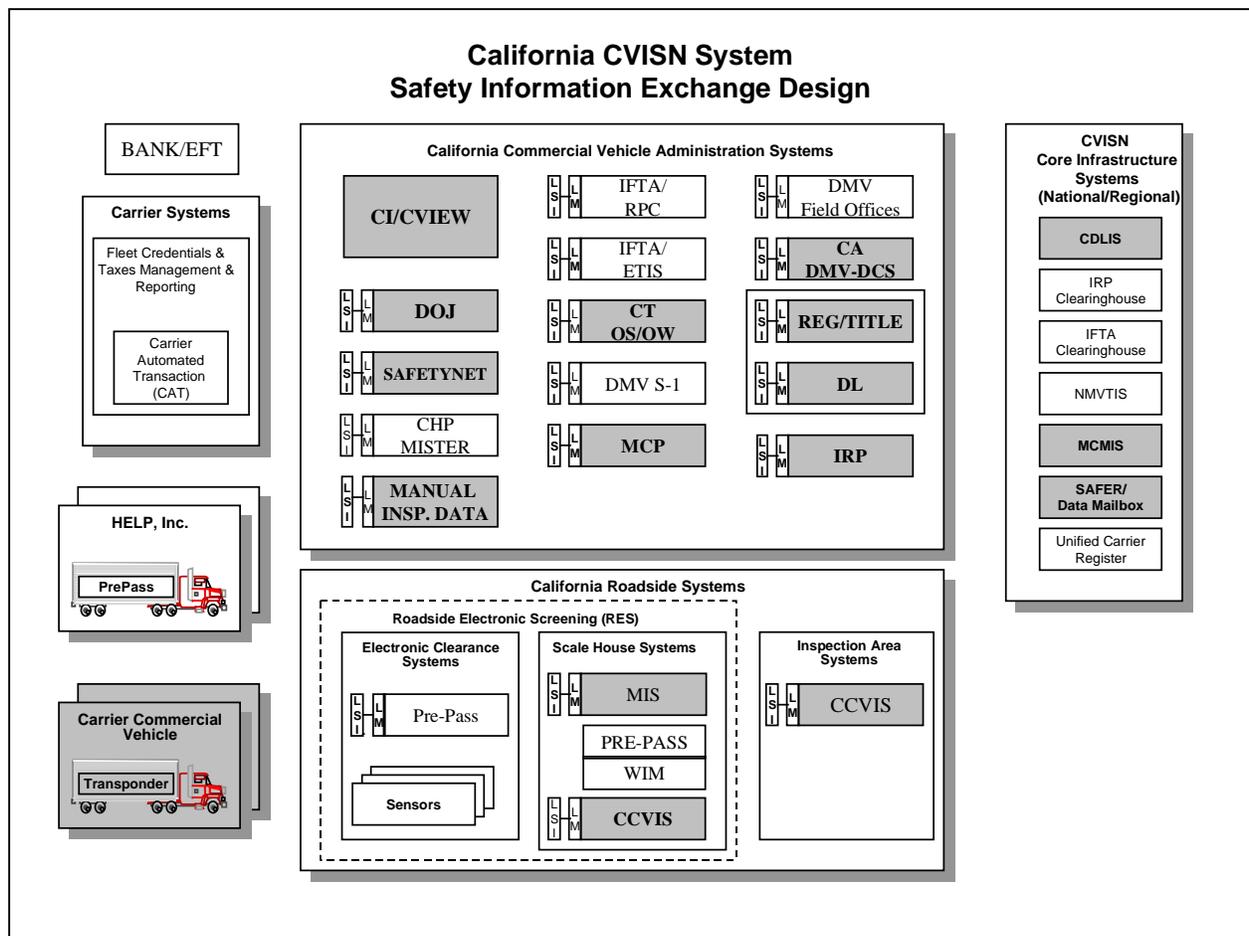


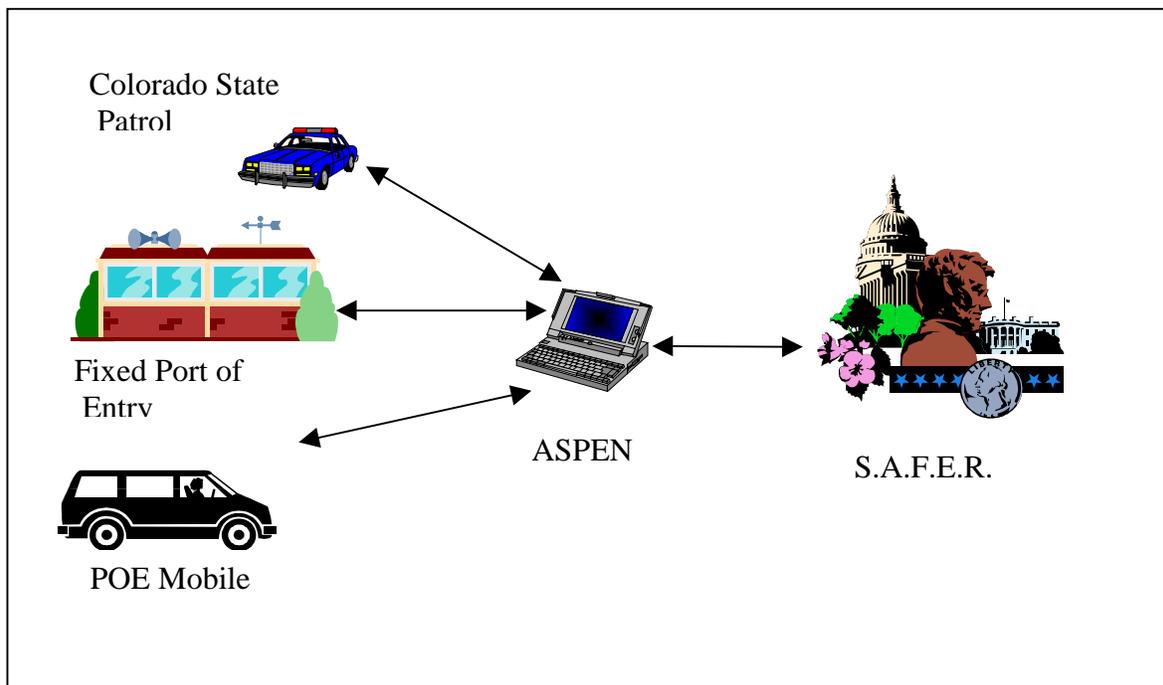
Figure 8-1. California CVISN System Design Template

Highlights of California Safety Information Exchange modifications and planned or existing capabilities include:

- Provided CCVIS (in lieu of ASPEN) computers to all 16 fixed inspection facilities throughout the state.
- Plan to conduct a pilot test in the fall of 1999, to utilize cellular communications to upload inspection data on a real time basis.
- Plan to provide laptops with the CCVIS software to mobile road enforcement officers, utilizing cellular communications.
- Plan to provide access to CVO legacy systems through CCVIS/MIS.
- Plan to provide state and SAFER snapshot data to CCVIS/MIS via CVIEW.
- Plan to upload inspection data to SAFER/SAFETYNET through a CVIEW interface.

## 8.2 Colorado

Colorado's safety efforts are currently focused on utilizing existing technology (See Figure 8-2). Laptop computers are being used by Colorado State Patrol's MCSAP units, the Port of Entry Mobile units and fixed Port of Entry sites. These 27 units are running the ASPEN software for entering inspections and doing Past Inspection Queries (PIQs). This data is sent and received from the Safety and Fitness Electronic Record (SAFER) system developed by the Johns Hopkins University's Applied Physics Laboratory.



**Figure 8-2. CO Safety Information Interfaces**

It is our intent to begin using the data generated by SAFER to "pre-screen" vehicles at every workstation within the state. This information will be used in determining which vehicles would be good candidates for an inspection. To do this, we are beginning to match Vehicle Identification Numbers (VIN) to USDOT numbers, which we can then associate with a safety rating. The SAFER score will be displayed on the POE Business System clearance screens used by the officers (see figure 8-3 below). These ratings will appear in **green** for vehicles that have what is considered a "good" rating, and in **red** for vehicles that have a "bad" rating, or if there is insufficient data to have a rating.

The screenshot displays a web-based form for vehicle clearance. On the left, three labels with arrows point to specific fields: 'Vehicle Id Number' points to the 'ID' field containing 'AB14035'; 'US DOT number' points to the 'VIN' field containing 'RW004740 AB14035'; and 'SAFER score' points to the 'SAFER' field, which is currently empty. The form includes various other fields such as 'DOT', 'GVW', 'Dy', 'OOS', 'Carrier', 'Owner', 'Street', 'City', 'State', 'Zip', 'Base State', 'License Plate', 'LVC', 'Truck Class', 'Registration', 'SSRS', 'Hazard', 'Hazmat Date', 'XGL', 'Fuel Type', 'IFTA Date', 'NM SCC', 'PRC', 'PUC Stamp', and 'Cab Card'. The 'Registration' and 'SSRS' fields are highlighted in red, while 'Hazmat Date' and 'SAFER' are highlighted in green. At the bottom, there are buttons for 'Done', 'Pat', 'Print', 'Refresh', and 'New'.

**Figure 8-3. CO POE Business System Clearance Screen**

Our web site can be found at:

**[www.state.co.us/gov\\_dir/revenue\\_dir/mcs\\_dir](http://www.state.co.us/gov_dir/revenue_dir/mcs_dir)**

### 8.3 Connecticut

No information was available from Connecticut at the time of publication of this document.

### 8.4 Kentucky

Figure 8-4 shows the Kentucky State CVISN System Design.

The following high-level system design template safety related functions targeted for inclusion in Kentucky’s CVISN deployment strategy. Additional information relating to CVISN and CVO activities can be found at <http://acvo.uky.edu> and <http://www.kytc.state.ky.us/motorcarrier/Motorcar.htm>.

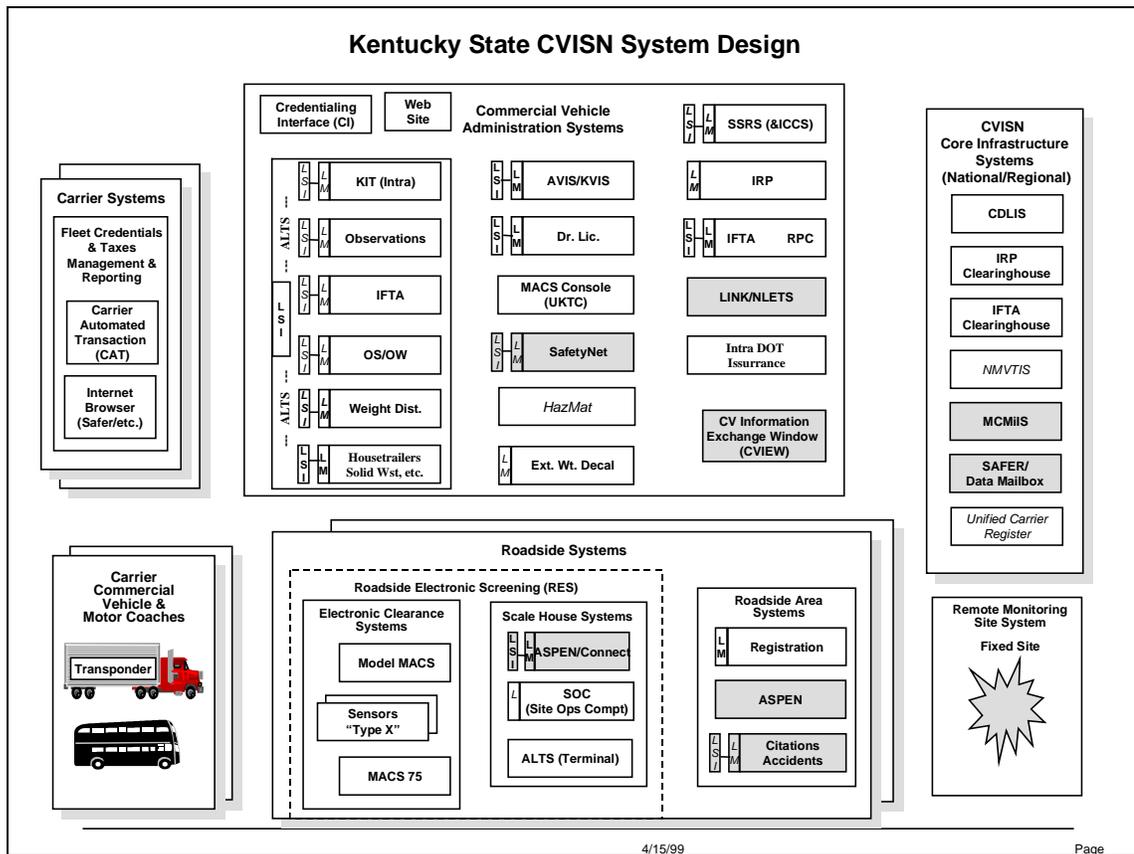


Figure 8-4. KY CVISN System Design Template

Safety regulation and the collection and exchange of the related information have been a long-term effort for Kentucky. Recent additions and enhancements in motor vehicle safety operations have taken place and are continuing as part of EMPOWER Kentucky – a re-engineering of various processes across the Commonwealth to improve services to the citizens.

As part of the re-engineering processes and of this CVISN project, Kentucky’s plans call for:

- ASPEN laptops for inspectors and officers
- Continued use of SAFETYNET 10/SAFETYNET 2000
- Use of CVIEW as a means of obtaining safety and credential data on carriers and vehicles
- Installation of Ethernet LAN’s and 56KB WAN’s in/to each weigh stations with available Ethernet hub ports to accommodate the easy networking of laptops
- Use of mobile communications by officers in their cruisers

### 8.5 Maryland

Figure 8-5 shows Maryland’s system design template, with the safety information exchange-related functions highlighted. More information about the MD CVISN project can be found at <http://www.mdot.state.md.us/mmcp/index.html>.

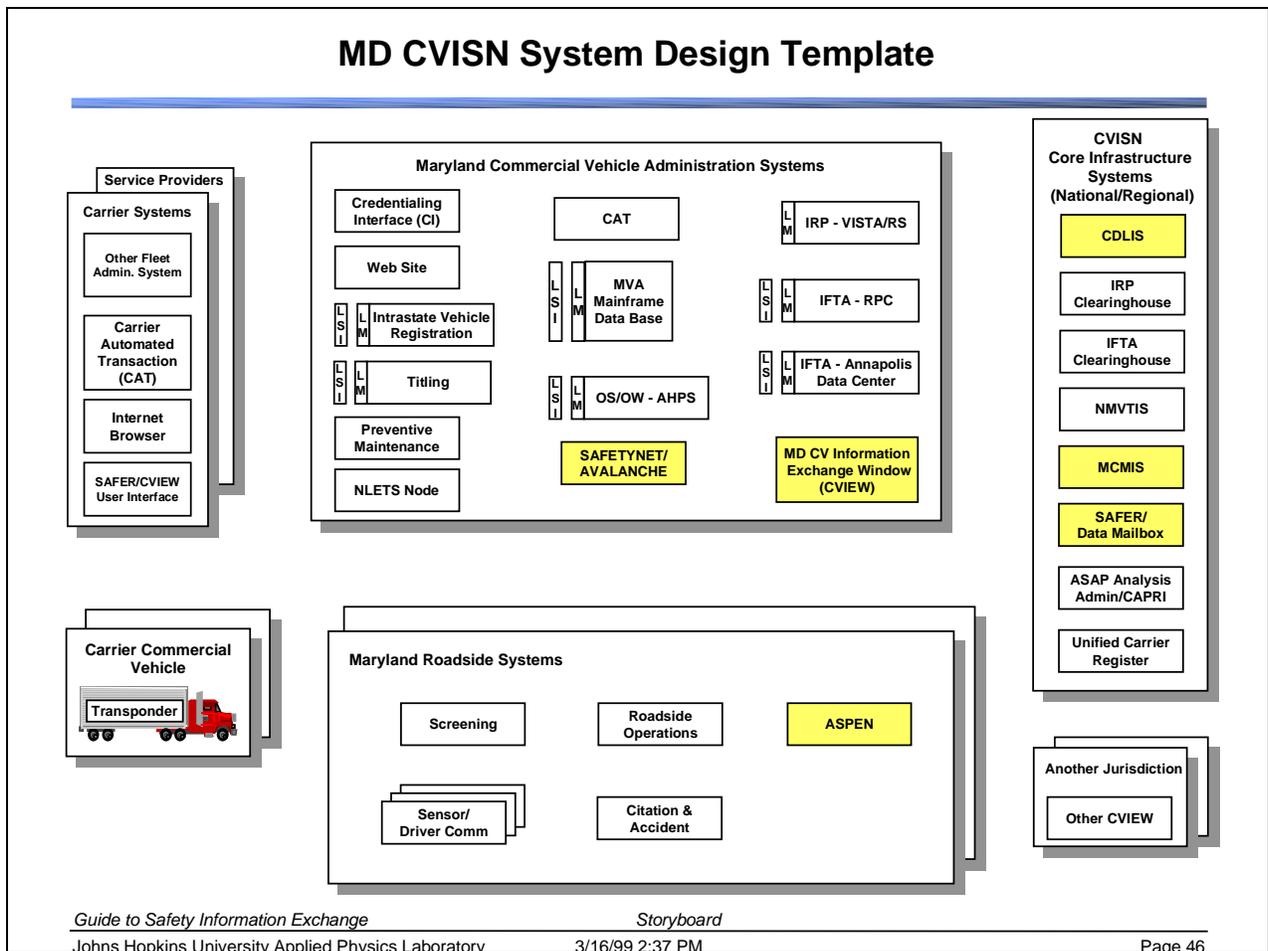


Figure 8-5. MD CVISN System Design Template

Highlights of Maryland's safety information exchange modifications and planned or existing capabilities MD include:

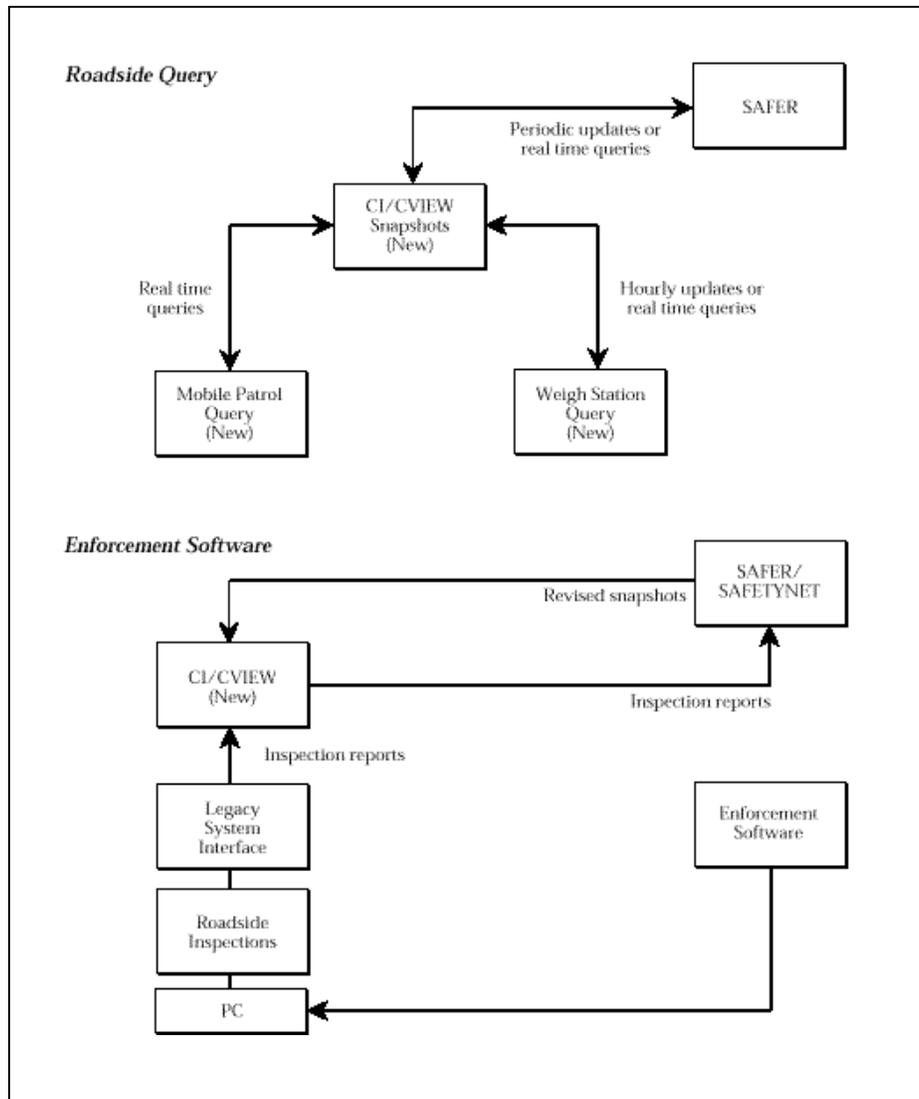
- Provided ASPEN laptops to all inspectors.
- Installed CVIEW; updating periodically as the product matures.
- Provided IRP data to CVIEW for snapshots via LSI.
- Added 2 Servers to support the CI, state office CATs, and CVIEW, with plans for two more to support operational mode

## 8.6 Michigan

The collection and dissemination of safety information about motor carriers – trucks and commercial buses – is a primary responsibility of the State Police and the Bus and Limousine unit of Michigan DOT. Safety enforcement at the roadside is the responsibility of the State Police.

In Michigan, the inspection data are gathered at the roadside by the State Police and MDOT (for commercial buses) using ASPEN software loaded on laptop computers. Outside the scope of the Michigan CVISN architecture, the State Police and the FMCSA conduct compliance reviews in the state, and police accident reports provide crash data on commercial vehicles. All of the above data are processed by SAFETYNET software, and sent electronically to MCMIS.

In Michigan, the current CVISN system architecture has an integrated CI/CVIEW sending inspection reports to and from SAFER and to SAFETYNET on a periodic basis. The CVIEW portion of the CI/CVIEW receives snapshot updates from SAFER and forwards these to users in the state such as weigh stations and mobile patrols. For intrastate carriers, as part of a process that does not include SAFER, the CI/CVIEW consolidates data and makes these data snapshots also available electronically to roadside locations. For safety data, the state's interaction with SAFER and SAFETYNET is shown in Figure 8-6. There are two components, roadside query and enforcement software.



**Figure 8-6. MI Interaction with Safety Systems**

- Roadside Query** – Weigh stations and mobile patrols will have on-line access to snapshots. Updates from SAFER will be transmitted to the CI/CVIEW for carrier, vehicle, and driver snapshots on a periodic basis, and CI/CVIEW will distribute the snapshots to the roadside locations. As previously noted, snapshot data will be delivered to weigh stations on an hourly basis and additionally in real time in cases of ad hoc query requests from facility personnel. For mobile patrols, the CI/CVIEW will deliver snapshots in real time in response to requests from the field.

- **Enforcement Software** – Enforcement software is used at the roadside to record inspection data. The data will be sent by modem or diskette to the deskside database. From the roadside inspections legacy system, through the legacy system interface, the inspection reports will be transferred to the CI/CVIEW, which will distribute the reports to SAFETYNET and SAFER. SAFER will use the information to update snapshots as needed, and distribute revised snapshots from all jurisdictions to CI/CVIEW for distribution within the state.

SAFER also includes credentials, insurance, and other data as well as safety data in the snapshots. On-line access to these data will facilitate roadside electronic screening, credentials checking by mobile assets, and industry self-checks.

For credential registration information, the following process generally applies:

- **Credentials** – SAFER will provide updated snapshots to the CI/CVIEW as a result of periodic or real time queries from CI/CVIEW. A real time query will be initiated by a deskside legacy system or a roadside query. On a periodic basis, the CI/CVIEW will transmit information to update SAFER. This information will come from CVISN legacy systems that transfer credentials information on a nightly basis to update the snapshots on the CI/CVIEW.

## 8.7 Minnesota

Figure 8-7 summarizes the system interactions in Minnesota’s safety information exchange design.

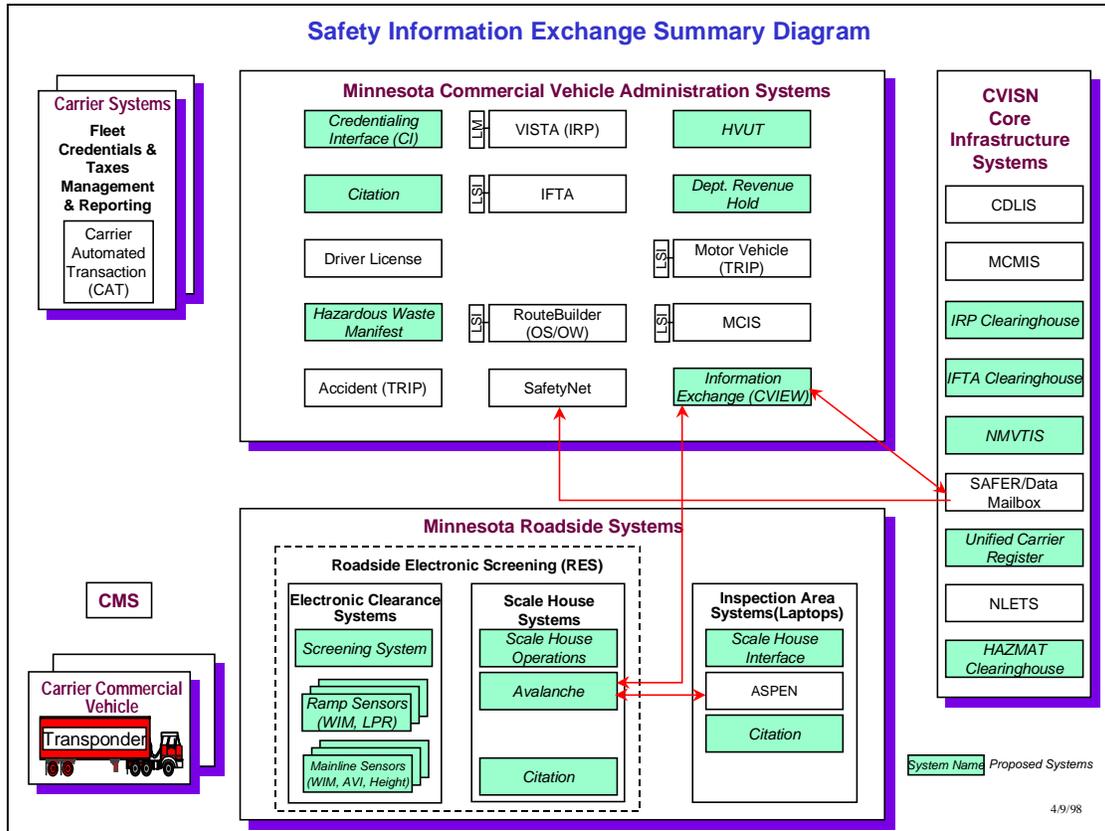


Figure 8-7. MN Safety Information Exchange

Highlights of Minnesota’s safety information exchange include:

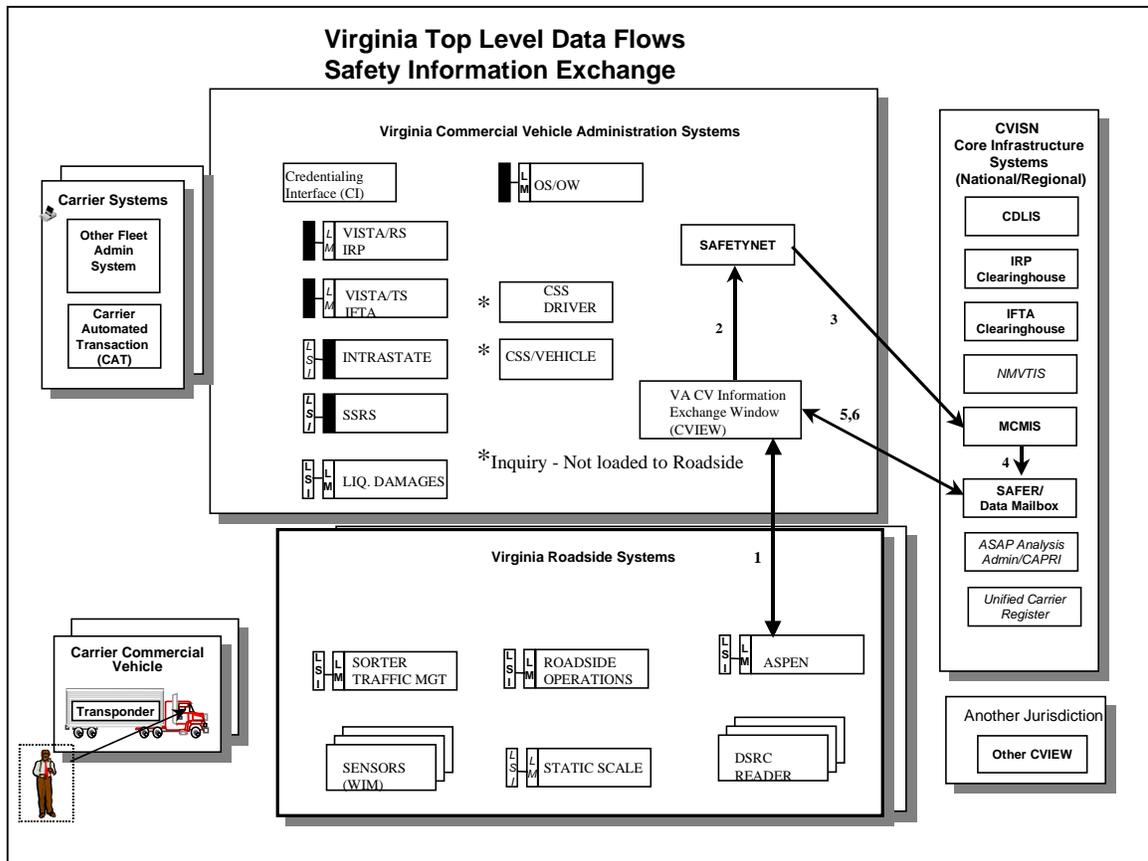
- Inspection data collected by ASPEN units will be transferred to the state’s CVIEW which will then relay data to SAFER and to the state’s SAFETYNET installation via the SAFER Data Mailbox.

## 8.8 Oregon

No information was available from Oregon at the time of publication of this document.

## 8.9 Virginia

Figure 8-8 shows Virginia's Top Level Data Flow for Safety Information Exchange.



**Figure 8-8. VA Safety Information Exchange**

Highlights of Virginia's safety information exchange current and planned capabilities include:

- Equipped 48 Motor Carrier Safety Troopers with ASPEN pen based computers and portable printers.
- Eliminated need for two data entry personnel. Inspections now entered in two weeks whereas the old paper forms averaged two months before entry.
- Installed desktop computer at Stephens City weigh station (I81) with direct access to SAFER. Provides capability to download Carrier safety inspection data. Similar capability planned for Dumfries weigh station (I95).
- Participated in SAFER Data Mailbox project to use laptops with CDPD communications; provides capability to do real time inquiry at the roadside. Purchased three laptops; currently awaiting software & hardware upgrades for CDPD capability.
- Awaiting installation of ASPEN ver1.5. Will enable use of modems to allow Trooper direct upload capability to SAFETYNET via SAFER. Will require 2-3 months to install and train all Troopers on the new ASPEN software.

- Require purchase of new laptops to replace pen-based units. Future ASPEN software requires 32-bit operating system which will not function on older units.

### 8.10 Washington

Figure 8-9 shows Washington’s inspection interfaces.

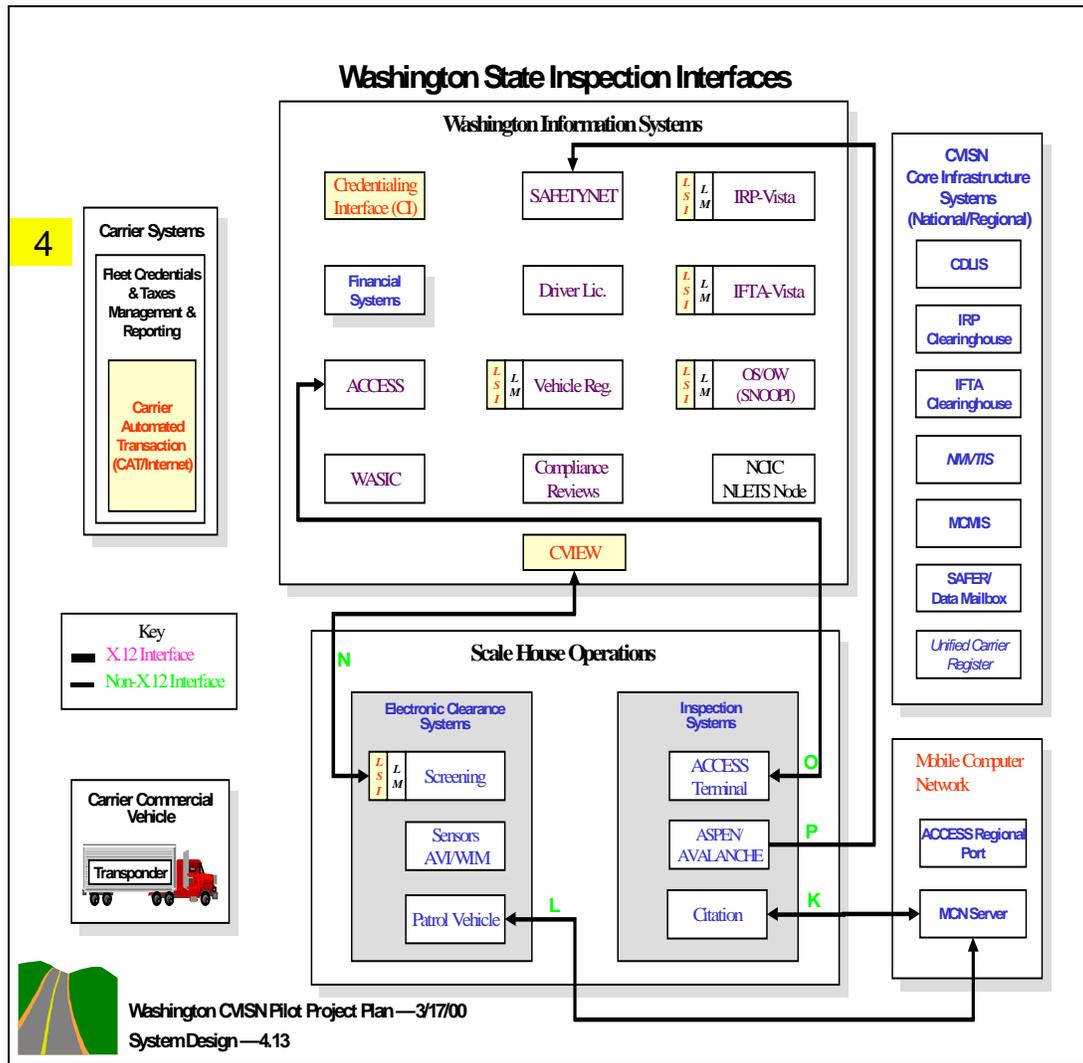


Figure 8-9. WA Inspection Interfaces

Washington used:  
 Microsoft NT Server  
 Windows Based Applications  
 in VB6 and C++6  
 MS SQL Database

More information about the WA CVISN project can be found at <ftp.CVISN.WSDOT.WA.Gov>

Please note: this is a secured site and you will need a user id and password for access. Call Anne Cline, CVISN Project Coordinator, at (360) 705-7341 for a user id and password.

Highlights of Washington's safety information exchange modifications and planned or existing capabilities include:

- Provided ASPEN laptops to all inspectors
- Established mailbox at SAFER
- Installed safety information on Screening Server at WSDOT headquarters

## 9. INTEROPERABILITY ISSUES/STATUS

The interoperability issues related to Safety Information Exchange are concentrated on the ability to exchange safety information and relate it to other information. Different legacy systems typically use different identifiers as look-up keys. The white paper on standard identifiers (Reference 13) provides detailed guidance on establishing a workable approach.

### 9.1 Issues

1. How will safety-related identifiers be cross-referenced to credentials-related identifiers?

First, an assessment of interstate carrier identifiers: For safety purposes, the United States Department of Transportation (USDOT) number is the main identifier (ID). For the International Fuel Tax Agreement (IFTA), the taxpayer ID is the main identifier. For the International Registration Plan (IRP), the IRP account number is used. The MCS-150 form captures many key identifiers (USDOT number, motor carrier operating authority number issued by the FMCSA or Interstate Commerce Commission, Dun & Bradstreet business number, taxpayer identifier) for carriers. Data from the MCS-150 are entered into the Motor Carrier Management Information System (MCMIS) database. The data from MCMIS is entered into the Safety and Fitness Electronic Records (SAFER) snapshot database. However, at this time, there is no requirement to keep that part of the MCMIS database up to date.

Under the Performance and Registration Information Systems Management (PRISM) processes, each vehicle must be associated with a safety carrier (using USDOT number to identify the carrier). The carrier's safety record is checked when the vehicle is registered. This provides an annual opportunity to confirm the carrier ID associated with each vehicle, and hence, to tie safety and IRP data together.

IFTA registration allows, but does not usually require that the USDOT be captured. If applicants routinely supplied the USDOT number, then a linkage between safety and IFTA data could be established.

Cross-referencing credentials and safety data will require a concerted effort. Linking the data together provides a better opportunity to identify high-risk operators.

2. Systems that were specified to handle interstate data should be evaluated to verify that they can also handle intrastate data.

Inspections are conducted on both intrastate and interstate operators. A copy of each inspection report, whether intrastate or interstate will be held in SAFER to facilitate access. To report and access intrastate inspections, the systems involved (ASPEN, CVIEW, SAFER, SAFETYNET) must be able to handle the identifiers used by the states for intrastate carriers. At this point in time, intrastate carriers are not required to have USDOT numbers, so that means that state-specific identifiers will be used.

## 9.2 Interoperability Tests

Interoperability tests for safety information exchange functions are being defined according to the criteria in the *CVISN Operational and Architectural Compatibility Handbook (COACH) Part 5, Interoperability Test Criteria* (Reference 6). The *CVISN Interoperability Test Suite Package* (References 19-21) explains the test scenarios, cases, procedures, and data. The tests are divided into two categories: those that test the interaction between pairs of products (pairwise tests) and those that verify a more complete functional thread (end-to-end tests). A complete list of tests planned for development that are related to credentials functions will be published as part of the next version of the Interoperability Testing Strategy (Reference 33).

## 10. LESSONS LEARNED – SAFETY INFORMATION EXCHANGE

This chapter contains “Lessons Learned” in the area of Safety Information Exchange. Specifically, the states were asked to respond to the following questions:

- What you did right that you'd recommend to other states.
- What you didn't do that you wish you had.
- What issues you wish you could have settled earlier.
- What requirements turned out to be key drivers for design.
- What design choices you considered and rejected/chose and why, etc.

### 10.1 Lessons Learned – California

#### **What you did right that you'd recommend some other state repeat?**

- Agreed to the concept that CVISN required a multi-agency and industry effort.
- Approved over 100 carriers who volunteered to participate in this demonstration project either directly, through agents, or through leasing companies.

#### **What you didn't do that you wish you had?**

- Seek federal funding through earmarks for funds committed.
- Evaluate, in detail, the availability and functionality of core infrastructure systems.
- State teams attending the workshops should demand significant break out sessions for open state interaction.
- Be concerned about lack of qualified vendors to support CVISN development.

#### **What issues you wish you could have settled earlier?**

- Finalize and encumber all federal funds early in the project, rather than on a year-by-year basis.
- Reduce the gap time between planning workshops.

#### **What requirements turned out to be the key drivers for design?**

- Development of the interfaces to all legacy systems in their native mode rather than EDI.
- Combining the CI/CVIEW functionality into a single computer platform.

#### **What design choices you considered and rejected/chose and why, etc.?**

- Rejection of a separate CI and CVIEW to minimize maintenance of test and operational systems.
- Choosing to produce final documents versus temporary documents as requested by the industry.

## 10.2 Lessons Learned – Colorado

- Colorado has long been involved in the MCSAP program. Cooperation between the State Patrol, the Port of Entry, and local police entities has resulted in identifying and removing unsafe commercial vehicles from the traffic flow.
- It was a "quick hit" to arm these officers with the tools necessary for them to become more productive in their jobs. It was easy to issue laptops with the ASPEN programs on them, get e-mail addresses for these officers, and subscribe to a SAFER mailbox. The end results are that both locally and nationally the results of these inspections are known in a near real-time fashion. That assists the "safe" companies, in that they are not continually stopped for inspections, and it assists the citizens by insuring that unsafe vehicles are either fixed or are put out-of-service.
- One of the things we haven't done is to fully populate our database in the fixed locations before we disseminated it. If we had associated VIN numbers to USDOT numbers from our IRP system to the PRISM system, we could then have assigned the SAFER scores. This would have eased the burden on our officers who have to collect the USDOT number from vehicles that they encounter.

## 10.3 Lessons Learned – Connecticut

No information was available from Connecticut at the time of publication of this document.

## 10.4 Lessons Learned – Kentucky

- Safety data may be several months old and unsatisfactory for use
- Citations, OOS, and credential information must be transmitted/received immediately to be effective.

## 10.5 Lessons Learned – Maryland

The lessons learned in Maryland have been incorporated throughout this document.

## 10.6 Lessons Learned – Michigan

In summary, Michigan has found that proper staffing and a strong commitment at the very beginning can avoid many pitfalls and lead to a much smoother project.

## 10.7 Lessons Learned – Minnesota

No information was available from Minnesota at the time of publication of this document.

## 10.8 Lessons Learned – Oregon

No information was available from Oregon at the time of publication of this document.

## 10.9 Lessons Learned – Virginia

### What went right:

- Employed enforcement personnel with computer knowledge to test equipment prior to deployment.
- Trained enforcement personnel with knowledgeable peers using a tiered approach.
- Timed purchase of ASPEN hardware to obtain best hardware available thereby maximizing useable life.

### What we didn't do, but should have:

- Purchased laptop in lieu of pen based ASPEN computers.

### What requirements were key drivers for design:

- Requirement for a state CVIEW.

## 10.10 Lessons Learned – Washington

- On screening software, an Enforcement Officer can enter an OOS inspection or correct an OOS inspection.

This Page Intentionally Blank

# APPENDIX A. REFERENCES

Note that not all of these references are explicitly cited in the text of this guide.

1. JHU/APL, *ITS/CVO CVISN Glossary*, POR-96-6997 V1.0, dated September 1998.
2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 - Operational Concept and Top-Level Design Checklists*, SSD/PL-99-0243, POR-97-7067 V 1.0, dated March 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
3. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 - Project Management Checklists*, Preliminary Version originally published in March 1997. Note: This document is scheduled to be updated in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
4. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 - Detailed System Checklists*, to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
5. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 - Interface Specification Checklists*, to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
6. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 - Interoperability Test Criteria*, SSD/PL-98-0399, POR-98-7126, D.0, dated June 1998. Note: This document is scheduled to be updated in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
7. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V1.0, March 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
8. JHU/APL, *Introductory Guide to CVISN*, POR-99-7186 to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
9. JHU/APL, *CVISN Guide to Credentials Administration*, POR-99-7192 to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
10. JHU/APL, *CVISN Guide to Electronic Screening*, POR-99-7193 to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
11. JHU/APL, *Safety and Fitness Electronic Records System (SAFER) and Commercial Vehicle Information Exchange Window (CVIEW), Carrier, Vehicle, and Driver Snapshots*, White Paper, to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
12. FMCSA, *PRISM Overview*, published on the World Wide Web at <http://www.mcs.dot.gov/factsfigs/prism.htm>.

13. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Recommendations for Primary Identifiers*. Note: This document is scheduled to be published in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>
14. ANSI ASC X12, *Electronic Data Interchange X12 Standards*, Draft Version 4, Release 2, (a.k.a. Release 4020), December 1998.
15. JHU/APL, *EDI Implementation Guide for Commercial Vehicle Safety and Credentials Information Exchange (Transaction Set 285)*, POR-96-6995 D.3, dated August 1998. Note: This document is scheduled to be updated in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
16. The U. S. Department of Transportation, *Interim Guidance on Conformity with the National ITS Architecture and Standards*, October 1998, available on the World Wide Web at <http://www.its.dot.gov/aconform/iguide.htm>. Updates via rulemaking are expected in late 1999.
17. A draft version of the Conformance Assurance Process Description is found on the World Wide Web at the TEA-21 Architecture & Standards Conformity page, <http://www.its.dot.gov/aconform/rg-toc.htm> by selecting ITS and Commercial Vehicle Operations. The title of the draft document is ITS/CVO Architecture Utilization Policy Implementation Tool.
18. JHU/APL, *CVISN Guide to Top-Level Design*, POR-99-7187 to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
19. JHU/APL, *CVISN Interoperability Test Suite Package, Part 1 - Test Specifications*, Draft, POR-98-7122 D.0, dated June 1998. Note: This document is scheduled for a significant update in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
20. JHU/APL, *CVISN Interoperability Test Suite Package, Part 2 - Test Cases and Procedures*, Draft, POR-98-7123 D.0, dated June 1998. Note: This document is scheduled for a significant update in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
21. JHU/APL, *CVISN Interoperability Test Suite Package, Part 4 - Test Data, Draft*, POR-98-7125 D.0, dated June 1998. Note: This document is scheduled for a significant update in 1999. The latest version will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
22. JHU/APL, *The Maryland Commercial Vehicle Information Systems and Networks (CVISN) Prototype System Design Description*, POR-96-6991, V.1, November 1997.
23. Intelligent Transportation Society of America, *ITS CVO Guiding Principles*, published on the World Wide Web at <http://www.itsa.org>, last updated March 27, 1998.
24. Intelligent Transportation Society of America, *Fair Information Principles for ITS/CVO*, published on the World Wide Web at <http://www.itsa.org>, last updated January 12, 1999.

25. Intelligent Transportation Society of America, *Interim ITS/CVO Interoperability Guiding Principles*, published on the World Wide Web at <http://www.itsa.org>, last updated January 12, 1999.
26. JHU/APL, *Introduction to ITS/CVO Training Material*, version 2.1, February 1999. The participant's manual is available from the Electronic Document Library at <http://www.its.dot.gov/welcome.htm>. Search for document number 8103.
27. JHU/APL, *Understanding ITS/CVO Technology Applications Training Material*, version 2.0, January 1999. The student's manual is available from the Electronic Document Library at <http://www.its.dot.gov/welcome.htm>. Search for document number 8143.
28. ASC X12D/W456, *ASC X12 Guideline for Electronic Data Interchange, EDI Implementation Reference Manual Guidelines*, Data Interchange Standards Association (DISA), February 1991.
29. Data Interchange Standards Association (DISA) Home Page: <http://www.disa.org/> - (DISA Reference Desk, Product Catalog, Internet Services).
30. JHU/APL, *Scope Workshop Notebook*, to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
31. ANSI/IEEE Std 1042-1987 (R1993), *An American National Standard IEEE Guide to Software Configuration Management*, 1988.
32. JHU/APL, *CVISN Guide to Integration and Test*, POR-99-7194 to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
33. JHU/APL, *ITS/CVO Architecture Conformance: Interoperability Testing Strategy*, update to be published in 1999. The document will be available on the JHU/APL CVISN Web site <http://www.jhuapl.edu/cvo/>.
34. Carol Gore, Federal Motor Carrier Safety Administration (FMCSA) - Field Systems Group (FSG) in Lakewood, CO, <http://www.inspector.org/fhwafsg1.htm>, a site maintained by the International Inspector's Competition.
35. JHU/APL, *SAFER-CVIEW Application Programming Interface for Win32 (SCAPI32)*. Available from Alan Mick, (240) 228-7386.
36. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), State of Maryland, Credentials Administration Requirements Specifications (CARS), SSD/PL-96-0613, Draft Issue D.1, dated November 1997*.
37. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), Commonwealth of Virginia, Credentials Administration Requirements Specifications (CARS), SSD/PL-98-0485, Version 2.0, dated September 1998*.
38. JHU/APL, *SAFER and CVIEW Carrier, Vehicle, and Driver Snapshots White Paper*, SSD/PL-99-0387, dated December 1999, posted on the CVISN Web Site at <http://www.jhuapl.edu/cvisn/downdocs/index.html#post-scope>

39. *JHU/APL, SAFER Interface Control Document , SSD/PL-99-0361, dated June 1999*
40. *CVISN Guide to Program and Project Planning, POR-99-7188, P.1, dated September 1999*
41. *CVISN Guide to Phase Planning and Tracking, POR-99-7189, to be published January 2000*

This Page Intentionally Blank

**APPENDIX B.**

**PRISM AND CVISN –**

**EXPLAINING THE RELATIONSHIP**

## PRISM and CVISN: *Explaining the Relationship*

### PRISM and CVISN share key concepts:

- focus safety enforcement on high risk operators
- use open standards for data communications
- use standardized algorithm for determining a carrier's safety fitness
- use data exchange systems, e.g. SAFER that conform with the National ITS Architecture

These concepts, implemented through state and national systems, link CVISN deployment and PRISM Program activities.

**PRISM (Performance and Registration Information Systems Management)** - A FMCSA-sponsored program that seeks to improve safety by linking vehicle registration actions to an evaluation of the related carrier's safety rating. The program includes procedures for a carrier to improve their safety rating.

**PRISM** is a comprehensive program of motor carrier safety assessment, enforcement and improvement. The core concept of PRISM is the linking of vehicle registration at the State level to acceptable carrier safety performance. Through the PRISM program, the safety performance of the carrier responsible for a vehicle being registered is considered at vehicle registration time. As a part of vehicle registration, participating States assure that the carrier is registered and meets the required safety criteria. Ultimately, subject to State laws, vehicle registration may be denied to unsafe carriers. As part of this process, the USDOT number of the carrier is recorded as part of the vehicle registration electronic record, thus linking the vehicle to the carrier responsible for the safe operation of the vehicle. That linkage can also be used at the roadside during screening operations and inspections. Six states (CO, IN, IA, MN, OR, and PA) currently participate in the PRISM program. Other states have been approved to participate.

The other major process in PRISM is the **MCSIP (The Motor Carrier Safety Improvement Program)**. MCSIP tracks carrier safety improvement through a series of levels intended to bring the carrier into full safety compliance. The MCSIP level is a crucial measure of a carrier's current status in this improvement process.

The safety assessment algorithm at the core of PRISM is **SafeStat**. From a comprehensive array of MCMIS carrier performance data (inspections, crashes, reviews, enforcement cases, citations) SafeStat computes a indicator and category for carriers that have sufficient data. The SafeStat indicator and category can be used to prioritize carriers for a possible on-site review. The SafeStat values are also available at the roadside for use in screening algorithms.

**CVISN (Commercial Vehicle Information Systems and Networks)** - The information systems and communications networks that support commercial vehicle operations. CVISN includes information systems owned and operated by governments, carriers, and other stakeholders. It excludes the sensor and control elements of ITS/CVO.

The **CVISN Architecture** provides a standardized framework for linking new and existing systems and networks to facilitate the exchange of information. The CVISN Prototype & Pilot states are deploying **CVISN Level 1 capabilities**: safety information exchange through snapshots, inspection reporting using ASPEN, electronic screening using transponders and snapshot data, electronic credentialing for IRP and IFTA, and supporting base state agreements via the IRP and IFTA Clearinghouses. Ten states (CA, CO, CT, KY, MD, MI, MN, OR, VA, and WA) are currently deploying CVISN Level 1 capabilities.

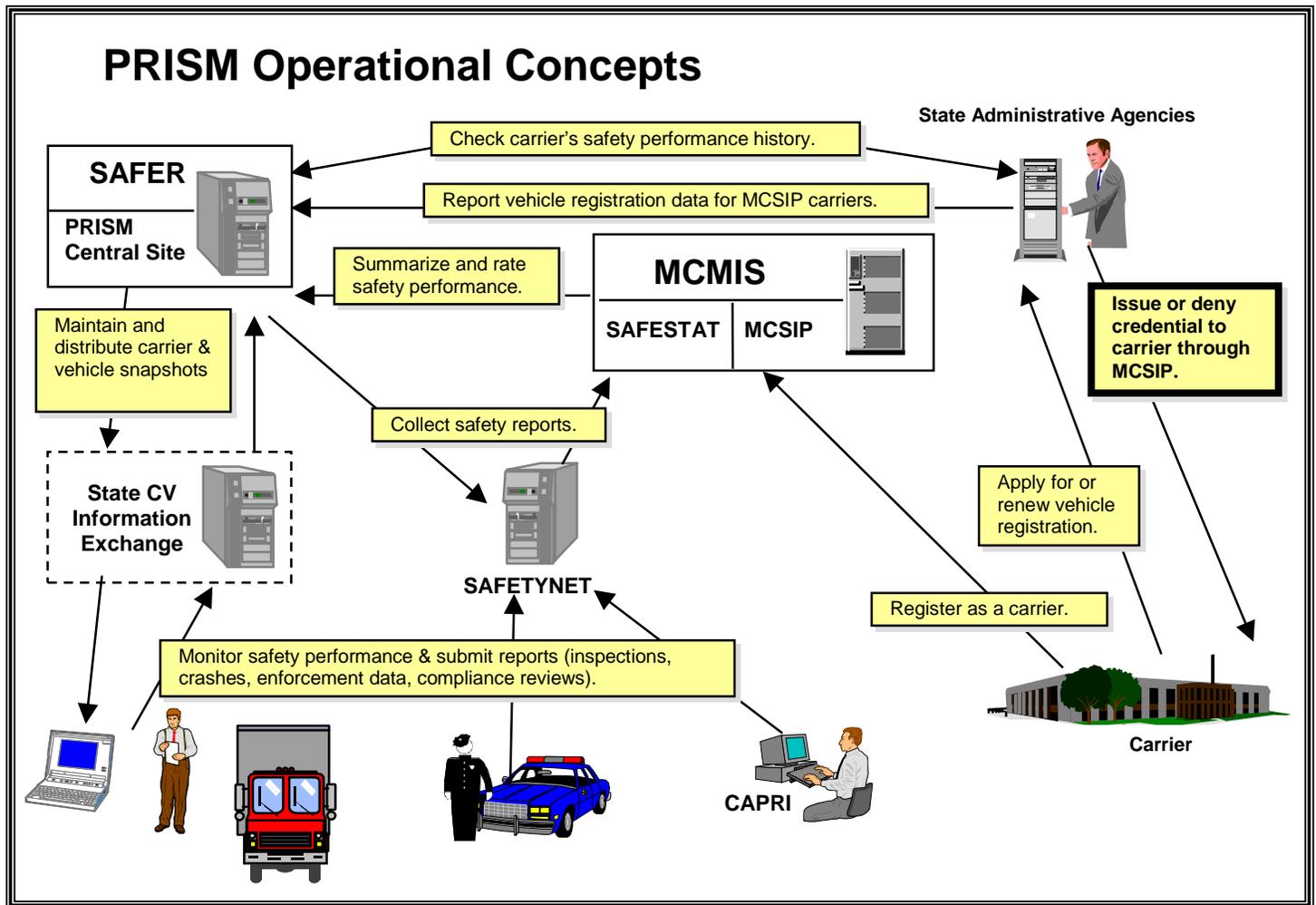
### ***HOW ARE PRISM AND CVISN RELATED?***

Access to safety information is necessary to support the safety performance evaluations that serve as a basis for accomplishing PRISM program goals. Information systems and networks that are part of the CVISN Architecture provide that access.

- To facilitate information exchange, several systems are being developed under CVISN. One of those systems is **SAFER (Safety and Fitness Electronic Records)**. SAFER and other information systems (e.g., SAFETYNET, MCMIS, ASPEN, CAPRI) are used to supply data for the PRISM processes.
- The values generated by PRISM's SafeStat algorithm are included in SAFER snapshots. Snapshots are used in roadside screening and inspection activities to focus resources on high-risk operators.

*Thus, the PRISM system concepts and approach are compatible with and utilize components of the CVISN Architecture.*

The PRISM operational concepts are illustrated in the figure below. Originally, the **PRISM Central Site** was maintained by the IOWA DOT. Today, modifications to SAFER are underway to provide PRISM Central Site data exchange support for participating PRISM states using open standards.



### SAFER is being modified to

- provide users with a logical view of the existing PRISM Target File, i.e. access to carrier and vehicle records for those carriers in the MCSIP,
- accept, process, and output MCSIP carrier vehicle records to requesting PRISM state systems,
- generate an historical audit of MCSIP carrier activities,
- support batch and interactive communications,
- provide PRISM users with enhanced query support and report generation capabilities.

# **APPENDIX C.**

## **OPERATIONAL SCENARIOS AND FUNCTIONAL THREAD DIAGRAMS**

This Page Intentionally Blank

# Operational Scenarios and Functional Thread Diagrams

---

- An “operational scenario” is a description of how a state intends that their customers and the state, or the state and core infrastructure systems should interact to accomplish key CVISN functions. An example was given in chapter 4. More examples are provided here.
- The operational scenario is shown as a list of sequential steps. To differentiate between different time schedules, numbers are used to show the interaction between the applicant and the state, and the state’s update of snapshots. Those interactions occur as soon as possible after the initial application is received by the state. Letters are used to show the state’s connections to the clearinghouses, since that occurs at a regular period instead of being triggered immediately by the carrier’s actions.
- Each operational scenario is illustrated by overlaying information onto the state system design template. The lines represent data flow between products, with arrows indicating the direction of flow. Each line is labeled with a number or letter. The complete set of lines constitutes a thread of activities that accomplish a function. Hence, the diagram is called a “functional thread diagram.”
- This appendix provides examples of operational scenarios and functional thread diagrams. They are included for reference, and as starting points for states that plan to implement similar processes.

# CVISN Level 1 Safety Information Exchange Key Operational Scenarios

---

- Record inspections electronically and report them to SAFER and MCMIS
  - **Example 1:** Operational Scenario for 2000: Record inspections electronically and report them to SAFER and MCMIS via CVIEW  
(ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)
  - **Example 2:** Operational Scenario for today: Record inspections electronically and report them to SAFER and MCMIS
  - **Example 3:** Operational Scenario for 2000: Record inspections electronically and report them to SAFER and MCMIS  
(ASPEN-32, SAFETYNET 2000, SAFER 3.0 (No CVIEW))
- Queries
  - **Example 4:** Operational Scenario for 2000: Past inspection report query to SAFER via CVIEW  
(ASPEN-32, SAFER/CVIEW 3.0)
  - **Example 5:** Operational Scenario for today: Past inspection report query to SAFER
  - **Example 6:** Operational Scenario for 2000: Carrier snapshot query to SAFER via CVIEW  
(ASPEN-32, SAFER/CVIEW 3.0)

## Operational Scenario Examples 1-3

- Record inspections electronically and report them to SAFER and MCMIS
  - Retrieve past inspections
  - Report inspection; update snapshots accordingly
  - Review inspection using SAFETYNET, and submit to MCMIS; update snapshots accordingly

**Example 1 Operational Scenario for 2000:  
Record inspections electronically and report them  
to SAFER and MCMIS via CVIEW  
(ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)**

1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to CVIEW's input mailbox in the CVIEW Data Mailbox (CDM), for all inspection reports relating to a particular carrier. The PIQ is in Application File Format (AFF), a precursor to EDI translation.
2. CVIEW passes the query to the SAFER, via a Remote Procedure Call (RPC).  
  
Note: All queries are passed to SAFER where Interstate and Intrastate Inspection Reports are stored for 45-day period.
3. SAFER receives the query, processes the request, and then retrieves the inspection report from data storage. SAFER sends all inspection reports matching the query to CVIEW, via RPC.
4. CVIEW passes the inspection reports to ASPEN via its query mailbox in the CDM, in AFF format. The PIQ detects and processes the report for display on ASPEN. The past inspections show that this carrier's vehicles often have brake problems.

**Example 1 Operational Scenario for 2000:  
Record inspections electronically and report them  
to SAFER and MCMIS via CVIEW  
(ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)**

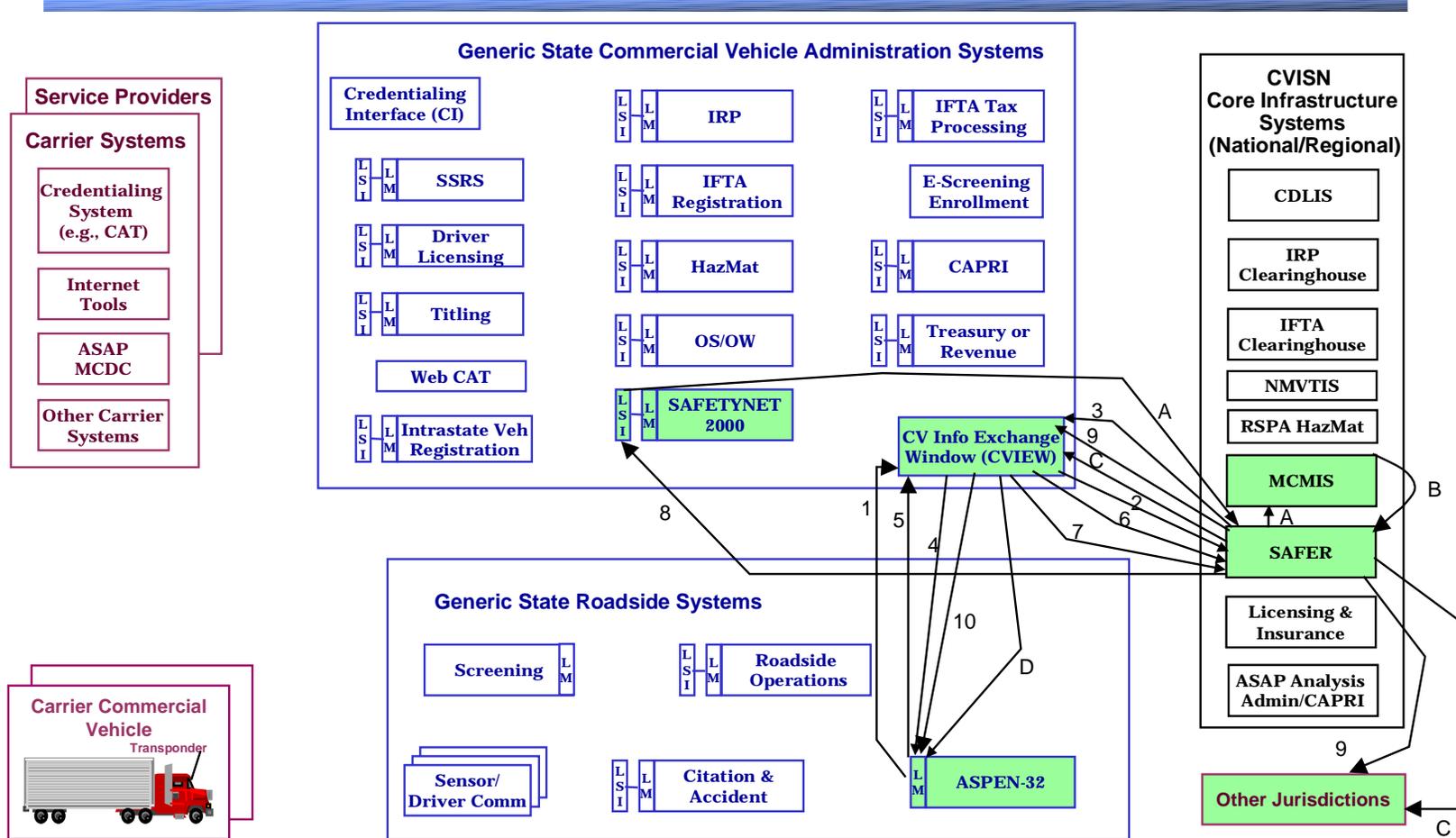
5. The enforcement officer conducts the inspection and finds that the brakes are not functioning properly. He completes the inspection and places the vehicle Out-Of-Service (OOS). ASPEN sends the inspection report to CVIEW's input mailbox in the CDM, in AFF.
6. The CVIEW passes the inspection report to SAFER, via RPC.
7. CVIEW sends the inspection report to SAFETYNET 2000's input mailbox in the SDM in AFF.
8. SAFETYNET retrieves the inspection report from its SDM mailbox.
9. SAFER updates the vehicle snapshot segment with inspection information, e.g., OOS status, Inspection history. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
10. CVIEW forwards vehicle snapshot views to ASPEN units via their subscription mailboxes in the CDM in AFF.

**Example 1 Operational Scenario for 2000:  
Record inspections electronically and report them  
to SAFER and MCMIS via CVIEW  
(ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)**

- A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the SDM.
- B. MCMIS receives the inspection report and updates carrier summary information and computes carrier safety statistics, e.g., carrier safety ratings and history, inspection summaries. Weekly, MCMIS sends SAFER updated carrier snapshot segments via flat file.
- C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
- D. CVIEW forwards carrier snapshot views to ASPEN units via their subscription mailboxes in the CDM in AFF.

*NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. The results of processing an incoming TS 285 are reported via TS 824.*

# Example 1 Functional Thread Diagram for 2000: Record inspections electronically and report them to SAFER and MCMIS via CVIEW (ASPEN-32, SAFETYNET 2000, SAFER/CVIEW 3.0)



## Example 2 Operational Scenario for today: Record inspections electronically and report them to SAFER and MCMIS

---

1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to SAFER's input mailbox in the SAFER Data Mailbox (SDM), for all inspection reports relating to a particular carrier, in ASPEN-Unique, non-EDI file format.

Note: Intrastate and Interstate Inspection reports are stored in SAFER for 45 days.

2. SAFER receives, processes, and sends all inspection reports matching the query to ASPEN, in ASPEN-Unique, non-EDI file format. The past inspections show that this carrier's vehicles often have brake problems

Note: The SAFER system retrieves the query from its input mailbox in the Safer Data Mailbox (SDM), processes the request, and then retrieves the inspection report from data storage. The report is placed in the requester's query mailbox in the SDM. The PIQ detects and processes the report for display on ASPEN.

## Example 2 Operational Scenario for today: Record inspections electronically and report them to SAFER and MCMIS

---

3. The enforcement officer conducts the inspection and finds that the brakes are not functioning properly. He completes the inspection and places the vehicle Out-Of-Service (OOS). ASPEN sends the inspection report to SAFER's input mailbox and SAFETYNET's input mailbox in the SDM, in ASPEN-Unique, non-EDI file format.
4. SAFER updates the vehicle snapshot segment with inspection information e.g., OOS status, Inspection history. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
5. SAFETYNET 9 or 10 retrieves the inspection report from its input mailbox on the SDM, still in ASPEN-Unique non-EDI file format.

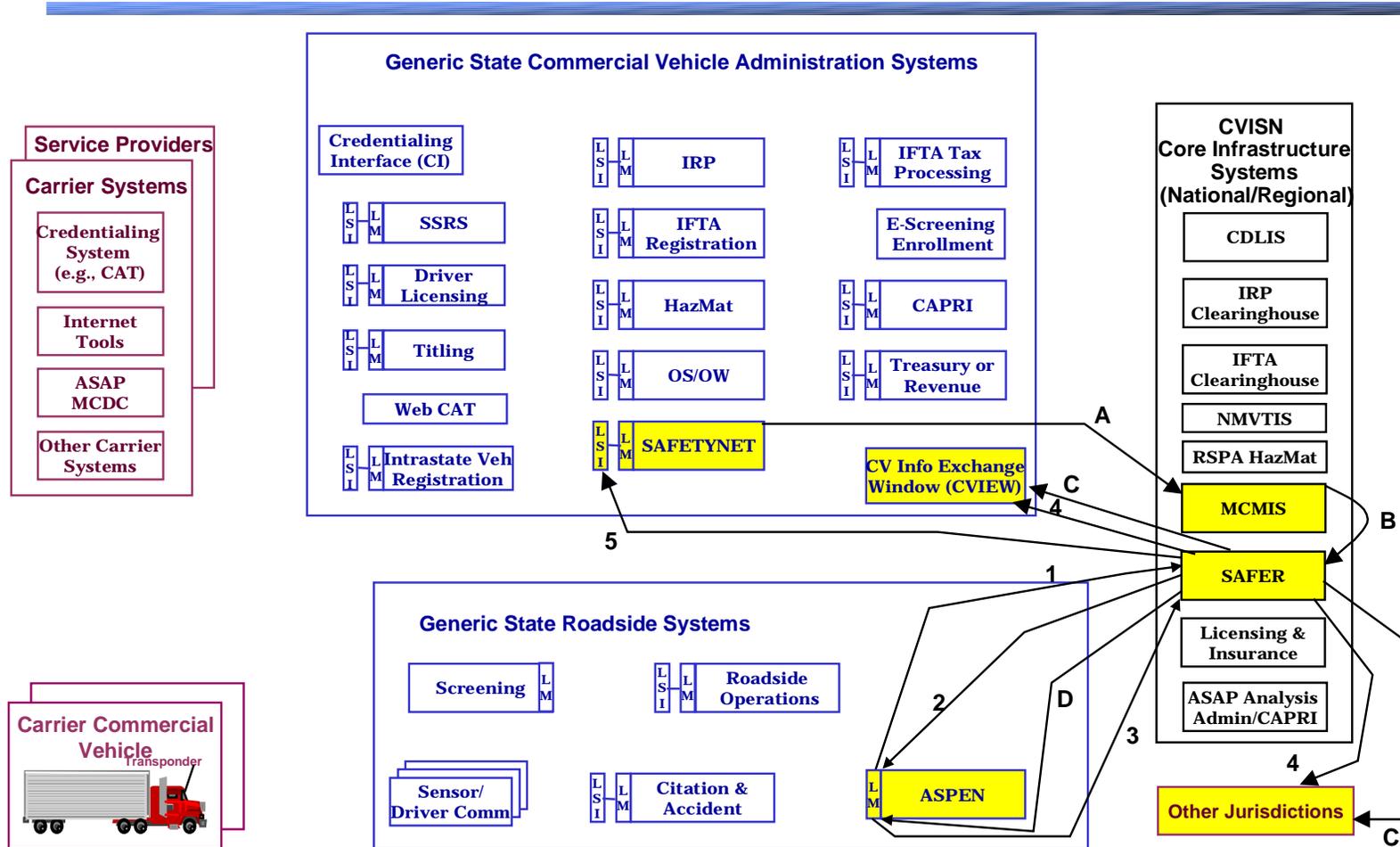
## Example 2 Operational Scenario for today: Record inspections electronically and report them to SAFER and MCMIS

---

- A. The SAFETYNET 9 or 10 staff member reviews the inspection report and sends it to MCMIS using existing methods.
- B. MCMIS receives the inspection report and updates carrier summary information and computes carrier safety statistics, e.g., carrier safety ratings, history and inspection summaries. Weekly, MCMIS sends SAFER updated carrier snapshot segments in flat file format.
- C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
- D. SAFER then forwards carrier snapshot views to ASPEN subscribers in non-EDI file format.

***NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. The results of processing an incoming TS 285 are reported via TS 824.***

## Example 2 Functional Thread Diagram for today: Record inspections electronically and report them to SAFER and MCMIS



---

## Example 3 Operational Scenario for 2000: Record inspections electronically and report them to SAFER and MCMIS (ASPEN-32, SAFETYNET 2000, SAFER 3.0 (No CVIEW))

---

1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to SAFER's input mailbox in the SAFER Data Mailbox (SDM), for all inspection reports relating to a particular carrier. The PIQ is in Application File Format (AFF), a precursor to EDI.

Note: SAFER stores Intrastate and Interstate Inspection Reports for 45-day period.

2. SAFER receives, processes, and sends all inspection reports matching the query to ASPEN, in AFF. The past inspections show that this carrier's vehicles often have brake problems.

Note: The SAFER system retrieves the query from its input mailbox in the Safer Data Mailbox (SDM), processes the request, and then retrieves the inspection report from data storage. The report is placed in the requester's query mailbox in the SDM. The PIQ detects and processes the report for display on ASPEN.

**Example 3 Operational Scenario for 2000:  
Record inspections electronically and report them  
to SAFER and MCMIS  
(ASPEN-32, SAFETYNET 2000, SAFER 3.0 (No CVIEW))**

---

3. The enforcement officer conducts the inspection and finds that the brakes are not functioning properly. He completes the inspection and places the vehicle Out-Of-Service (OOS). ASPEN sends the inspection report to SAFER's input mailbox and SAFETYNET's input mailbox in the SDM, in AFF.
4. SAFER updates the vehicle snapshot segment with inspection information e.g., OOS status, Inspection history. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
5. SAFETYNET 2000 retrieves the inspection report from its input mailbox on the SDM in AFF.

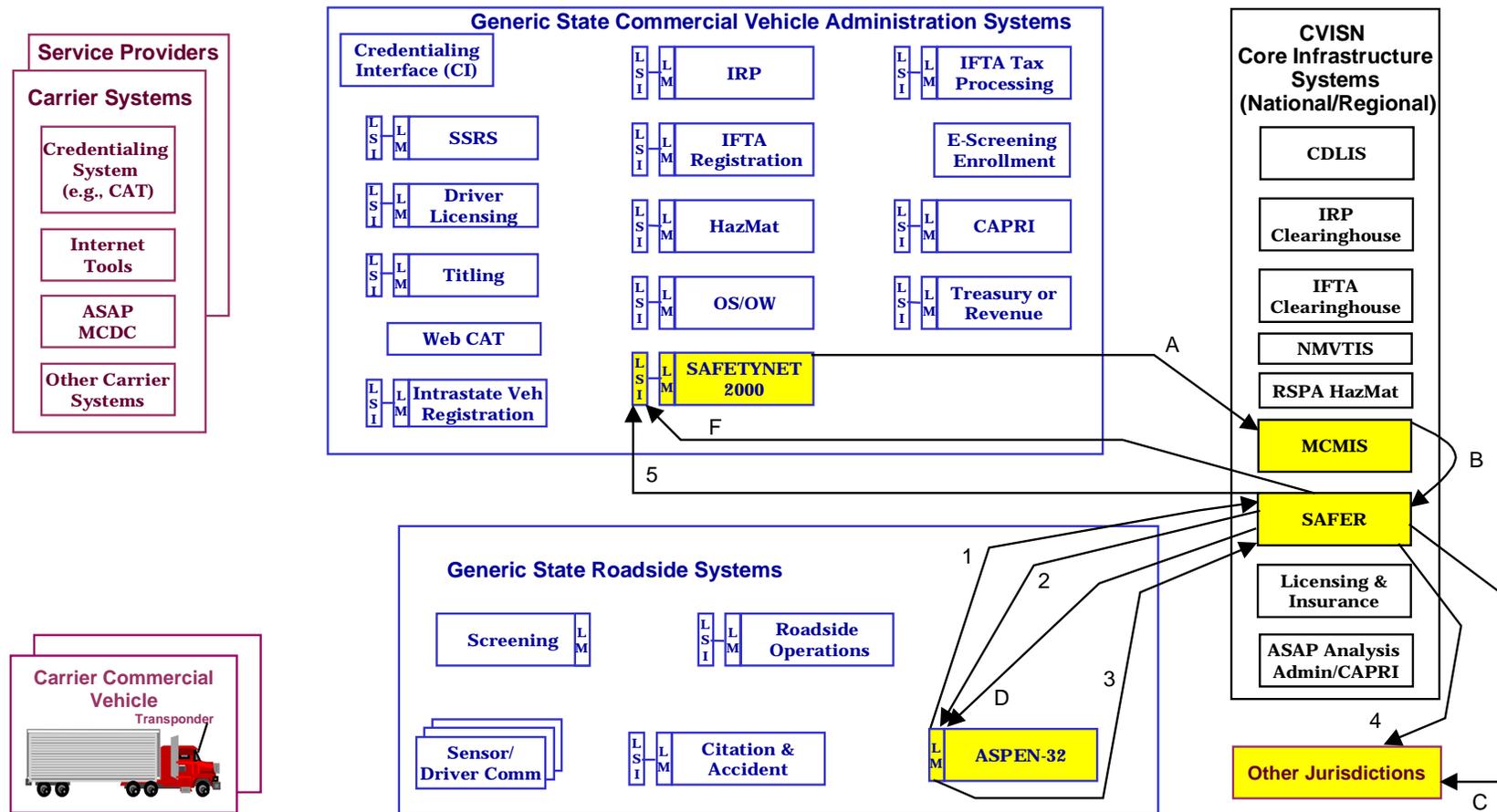
**Example 3 Operational Scenario for 2000:  
Record inspections electronically and report them  
to SAFER and MCMIS  
(ASPEN-32, SAFETYNET 2000, SAFER 3.0 (No CVIEW))**

---

- A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the SDM.
- B. MCMIS receives the inspection report and updates carrier summary information and computes carrier safety statistics, e.g., carrier safety ratings, history and inspection summaries. Weekly, MCMIS sends SAFER updated carrier snapshot segments in flat file format.
- C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.
- D. SAFER then forwards carrier snapshot views to ASPEN subscribers in AFF.

***NOTE: Functional acknowledgment for all EDI messages (except TS 997) is made by responding with a TS 997. The results of processing an incoming TS 285 are reported via TS 824.***

# Example 3 Functional Thread Diagram for 2000: Record inspections electronically and report them to SAFER and MCMIS (ASPEN-32, SAFETYNET 2000, SAFER 3.0 (No CVIEW))



## Example 4 Operational Scenario for 2000: Past inspection report query to SAFER via CVIEW (ASPEN-32, SAFER/CVEIW 3.0)

---

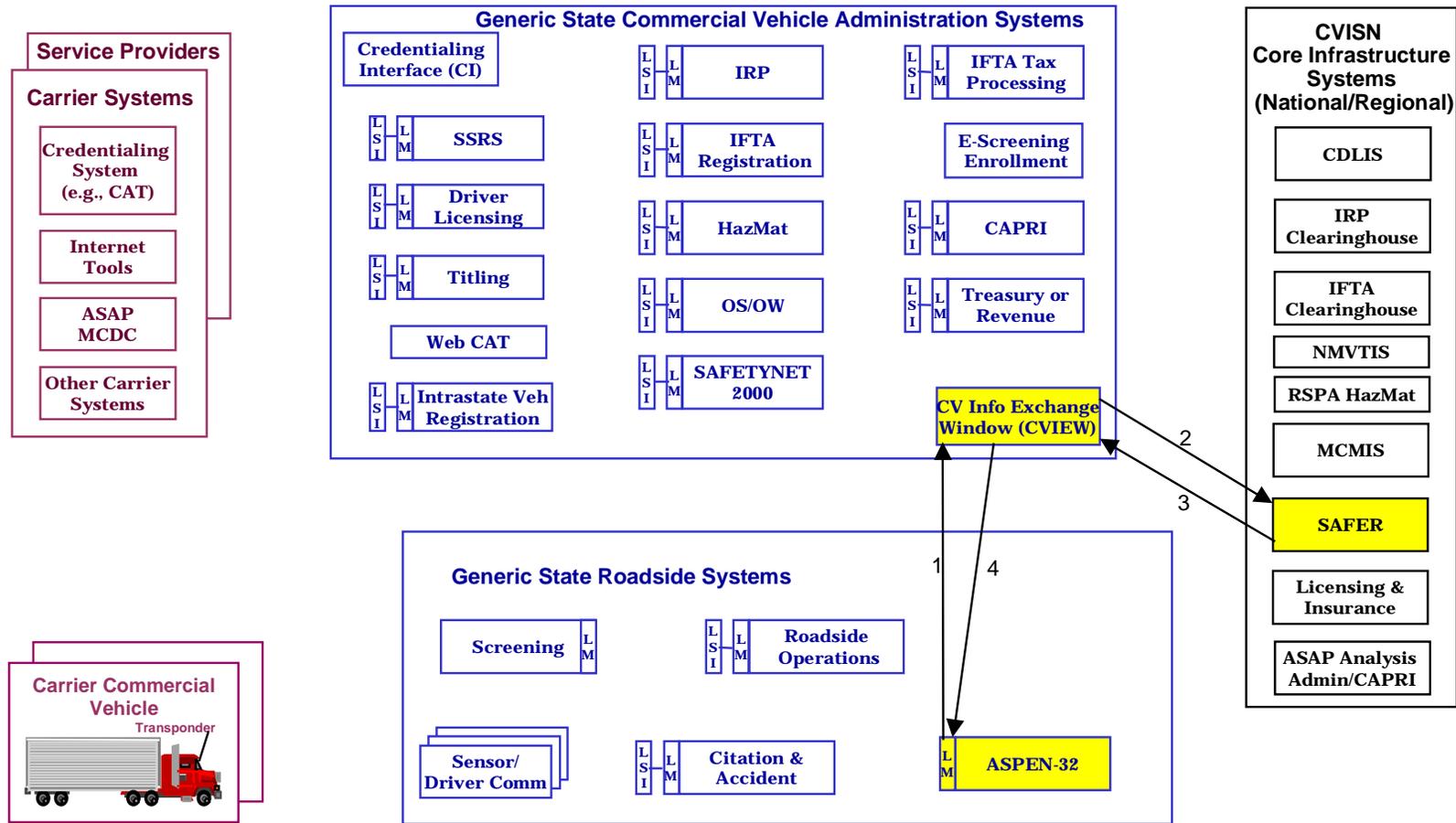
1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to CVIEW's input mailbox in the CVIEW Data Mailbox (CDM), for all inspection reports relating to a particular carrier. The PIQ is in Application File Format (AFF), a precursor to EDI translation.
2. CVIEW passes the query to the SAFER, via a Remote Procedure Call (RPC).

Note: All queries are passed to SAFER where Interstate and Intrastate Inspection Reports are stored for 45-day period.

3. SAFER receives the query, processes the request, and then retrieves the inspection report from data storage. SAFER sends all inspection reports matching the query to CVIEW, via RPC.
4. CVIEW passes the inspection reports to ASPEN via its query mailbox in the CDM, in AFF format. The PIQ detects and processes the report for display on ASPEN.

## Example 4 Functional Thread Diagram for 2000: Past inspection report query to SAFER via CVIEW

(ASPEN-32, SAFER/CVEIW 3.0)



## Example 5 Operational Scenario for today: Past inspection report query to SAFER

---

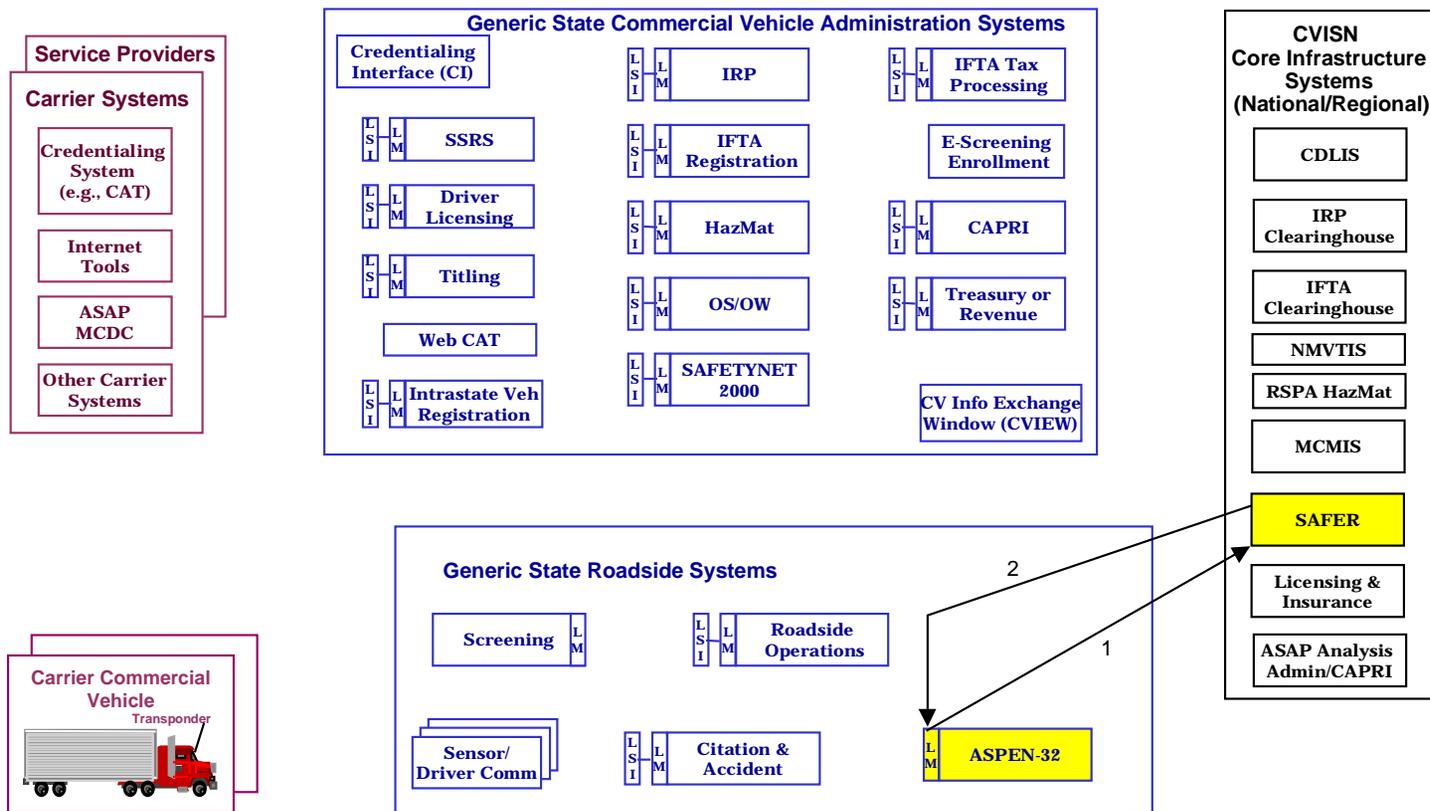
1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to SAFER's input mailbox in the SAFER Data Mailbox (SDM), for all inspection reports relating to a particular carrier, in ASPEN-Unique, non-EDI file format.

Note: Intrastate and Interstate Inspection reports are stored in SAFER for 45 days.

2. SAFER receives, processes, and sends all inspection reports matching the query to ASPEN, in ASPEN-Unique, non-EDI file format.

Note: The SAFER system retrieves the query from its input mailbox in the Safer Data Mailbox (SDM), processes the request, and then retrieves the inspection report from data storage. The report is placed in the requester's query mailbox in the SDM. The PIQ detects and processes the report for display on ASPEN.

## Example 5 Functional Thread Diagram for Today: Past inspection report query to SAFER



## Example 6 Operational Scenario for 2000: Carrier snapshot query to SAFER via CVIEW (ASPEN-32, SAFER/CVIEW 3.0)

---

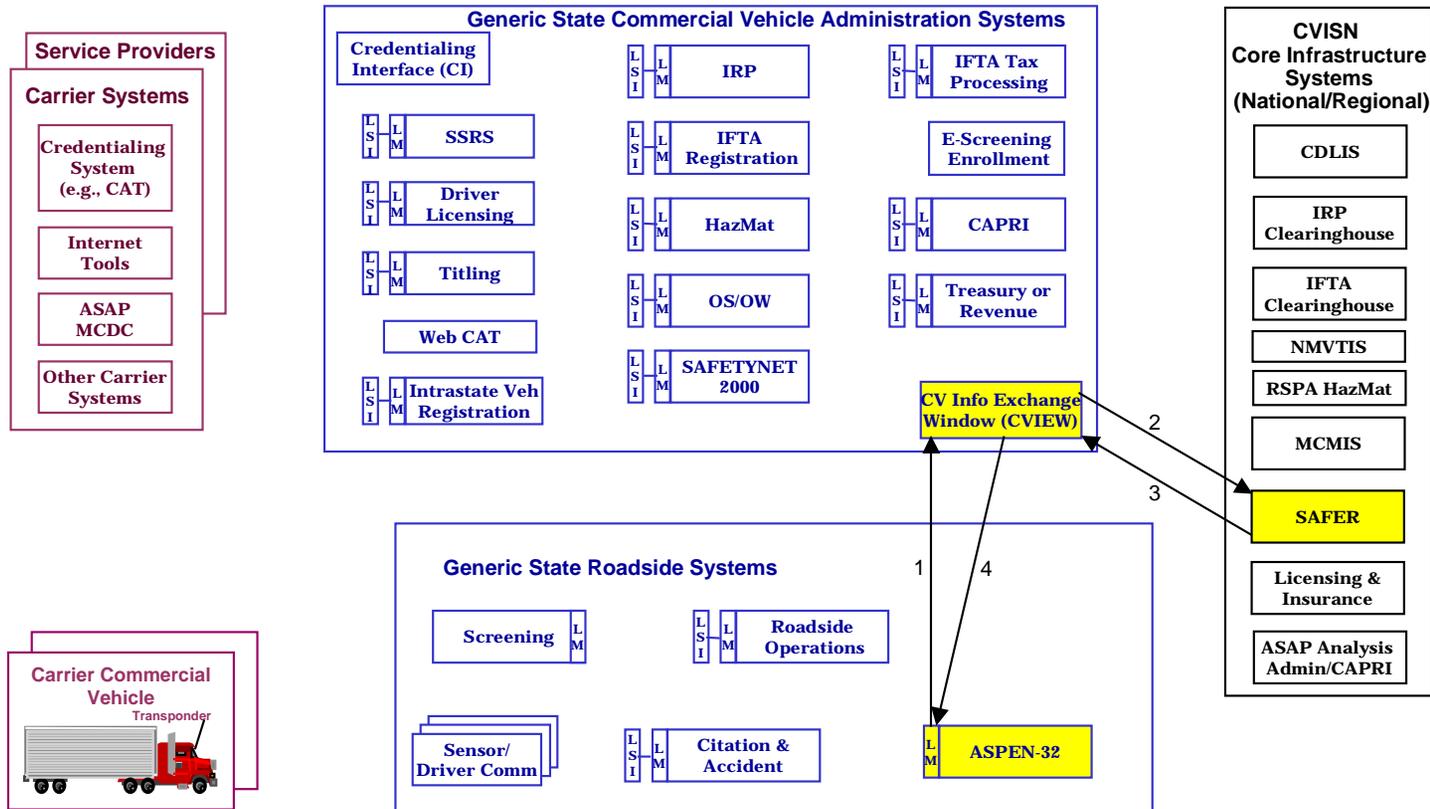
1. While performing a level 5 inspection, the enforcement officer, using ASPEN's Inspection Selection System (ISS), issues a query to CVIEW's Data Mailbox (CDM), for a carrier snapshot to check the carrier's SafeStat values, via Application File Format (AFF).

Note: Query parameters for a specific motor carrier snapshot may be by Primary Carrier ID, Name, ICC Number, or State in which the carrier is domiciled.

2. CVIEW passes the query to SAFER, via a Remote Procedure Call (RPC).
3. SAFER receives, processes, and sends the carrier snapshot matching the query CVIEW, via RPC.
4. CVIEW passes the carrier snapshot to ASPEN's ISS.

Note: A review of the SafeStat values shows the Carrier is ranked average relative to other motor carriers.

## Example 6 Functional Thread Diagram for 2000: Carrier snapshot query to SAFER via CVIEW (ASPEN-32, SAFER/CVIEW 3.0)



This Page Intentionally Blank