CVISN Guide to Safety Information Exchange

POR-99-7191

Baseline Version 1.0

February 2002

Commercial Vehicle Information Systems and Networks (CVISN) Guide to Safety Information Exchange

POR-99-7191

Baseline Version V1.0

February 2002

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 U.S. 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 Intelligent Transportation Systems (ITS) / Commercial Vehicle Operations (CVO) program, a voluntary effort involving public and private partnerships that uses information systems, innovative technologies, and business practice re-engineering to improve safety, simplify government administrative systems, and provide savings to states and motor carriers. The FMCSA works closely with the FHWA ITS Joint Program Office (JPO) to ensure the integration and interoperability of ITS/CVO systems with the national ITS program.

Baseline Issue

This is a baseline document, which has completed internal and external reviews of previously published drafts and preliminary versions. All comments received to date have been incorporated or addressed.

It is disseminated in the interest of information exchange. The Johns Hopkins University Applied Physics Laboratory (JHU/APL) assumes no liability for its contents or use thereof. This document 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 objective of this document.

This and other CVISN-related documentation are available for review and downloading from the JHU/APL CVISN site on the World Wide Web (http://www.jhuapl.edu/cvisn/).

Please Provide Comments

The authors would appreciate any and all feedback about this document, from modest typos to egregious errors. We are especially interested in hearing from you if you find a topic is missing or if our emphasis is wrong.

Ms. Mary W. Stuart
The Johns Hopkins University Applied Physics Laboratory
CVISN Project
11100 Johns Hopkins Road
Laurel, MD 20723-6099

Phone: 240-228-7001
Fax: 240-228-6149
E-Mail: mary.stuart@jhuapl.edu

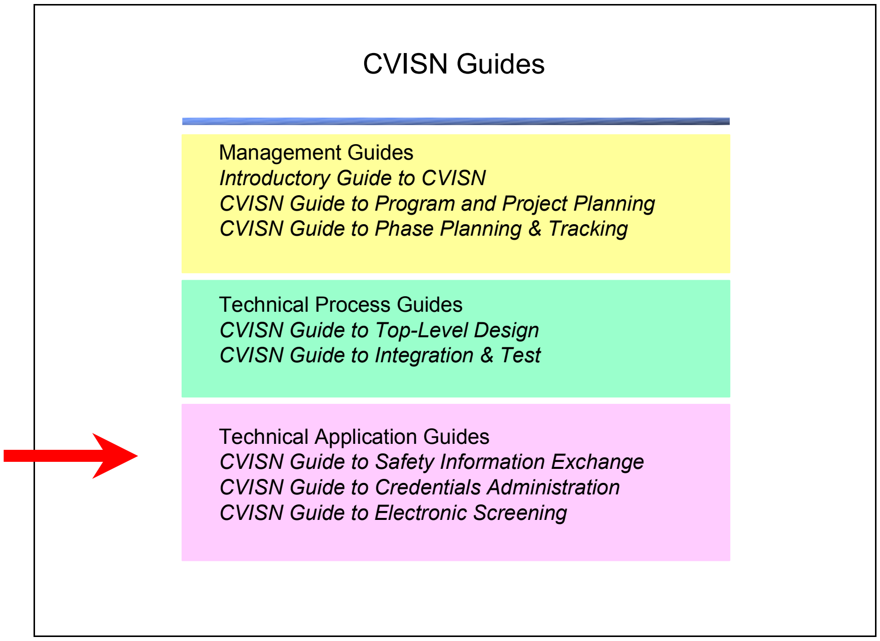
CVISN Guide to Safety Information Exchange

Table of Contents

1. INTRODUCTION

Safety Information Exchange is one of the three key program areas in Commercial Vehicle Information Systems and Networks (CVISN). 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/cvisn/). The list of CVISN Guides is shown in Figure 1–1.



CVISN Guides

Management Guides
Introductory Guide to CVISN
CVISN Guide to Program and Project Planning
CVISN Guide to Phase Planning & Tracking

Technical Process Guides
CVISN Guide to Top-Level Design
CVISN Guide to Integration & Test

Technical Application Guides
CVISN Guide to Safety Information Exchange
CVISN Guide to Credentials Administration
CVISN Guide to Electronic Screening

Figure 1–1. CVISN Guides

Factors to Consider in Safety Information Exchange

Some factors to consider when working in the safety information exchange area are:

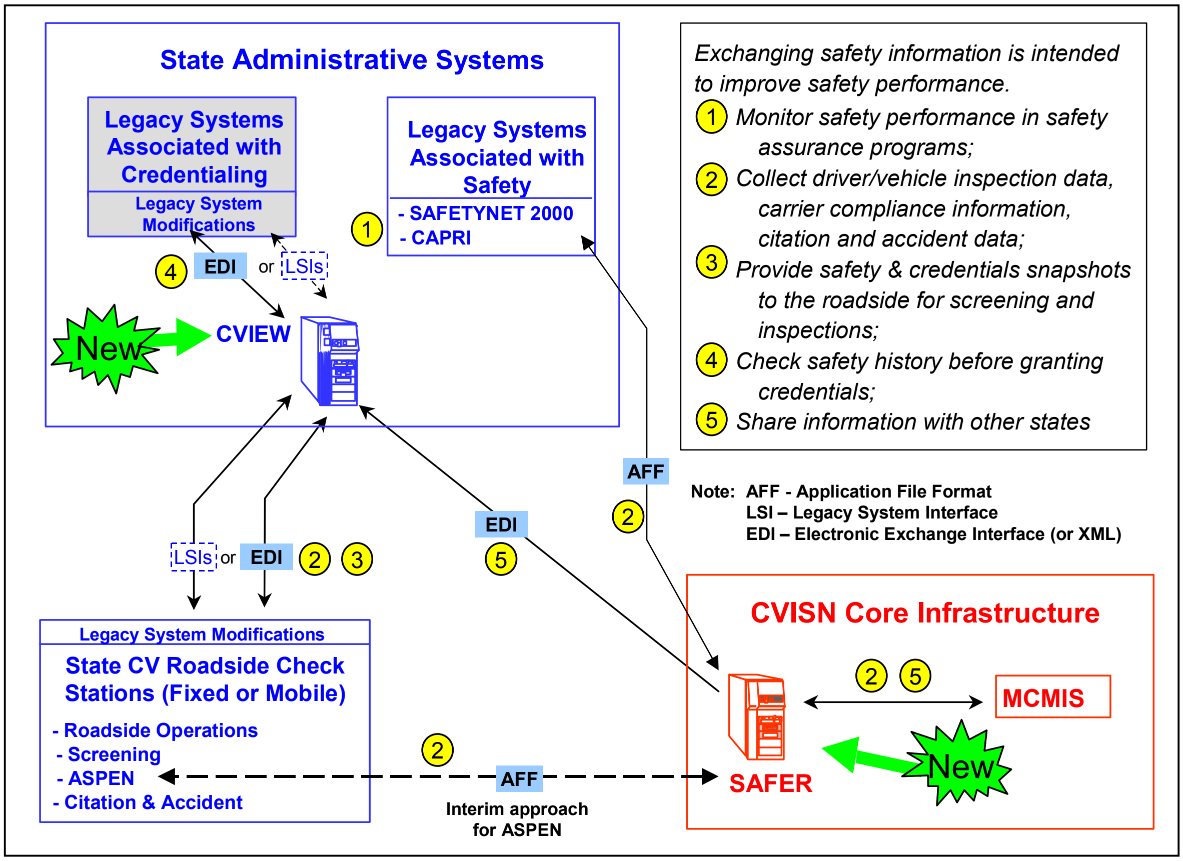
- One of the more critical decisions a state needs to make is how to integrate inter- and intrastate safety information and provide it to the roadside to facilitate electronic screening and inspection operations, i.e., will a state plan on building and deploying a Commercial Vehicle Information Exchange Window (CVIEW) system, such as the Federal Motor Carrier Safety Administration (FMCSA)-developed CVIEW or an equivalent system, or will it plan on using Safety and Fitness Electronic Records (SAFER) to fill that role.
- The development process for CVIEW or the interface to SAFER 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 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 Commercial Vehicle Safety Alliance (CVSA), American Association of Motor Vehicle Administrators (AAMVA), American Association of State Highway and Transportation Officials (AASHTO), International Fuel Tax Agreement (IFTA) Inc., and International Registration Plan (IRP), Inc.
  - Monthly teleconferences organized by FMCSA among CVISN states
  - CVISN development forums organized by FMCSA
  - Status of Electronic Data Interchange (EDI) standards and implementation guides
  - Activities of SAFER Option Working Group (SOWG)

2. WHAT IS SAFETY INFORMATION EXCHANGE?

Safety information exchange is the electronic exchange of safety data and supporting credentials 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 that are based on historical safety performance information. Figure 2–1 defines the intent of safety information exchange and provides an overview of the systems, interfaces, and data flows involved in accomplishing that intent. The CVIEW and SAFER components are relatively new systems that were developed by FMCSA specifically to support the CVISN effort.


State Administrative Systems
Legacy Systems Associated with Credentialing
Legacy System Modifications
Legacy Systems Associated with Safety
- SAFETYNET 2000
- CAPRI
1
4
EDI
or
LSIs
New
CVIEW
AFF
2
EDI
5
LSIs
or
EDI
2
3
Legacy System Modifications
State CV Roadside Check Stations (Fixed or Mobile)
- Roadside Operations
- Screening
- ASPEN
- Citation & Accident
2
AFF
Interim approach for ASPEN
CVISN Core Infrastructure
2
5
MCMIS
New
SAFER

Exchanging safety information is intended to improve safety performance.

1. *Monitor safety performance in safety assurance programs;*
2. *Collect driver/vehicle inspection data, carrier compliance information, citation and accident data;*
3. *Provide safety & credentials snapshots to the roadside for screening and inspections;*
4. *Check safety history before granting credentials;*
5. *Share information with other states*

Note: AFF - Application File Format
LSI – Legacy System Interface
EDI – Electronic Exchange Interface (or XML)

Figure 2–1. Safety Information Exchange

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 safety and credentials 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.

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 (USDOT) 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 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 established a goal to reduce the number of fatalities and injuries for commercial vehicle accidents by 50 percent by 2010. 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 intrastate operators.

3. WHAT ALREADY EXISTS?

Key components already exist for carrier, state and CVISN core infrastructure systems. These include national systems developed for the storage, processing and exchange of safety data, 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. In other words, many components necessary to create a comprehensive inter- and intrastate commercial vehicle safety information system already exist. 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 used for safety information exchange. By comparing the components that are presently in place for a particular state with the overall National Intelligent Transportation Systems (ITS) Architecture (http://www.its.dot.gov/) a plan can be produced to develop the components required to complete the system for that state.

An overview of the connectivity between these systems is provided in Figure 3–1. A more detailed description of each application/system as it affects the exchange of safety information within a state is provided in the following sections. In each case, the description of safety information element flow among the components shown in Figure 3–1 will include a more complete flow diagram containing only those components that are involved in the process.

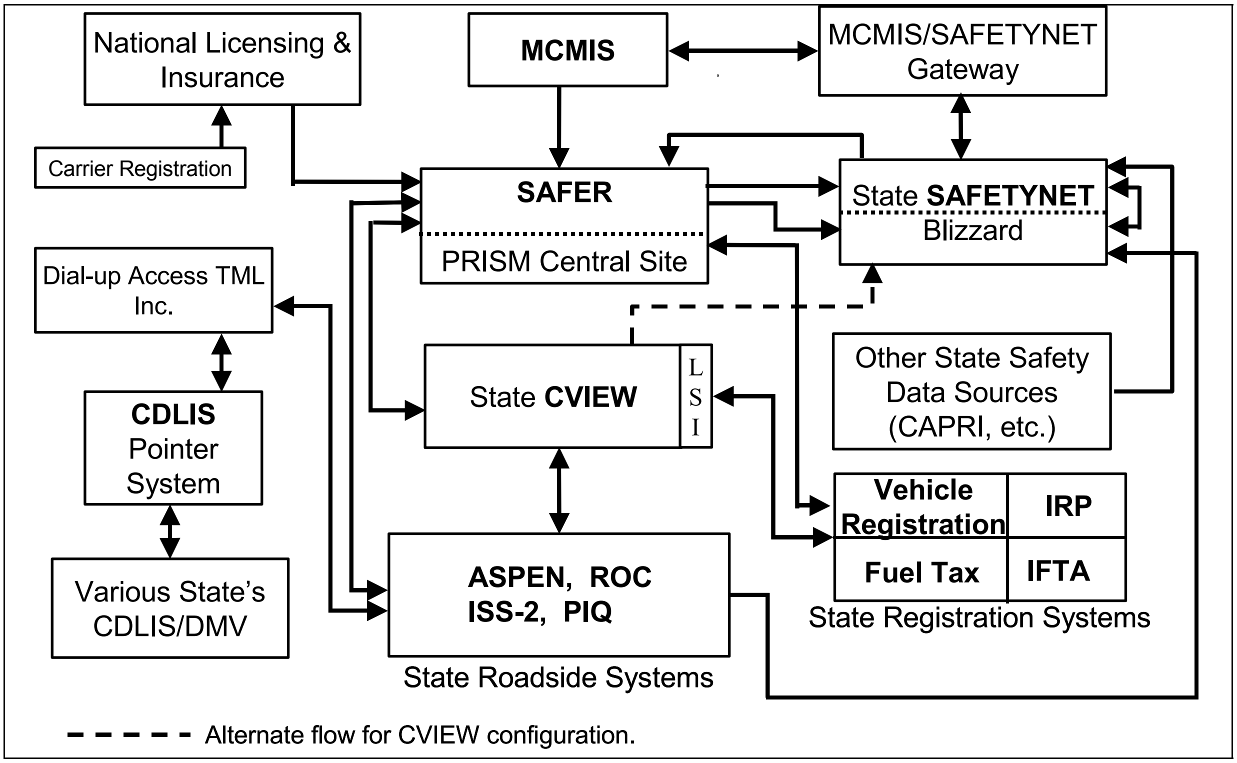


Figure 3–1. Overall Connectivity Between Commercial Vehicle Information Systems

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 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 (http://www.safersys.org/) also provides access to Licensing and Insurance (L&I) information for those carriers required to obtain insurance and federal operating authority. SAFER and MCMIS may be expanded in the near future to include information for intrastate carriers as well.

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 CVIEW and SAFETYNET systems; state roadside systems, which include ASPEN, the Past Inspection Query (PIQ), the Inspection Selection System (ISS-2) and the Roadside Operations Computer (ROC); and other applications that fall into neither category such as the Carrier Automated Performance Review Information (CAPRI) application. At least some of these systems also interact with national systems such as SAFER to access or exchange safety and other information about commercial vehicles and motor carriers.

3.2.1 Commercial Vehicle Information Exchange Window (CVIEW)

CVIEW 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[1] and reports for exchange within the state (e.g., to roadside sites) and with the SAFER system. In CVISN Level 1, there is a requirement to implement CVIEW (or a CVIEW equivalent) system for exchange of intrastate and interstate data within the state. The FMCSA-developed CVIEW is a distributed version of the FMCSA-developed SAFER system. It is owned by, located in, and usually customized by a state. The state can choose to implement the FMCSA-developed CVIEW or an equivalent system that performs the same functions. Throughout this chapter the term CVIEW is used to refer to the FMCSA-developed CVIEW or any equivalent system that a state may deploy.

[1] A ***Snapshot*** is a concise collection of safety and credential data about carriers, vehicles, and (future) drivers. It is designed to facilitate the process of making screening and inspection decisions at roadside vehicle weigh stations. It is an electronic record of safety and credential data including identification, size, commodity information, safety record (including safety rating (if any) and roadside out-of-service inspection data), registration and permit information, and other related data. More information about data snapshots and data elements exchanged in vehicle and carrier updates and data retrieval can be found in Reference 3.

The functions that CVIEW, or its equivalent, will perform are listed below:

- Provide for the electronic exchange of:
  - **interstate** carrier and vehicle credential data between state source systems, users, and SAFER
  - **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
  - **intrastate** carrier and vehicle safety and credential data
- Support safety inspection data reporting and retrieval by roadside enforcement personnel
- Provide inter- and intrastate carrier and vehicle safety and credential data to the roadside to support electronic screening and other roadside operations
- Perform electronic exchange using one or more of the following standards:
  - EDI standards
  - non-EDI standards, the selection of which is system-dependent
  - new open standard methods of information exchange (e.g., XML) as they become available and are requested by users
- Allow the general public to access data without the security risk of providing a direct connection to sensitive legacy systems.

Each state is responsible for maintaining the credential segments of the snapshots for interstate carriers for vehicles based within the state. CVIEW is also responsible for assembling and storing complete snapshots for intrastate carriers and vehicles and making those data available to the roadside and other state agencies. The safety data exchange using CVIEW is depicted in Figure 3–2.

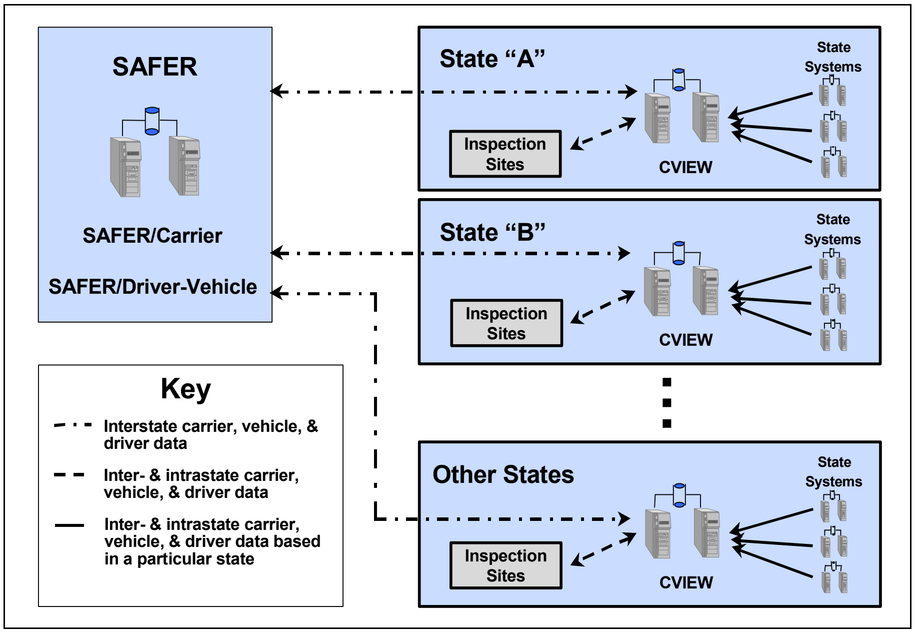


Figure 3–2. SAFER/CVIEW Data Exchange

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 3–3.

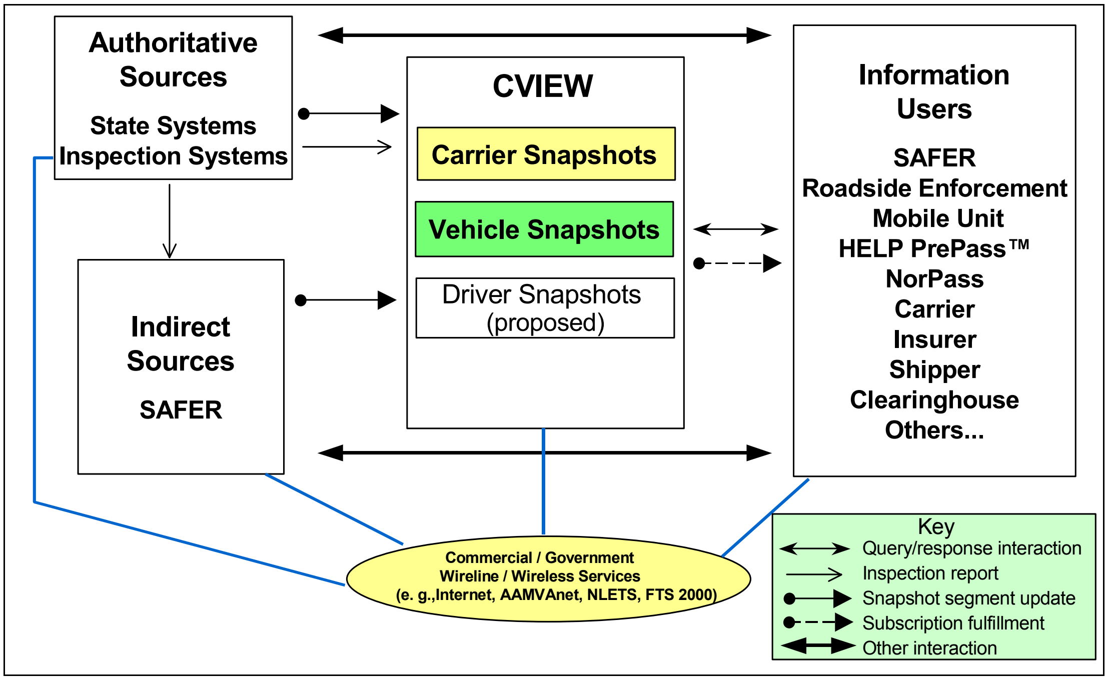


Figure 3–3. CVIEW Design Overview

CVIEW performs on a state level the same functions that SAFER performs 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. For more information on CVIEW interface specifications, see Reference 44.

In addition to snapshot-related functions, CVIEW may serve as the single interface system for ASPEN units in the field. ASPEN may upload and retrieve inspection reports to/from SAFER via CVIEW.

3.2.1.1 CVIEW Data Exchange Mechanism

The FMCSA-developed CVIEW has similar Data Mailbox facilities to SAFER to facilitate the exchange of information among state users within the state agencies. The CVIEW clients can log onto the CVIEW service to send queries and updates to CVIEW via the CVIEW inbox, and they retrieve query responses and data downloads by accessing their CVIEW Data Mailbox (CDM) on the CVIEW system. The data that is downloaded to the mailbox is specified in the subscription process. A subscription is a request for information (e.g., specific carrier or vehicle data elements) that is stored and serviced by a system (e.g., SAFER or CVIEW). A subscription's definition includes the conditions under which the information is to be sent to recipients. New records or changes to existing records that satisfy the rules defined in the subscription will result in the generation of a snapshot for that record and its transmission to the recipients identified in the subscription.

CVIEW retrieves safety and credentials data from the SAFER system by subscribing to SAFER data on behalf of the entire state. CVIEW retrieves carrier and vehicle snapshot updates from its SAFER Data Mailbox (SDM) on a periodic basis, and forwards those data to each CVIEW user via the CDM (e.g., each roadside system, as well as to each ASPEN unit with the release of CVIEW Version 3). Similarly, CVIEW sends interstate registration, taxation and permitting data to SAFER, at the discretion of the state, via SAFER's subscription mailbox on the state CVIEW system.

SAFER was initially built to provide snapshot data to CVIEW using EDI. That is the mechanism by which the FMCSA-developed CVIEW currently receives subscription data from SAFER. SAFER also responds to EDI queries for snapshots. In the FMCSA version of CVIEW, however, snapshot queries (carrier only) are sent to SAFER via remote procedure call (RPC), not EDI. The RPC capability was implemented in both SAFER and CVIEW to improve performance for the near-term, but its long-term support is uncertain and continued availability is not guaranteed. EDI is the current official interface and states can enhance the FMCSA-developed CVIEW by implementing EDI snapshot queries. However, in the future, the snapshot query interface is expected to be Web-based, using XML and Hypertext Transfer Protocol (HTTP); new developers should concentrate on that approach.

3.2.1.2 CVIEW Information Flow

The flows of credentials information and safety information through CVIEW are depicted in Figures 3–4 and 3–5, respectively. The bolded text and lines denote the data flows into and out of CVIEW.

Figure 3–4 represents the transmission of registration and fuel tax information from state legacy systems, via LSIs, to the state's CVIEW system.

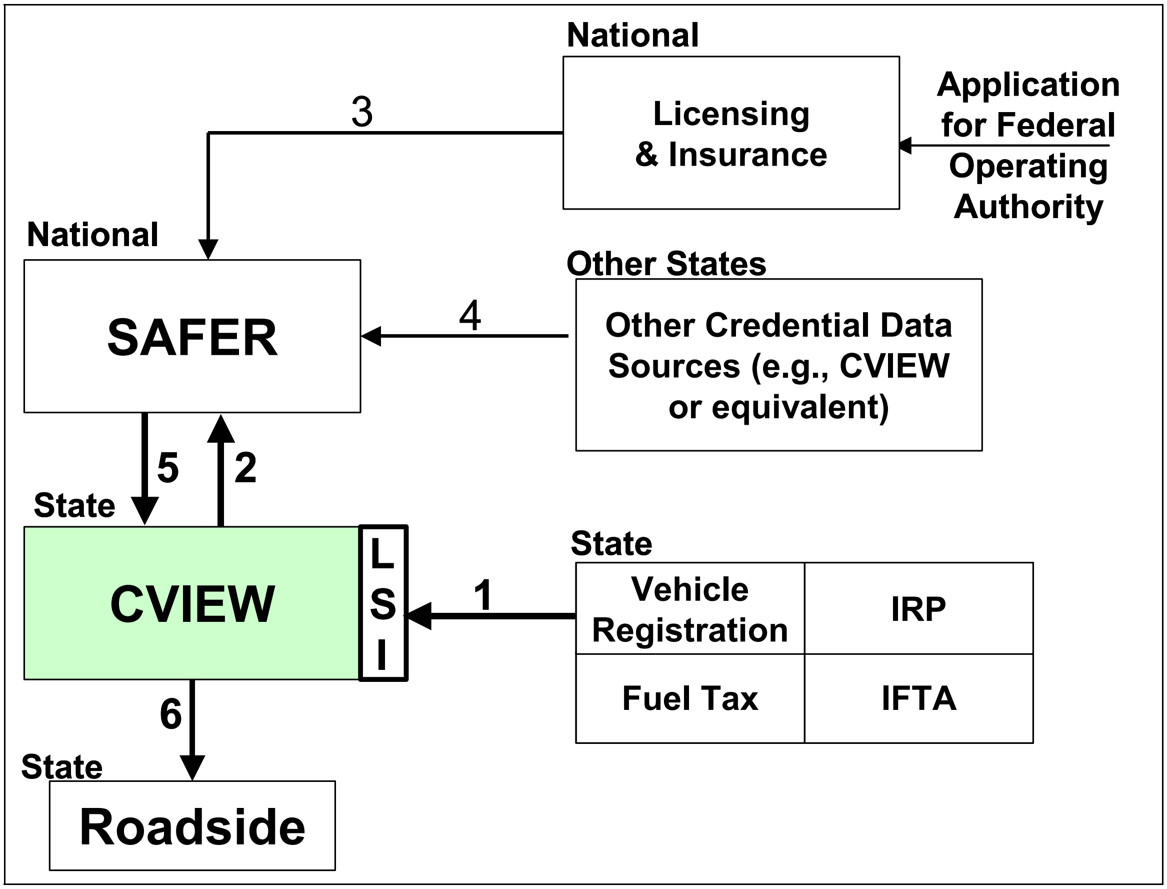


Figure 3–4. CVIEW Credentials Information Flow

The individual credentials information flow elements presented in Figure 3–4 are described below.

Flow 1. CVIEW receives registration and fuel tax information from state legacy systems via LSIs.
Flow 2. CVIEW sends interstate credential data received from the state legacy systems to SAFER via the subscription process.
Flow 3. SAFER receives interstate credential data from the national L&I system.
Flow 4. SAFER receives interstate credential data from other states via state CVIEW or equivalent.
Flow 5. CVIEW receives interstate credentials data from SAFER via the subscription process.
Flow 6. CVIEW sends inter- and intrastate credential data to the roadside via the subscription process.

Figure 3–5 represents the transmission of vehicle and/or driver inspection data from the roadside, via the ASPEN client or equivalent. CVIEW does not store the inspection data but rather passes the data through to SAFER, where the data are stored for a 60-day period, and subsequently transmitted through CVIEW to the roadside. In addition to the CVIEW-specific flow elements, information from other sources is made available for use in roadside operations by connections to MCMIS, SAFETYNET, and other state sources through the CVIEW-to-SAFER connection.

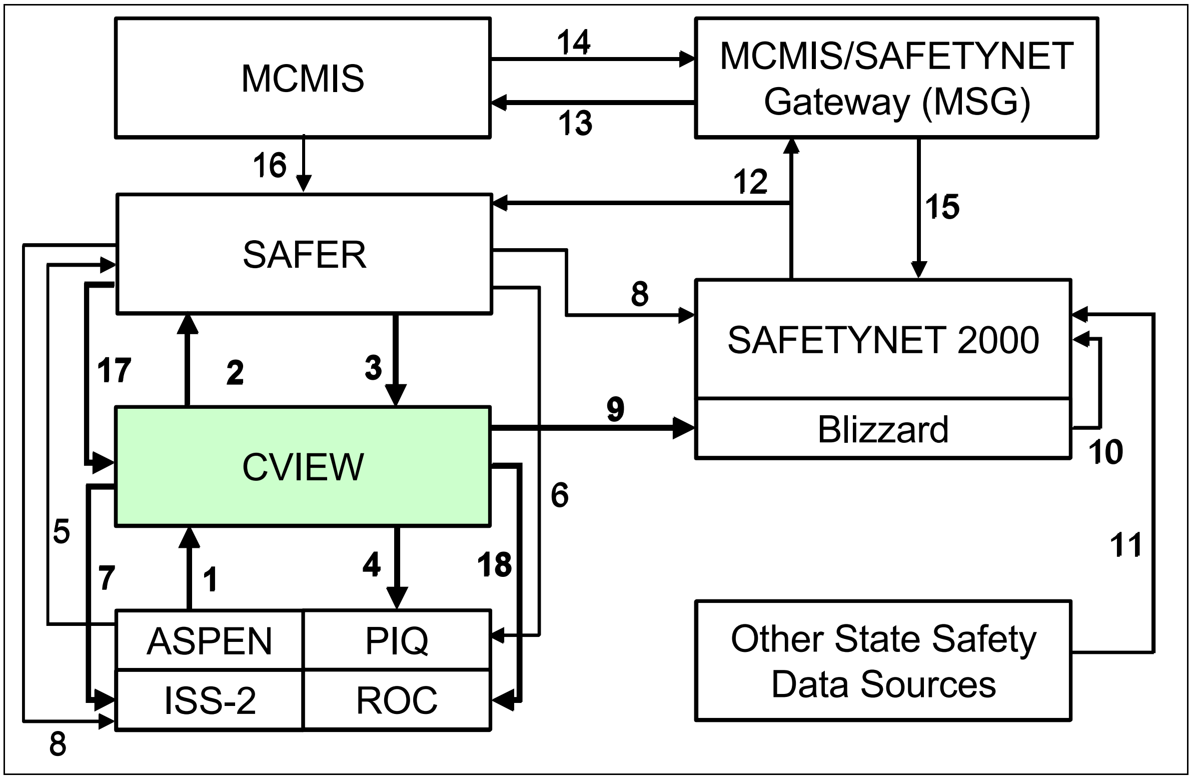


Figure 3–5. CVIEW Safety Information Flow

The individual safety information flow elements presented in Figure 3–5 are described below.

Note: Flows 1, 2, 3 and 4 are CVIEW capabilities incorporated in Version 3 of the software. All other flows are current CVIEW capabilities.

Flow 1. The vehicle and/or driver inspection data are transmitted from the roadside, via the ASPEN client or equivalent, to a state's CVIEW system. The inspection report is copied to the state safety data mailbox for retrieval by Blizzard.

Flow 2. The inspection data are passed through to SAFER (and not stored by CVIEW).

Flow 3. One or more inspection reports are returned from SAFER to CVIEW (for transmission to the roadside).

Flow 4. One or more inspection reports are returned from CVIEW to the roadside in response to a query from a user via the PIQ.

Note: Flows 5, 6, and 8 represent the information flow from SAFER to users when ASPEN interfaces directly with SAFER.

Flow 5. Inspection reports are sent to and stored in SAFER. The inspection report is copied to the state safety data mailbox for retrieval by Blizzard.
Flow 6. Inspection reports are retrieved from SAFER via PIQ.
Flow 7. CVIEW transmits weekly updates of safety data to the ISS-2 clients via the subscription process.
Flow 8. SAFER sends weekly updates of carrier safety data to the ISS-2 clients and SAFETYNET via the subscription process.
Flow 9. CVIEW via CDM sends inspection reports (IRs) recorded from ASPEN to Blizzard. (SAFER can also perform this function depending on whether ASPEN interfaces to CVIEW or SAFER.)
Flow 10. Blizzard forwards IRs to SAFETYNET 2000.
Flow 11. Other State Safety Data Sources send compliance review (CR), crash, enforcement, and manual IRs to SAFETYNET.
Flow 12. SAFETYNET sends CRs, crash, and enforcement data to MCMIS/SAFETYNET Gateway (MSG), and manual IRs to SAFER.
Flow 13. MSG sends CRs, crash, enforcement, and IRs to MCMIS via File Transfer Protocol (FTP).
Flow 14. MCMIS sends CRs, IR facsimiles, CRASHFAC, Enforcement, Carrier Profile, F-Number Reports, and Management Reports to MSG via FTP.
Flow 15. The MSG forwards data from MCMIS to SAFETYNET.
Flow 16. MCMIS sends SAFER carrier snapshots weekly.
Flow 17. Via the subscription process, SAFER transmits safety snapshot data to CVIEW.
Flow 18. Safety snapshot data are forwarded by CVIEW to a ROC.

3.2.2 Alternative CVIEW Implementation Approaches

A variety of options for achieving CVIEW Level 1 functionality is currently being explored by FMCSA and the states. The alternative CVIEW implementation approaches include:

- Use of SAFER functionality rather than deploying a state CVIEW (referred to as the “SAFER option”)
- Joint development of a “Regional CVIEW” by states in the same geographic area
- Use of alternative data exchange standards.

3.2.2.1 SAFER Option

Planning for SAFER and CVIEW began in 1996; many system capabilities and state business practices have changed since then. Originally, CVIEW was created for:

- Storage of intrastate snapshots (at the time, most states weren't considering assigning USDOT numbers)
- Data control (some states were reluctant to let their intrastate and credentialing data out of their control)
- Credentialing data (during the early days of SAFER, it was not designed to hold credentials flags or data)
- Performance (it wasn't clear whether SAFER could support direct connections to potentially dozens of ASPEN and screening systems in all states)
- State-specific data (states felt they had need of specific fields that were not in SAFER)
- LSIs (CVIEW provided a mechanism for developing custom interfaces to state legacy systems).

SAFER can store carrier and vehicle intrastate data, provided that the USDOT number is used as the primary carrier identifier. SAFER now stores credentialing check flags for IRP and IFTA. At this time, SAFER cannot store state specific data fields, nor does SAFER support any data exchange format other than EDI for snapshots and Application File Format (AFF) for inspection reports.

The state-led SAFER Option Working Group (SOWG), formed in October 2000, is currently working on demonstrating the feasibility of using SAFER to receive and distribute carrier and vehicle safety, credentialing, and transponder data for all interstate carriers and, where possible, for intrastate carriers, with or without an intermediate CVIEW. An Interface Control Document (Reference 43) that describes the requirements for data exchange formats (flat file and XML) and exchange methods between state systems and SAFER is in progress.

3.2.2.2 Regional CVIEW

A regional CVIEW acts as a catalyst to allow groups of states to accelerate their CVIEW implementation and simplify their access to credential information in neighboring states. LSI systems developed for each state will feed credential data directly into the regional CVIEW. The collected data will be designed to meet the roadside screening needs for the region as well as for the providing state. This information will then be uploaded to SAFER for use by states outside the region. Whenever the regional CVIEW is updated (either from the LSI systems or from SAFER), the updates will be replicated to the CVIEW databases in the subscribing states in the region. The State of Washington is developing a regional CVIEW that will act as a focal point for the collection of IRP and IFTA credential information from its neighboring states, Idaho and Utah.

3.2.2.3 Data Exchange Standards

The use of X12 EDI was initially required for the state-to-CVISN core infrastructure systems computer-to-computer interface. However, technology is changing rapidly, and XML has emerged as an alternative to X12 EDI. The use of an open interface standard, other than X12 EDI, is now permissible under the CVISN architecture. Some states that are not already committed to using X12 EDI are now exploring the use of XML. In particular, the Washington regional CVIEW will explore using XML as the data format for the state to SAFER interface.

3.2.3 SAFETYNET

SAFETYNET is a cooperative effort to share motor carrier information among states and FMCSA. The SAFETYNET system consists of software located in state and federal offices, a communications component that provides for the electronic transmission of data between these offices, and software that resides on an FMCSA mainframe computer to process the data and load it into the 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, FMCSA released SAFETYNET Version 9.0a, which integrated separate state and federal office functions into a single application. Prior to that, state offices primarily used the SAFETYNET system only.

The newest version of SAFETYNET, SAFETYNET 2000, was rewritten as a 32-bit Windows-based application that uses the SAFER system, i.e., the SAFER Data Mailbox (SDM), to send and retrieve information to/from the MCMIS via the MCMIS-SAFETYNET Gateway (MSG). The interface between the SAFETYNET system and SAFER for inspection report data is an application known as Blizzard that retrieves inspection reports from the SAFER Data Mailbox and transmits them to SAFETYNET. SAFETYNET also can retrieve carrier snapshots from a subscription mailbox on the SDM system separately from the Blizzard interface.

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 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.

The flow of information through SAFETYNET is depicted in Figure 3–6. The bolded text and lines in the Figure denote the relevant data flows into and out of SAFETYNET.

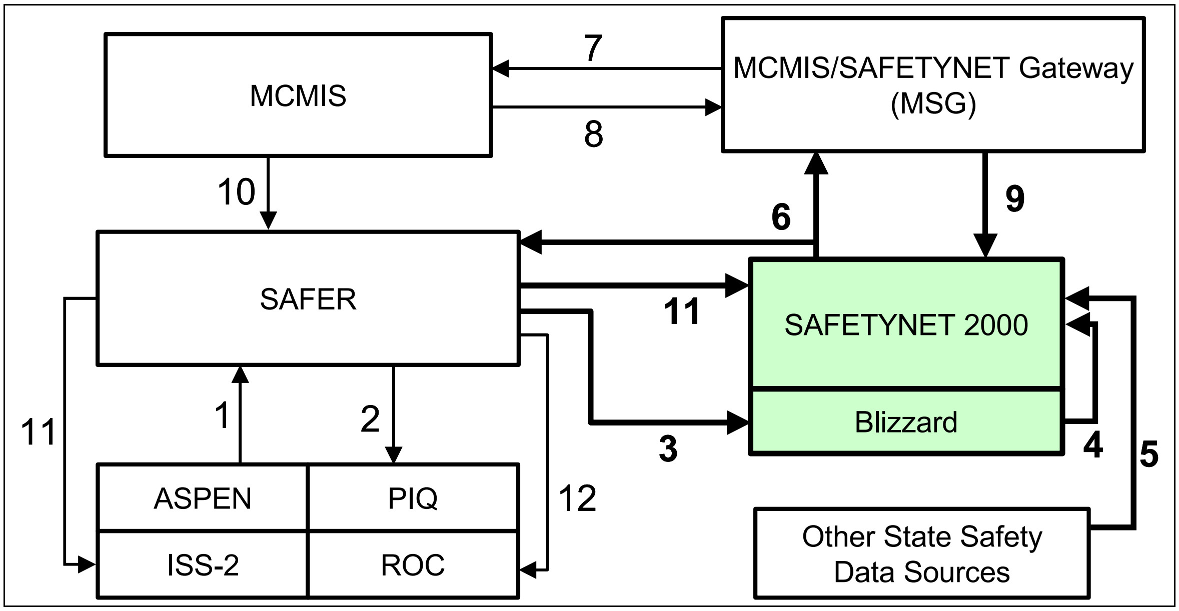


Figure 3–6. SAFETYNET Safety Information Flow

The individual safety information flow elements presented in Figure 3–6 are described below.

Flow 1. The vehicle and/or driver inspection data are transmitted from the roadside, via the ASPEN client or equivalent, to SAFER where it is stored for a 60-day period. It is also copied to the state safety data mailbox for retrieval by Blizzard.

Flow 2. One or more inspection reports are returned from SAFER to the roadside in response to a query from a user via the PIQ.

Flow 3. Blizzard retrieves inspection report data from the state safety data mailbox on the SAFER Data Mailbox (SDM) system.

Flow 4. Blizzard sends the inspection report data to SAFETYNET.

Flow 5. CR 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 6. SAFETYNET sends CRs, crash, and enforcement data to MCMIS/SAFETYNET Gateway (MSG), and manual IRs to SAFER.

Flow 7. CR data, crash data, enforcement data, and manually generated inspection reports are transmitted from the MSG to MCMIS.

Flow 8. MCMIS sends safety data updates to the MSG via FTP.

Flow 9. SAFETYNET receives the safety data updates from MCMIS via the MSG.

Flow 10. Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis.

Flow 11. Via the subscription process, SAFER transmits weekly updates of carrier safety snapshot data to the ISS-2 clients and to SAFETYNET.

Flow 12. SAFER could send snapshot data to a ROC; however, no ROC subscriptions are currently defined on the SAFER system.

3.2.4 State Roadside Systems

Many states today use a variety of software applications for exchanging safety information electronically for use at roadside inspection and weigh stations. The applications include ASPEN, the PIQ, the ISS-2, ROC and other applications such as the CAPRI application. Some of these systems also interact with national systems such as SAFER to access or exchange safety and other information about commercial vehicles and motor carriers. Information on acquiring/configuring these systems are available through FMCSA.

3.2.4.1 ASPEN

FMCSA has developed and is deploying pen- and laptop-based computer software and communications for conducting 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 and 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 such as SAFETYNET and from there into the national MCMIS. This is accomplished through either direct communications with SAFETYNET or via the use of the SAFER Data Mailbox, or the CVIEW Data Mailbox (with CVIEW Version 3), depending on the state's design configuration. Inspection data sent to SAFER are stored for a 60-day period during which any stored inspection can be retrieved via the PIQ application, which is described below.

Inspection data are used in the process of generating carrier snapshots and carrier profiles that are shared with other states via SAFER. Inspections, along with accident data, provide the basis for carrier safety performance measures, which are computed via the SafeStat algorithm on MCMIS. These safety performance data are used in the ISS-2 in ASPEN to provide an effective mechanism to ensure greater levels of safety on the nation's highways.

3.2.4.2 Inspection Selection System (ISS-2)

A companion to ASPEN is the ISS-2, an application that 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 (including SafeStat scores) on any of the nation's 800,000+ motor carriers based on the USDOT number.

Carrier census and safety data needed by the ISS-2 application are 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.

3.2.4.3 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 SDM, to query and retrieve past inspections based on power unit plate number and USDOT number. These "past" inspections are saved in SAFER for a 60-day period. Using PIQ, inspection reports can be queried and retrieved at the roadside within seconds of a user's request (see Figure 3–5 to see the relationship between PIQ and SAFER when a CVIEW system is involved).

3.2.4.4 Roadside Operations Computer (ROC)

A ROC is designed to perform the roadside electronic screening functions proposed in the 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 a ROC, using safety and credential snapshot data obtained from either SAFER (see Figure 3–7), CVIEW or its equivalent (see Figure 3–5).

3.2.4.5 Query Central

Query Central is a web-based intelligent query system that combines several existing query systems (ISS, CDLIS, PIQ, PRISM, L&I) and new data systems (Mexican CDL and carrier registration) into one system with a single, simple user interface with advanced drill-down and inferential functionality. It is a third generation query system that will access motor carrier safety information for State and federal law enforcement personnel. It is currently in Beta testing.

Query Central operates as a website on the FMCSA Intranet or via VPN on the Internet. It links directly to the SAFER and L&I databases, and via XML to CDLIS and the Mexican databases. Query Central is not shown on the diagrams in this guide. More information will be available at a later date via the CVISN website.

3.2.4.6 Roadside Systems Information Flow

The flow of information from SAFER through ASPEN, PIQ, ISS-2, and a ROC is depicted in Figure 3–7. The bolded text and lines in the figure denote the relevant data flows into and out of the roadside system.

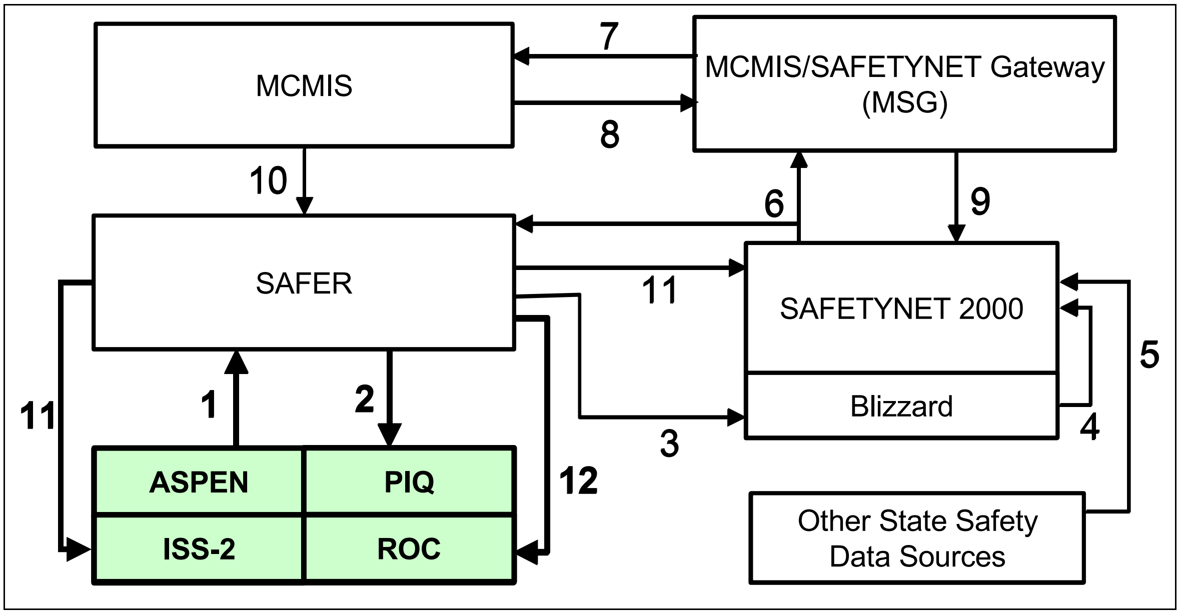


Figure 3–7. ASPEN, PIQ, ISS-2, ROC Safety Information Flow

The individual safety information flow elements presented in Figure 3–7 are described below.

Flow 1 The vehicle and/or driver inspection data are transmitted from the roadside, via the ASPEN client or equivalent, to SAFER where it is stored for a 60-day period. It is also copied to the state safety data mailbox for retrieval by Blizzard.

Flow 2 One or more inspection reports are returned from SAFER to the roadside in response to a query from a user via the PIQ.

Flow 3 Blizzard retrieves inspection report data from the state safety data mailbox on the SDM System.

Flow 4 Blizzard sends the inspection report data to SAFETYNET.

Flow 5 CR 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 6 SAFETYNET sends CRs, crash, and enforcement data to MCMIS/SAFETYNET Gateway (MSG), and manual IRs to SAFER.

Flow 7 CR data, crash data, enforcement data, and manually generated inspection reports are transmitted from the MSG to MCMIS.

Flow 8 MCMIS sends safety data updates to the MSG via FTP.

Flow 9 SAFETYNET receives the safety data updates from MCMIS via the MSG.

Flow 10 Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis.

Flow 11 Via the subscription process, SAFER transmits weekly updates of safety snapshot data to the ISS-2 clients and SAFETYNET.

Flow 12 SAFER could send snapshot data to a ROC; however, no ROC subscriptions are currently defined on the SAFER system.

3.3 CVISN Core Infrastructure Systems

3.3.1 Motor Carrier Management Information System (MCMIS)

The MCMIS is the national system that consolidates and processes motor carrier safety data from sources throughout the U.S. The system contains safety records in excess of 800,000 active interstate motor carriers, over 150,000 safety and CRs, 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 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 CRs 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 roadside to prioritize vehicles for inspection. 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 Interstate Commerce Commission (ICC) number, name and address, and summarized safety data from past inspections, CRs, crashes, and enforcement activities.

The flow of information through MCMIS is depicted in Figure 3–8. The bolded text and lines in the Figure denote the relevant data flows into and out of MCMIS.

The figures in this guide reflect current operations and interfaces with respect to MCMIS. The FMCSA is in the process of building a new version of MCMIS, referred to as "New MCMIS", which is scheduled for completion by September 2002. New MCMIS will be designed and built on a new platform comprised of a centralized Oracle database with a browser based front-end user interface. Existing legacy system functions and interfaces will continue to be supported with the New MCMIS platform; additional functionality will be added following the transition to the new system.

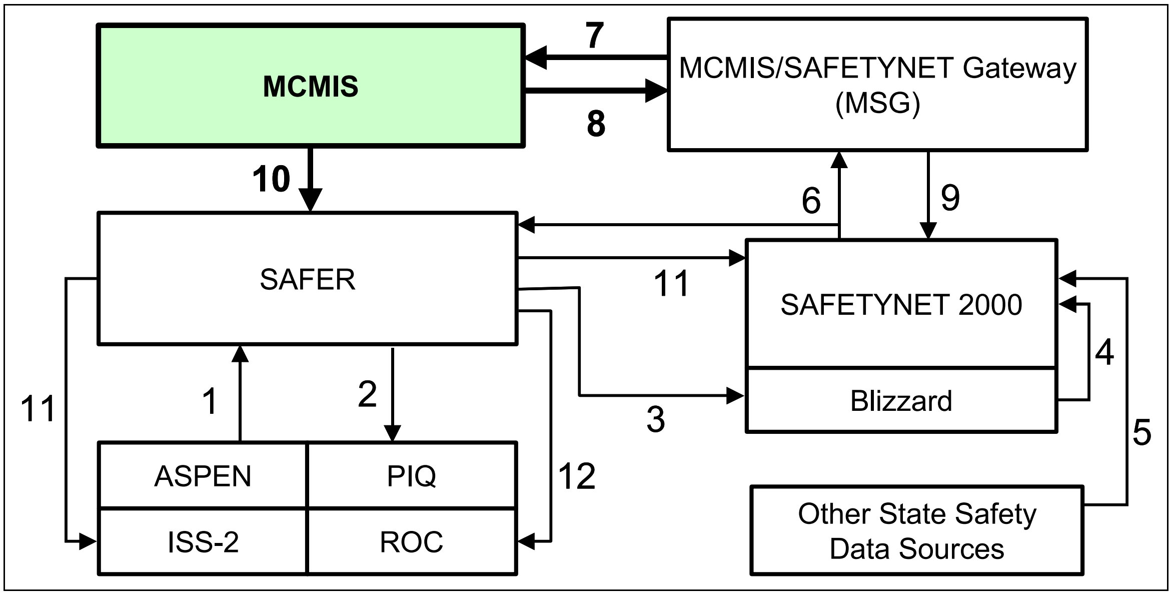


Figure 3–8. MCMIS Safety Information Flow

The individual safety information flow elements presented in Figure 3–8 are described below.

Flow 1 The vehicle and/or driver inspection data are transmitted from the roadside, via the ASPEN client or equivalent, to SAFER where it is stored for a 60-day period. It is also copied to the state safety data mailbox for retrieval by Blizzard.

Flow 2 One or more inspection reports are returned from SAFER to the roadside in response to a query from a user via the PIQ.

Flow 3 Blizzard retrieves inspection report data from the state safety data mailbox on the SDM System.

Flow 4 Blizzard sends the inspection report data to SAFETYNET.

Flow 5 CR 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 6 SAFETYNET sends CRs, crash, and enforcement data to MCMIS/SAFETYNET Gateway (MSG), and manual IRs to SAFER.

Flow 7 CR data, crash data, enforcement data, and manually generated inspection reports are transmitted from the MSG to MCMIS.

Flow 8 MCMIS sends safety data updates to the MSG via FTP.

Flow 9 SAFETYNET receives the safety data updates from MCMIS via the MSG.

Flow 10 Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis.

Flow 11 Via the subscription process, SAFER transmits weekly updates of safety snapshot data to the ISS-2 clients and to SAFETYNET.

Flow 12 SAFER could send snapshot data to a ROC; however, no ROC subscriptions are currently defined on the SAFER system.

The MCMIS application is currently being redesigned based on a client-server paradigm and a relational data model. The most significant impact of this redesign 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; the current system is 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 (SAFER)

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 (SDM) 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 3–9). This information includes identity data about carriers, vehicles, and drivers, summaries of past safety performance histories (inspections, accidents, and other data) and 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 and vehicle 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 for inspection based on the number of prior carrier inspections and the safety and credential history.

3.3.2.1 SAFER Interface and Data Transfer Protocols

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

The SAFER system supports two main functions, query and update, each of which dictates specific interface characteristics. Data to be interchanged can be formatted utilizing several different techniques: X12 EDI, SAFER/CVIEW Application Programming Interface Application File Format (SCAPI AFF), and RPC data marshalling.

The system also utilizes several data transfer protocols: Simple Mail Transfer Protocol/Post Office Protocol 3 (SMTP/POP3), FTP, and the Distributed Computing System Remote Procedure Call (DCS RPC). Note that these data formatting and data transfer techniques cannot be used interchangeably across all SAFER functions. Standard e-mail applications may be used to interact with the SDM via SMTP/POP3; however, the information must be organized, prior to e-mailing, according to specific conventions. In addition, if a state does not implement a CVIEW, the state's LSIs to SAFER must be compatible with the formatting and data transfer protocols maintained by SAFER. SAFER will not support all flat file formats. More information on SAFER interface specifications is provided in Reference 20.

3.3.2.2 SAFER Credential Information Flow

An overview of the SAFER design is shown in Figure 3–9. The flow of information through SAFER is depicted in Figures 3–10 and 3–11. The bolded text in the figures denotes the relevant data flows into and out of SAFER.

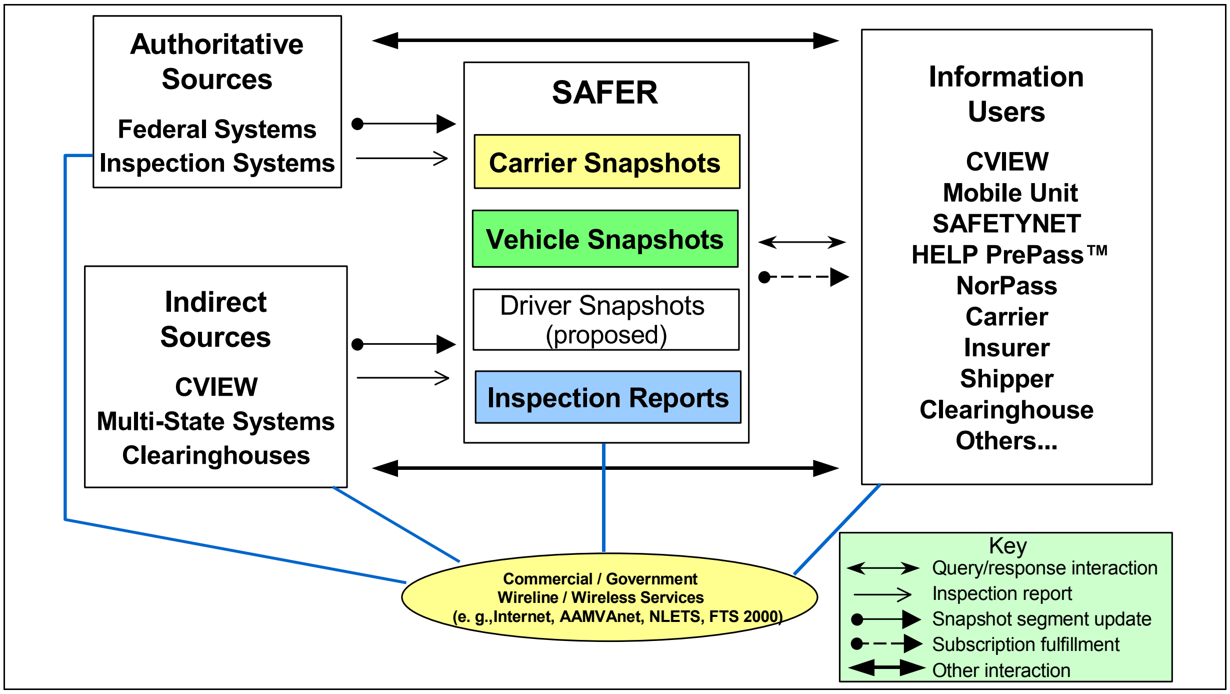


Figure 3–9. SAFER Design Overview

All states support systems for the administration of the IRP for commercial vehicles and the IFTA for interstate operations. The carrier licensing "authority" and insurance certification required by the former ICC remain in effect for most for-hire carriers (about 85,000 carriers).

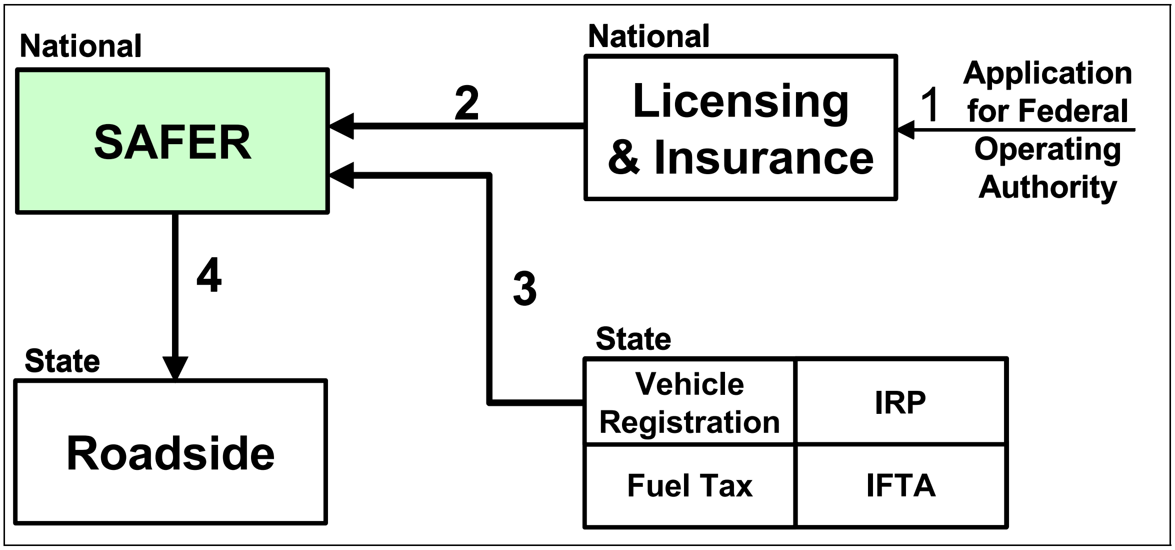


Figure 3–10. SAFER Credentials Information Flow

The individual credentials information flow elements presented in Figure 3–10 are described below:

Flow 1. L&I system tracks applications for federal operating authority and insurance.
Flow 2. L&I sends a summary of that information to SAFER for display on the SAFER web site and for incorporation into carrier snapshots.
Flow 3. State IRP/IFTA systems send registration and title 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.

Some method is needed to deliver similar **intrastate** data to roadside locations within a state. In most cases, there is no roadside access to intrastate vehicle registration, fuel taxation and permit data within a state. In terms of the credential data flow via SAFER, an underlying problem is that there is no uniform way of identifying intrastate carriers at a national level as there is with the USDOT registration for interstate carriers. Some states have state-specific intrastate carrier registration and carrier numbers; some states use USDOT numbers for all carriers. The solution recommended for CVISN Level 1 is for states to implement CVIEW or an equivalent system to handle information exchange for both interstate and intrastate carriers and vehicles. Figure 3–4 illustrates the relationship between credentials data exchange and SAFER when a CVIEW system is involved.

3.3.2.3 SAFER Safety Information Flow

The SAFER safety information exchange data flows are shown in Figure 3–11.

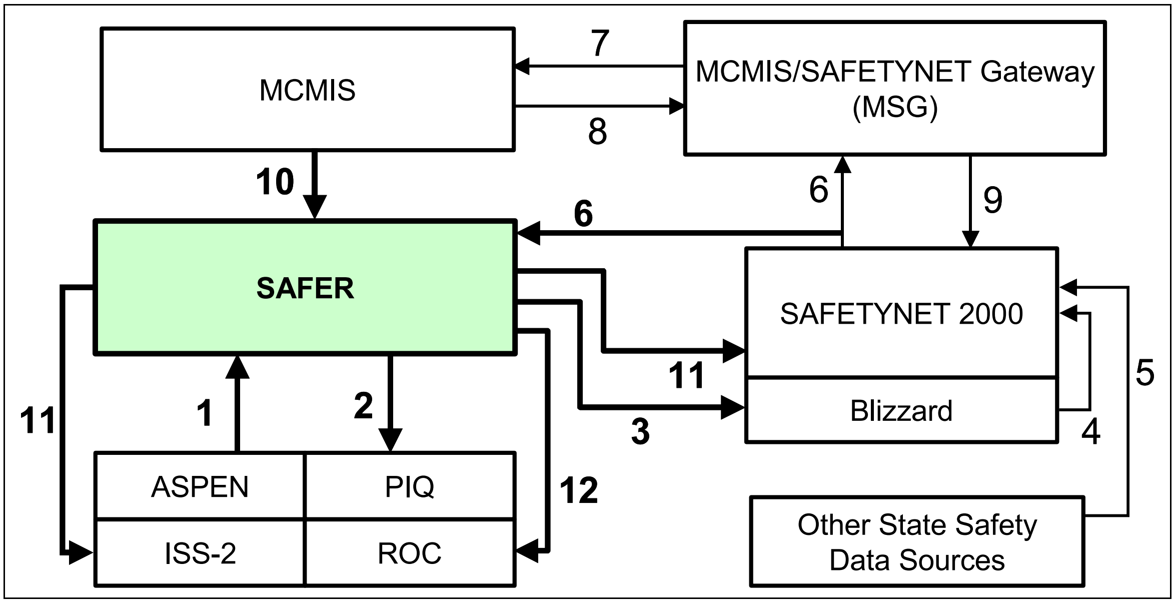


Figure 3–11. SAFER Safety Information Flow

The individual safety information flow elements presented in Figure 3–11 are described below:

Flow 1. The vehicle and/or driver inspection data are transmitted from the roadside, via the ASPEN client or equivalent, to SAFER where it is stored for a 60-day period. It is also copied to the state safety data mailbox for retrieval by Blizzard.

Flow 2. One or more inspection reports are returned from SAFER to the roadside in response to a query from a user via the PIQ.

Flow 3. Blizzard retrieves inspection report data from the state safety data mailbox on the SDM System.

Flow 4. Blizzard sends the inspection report data to SAFETYNET.

Flow 5. CR 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 6. SAFETYNET sends CRs, crash, and enforcement data to MCMIS/SAFETYNET Gateway (MSG), and manual IRs to SAFER.

Flow 7. CR data, crash data, enforcement data, and manually generated inspection reports are transmitted from the MSG to MCMIS.

Flow 8. MCMIS sends safety data updates to the MSG via FTP.

Flow 9. SAFETYNET receives the safety data updates from MCMIS via the MSG.

Flow 10. Based on the safety data received from SAFETYNET and the roadside, MCMIS generates safety snapshot data, a collection of interstate carrier census and summary safety information, which it sends to SAFER on a weekly basis.

Flow 11. Via the subscription process, SAFER transmits weekly updates of safety snapshot data to the ISS-2 clients and SAFETYNET.

Flow 12. SAFER could send snapshot data to a ROC; however, no ROC subscriptions are currently defined on the SAFER system.

3.3.3 Commercial Driver License Information System (CDLIS)

CDLIS was developed to support the Commercial Driver License (CDL) 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 Figure 3–12.

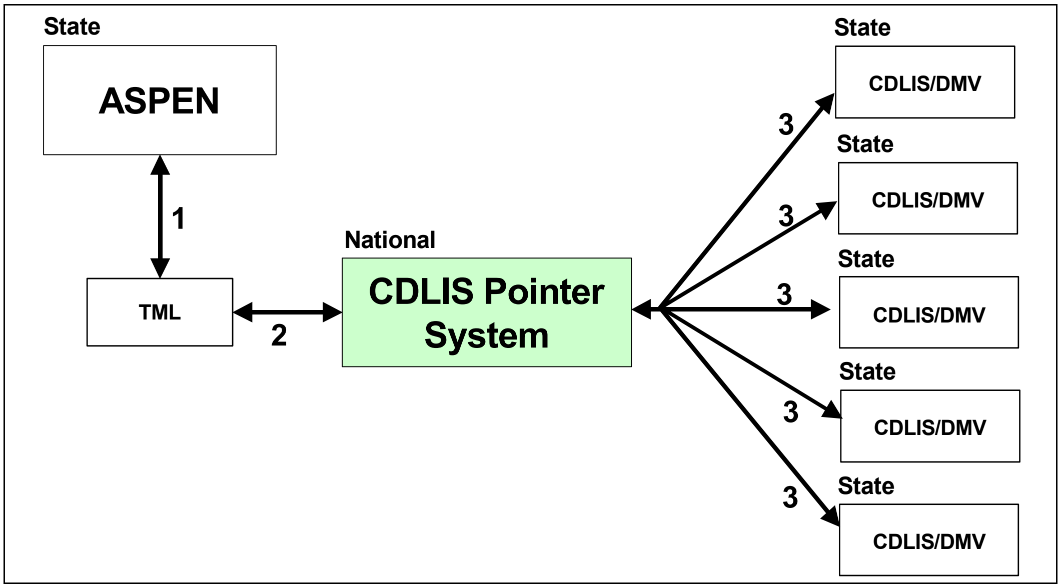


Figure 3–12. CDLIS Credential Information Flow

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.

Flow 2. TML uses the CDLIS Pointer system to determine which state's Department of Motor Vehicles (DMV) contains the requested information.

Flow 3. 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).

Users connecting directly to SAFER can also establish a web-based link to CDLIS via a TML Web server. For example, an ASPEN user, having connected wirelessly to SAFER via a Verizon Cellular Digital Packet Data (CDPD) network, is able to query CDLIS via a Web browser over the existing CDPD link to SAFER. Linkage from SAFER to TML is accomplished via the FTS2001 WAN. SAFER handles the routing from one network to another on behalf of the user, e.g., Verizon to FTS2001.

3.4 Data Interchange Standards

Use of American National Standards Institute (ANSI) Accredited Standards Committee (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 was developed to support the exchange of various types of safety reports, e.g., inspection reports. However, it is not currently supported in any of the federal safety systems such as SAFER and SAFETYNET. The following transaction sets currently support safety data exchange:

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

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

4. OPERATIONAL CONCEPTS AND SCENARIOS

The term “operational concept” is generally used to indicate “how a system is used in various operational scenarios.” The term “system” is used in a broad sense to include people and manual processes as well as sensor, control and automated information 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.

Operational concepts are related to the guiding principles developed by the stakeholder community. The concepts were derived by first analyzing user services that discuss how to improve commercial vehicle operations, then interpreting 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 and 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.

A core component of safety information exchange concepts is the “snapshot” – a collection of carrier, vehicle, and (in the 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 SAFER system and the state 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. Currently, the assembly and transmission of snapshots are accomplished using ANSI ASC X12 EDI TS 285. Alternative data formats, such as flat files or XML, are being explored by FMCSA and some states.

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 CVSA decal and electronic Out-Of-Service (OOS) 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 3.

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
- Ability to correct errors
- Determination of 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)
- CRs 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 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 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 errors.

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 4)

Jurisdictions support a standard set of criteria for inspection selection. The ASPEN inspection support system includes an algorithm called the ISS-2. 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 5)

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 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 SAFER/CVIEW Carrier, Vehicle and Driver Snapshots

The national SAFER system and its distributed version, the state CVIEW system or equivalent, manage information relating to the safety and credentials of motor carriers and vehicles. The information stored in both SAFER and CVIEW today is organized into two major types of data, carrier and vehicle. The design also accommodates a driver data type for future use. These data types are called snapshots since they provide summary information that is intended to give a quick picture of the safety performance history and basic credentials information. In addition, SAFER and CVIEW make available, but do not permanently store, more detailed information contained in reports.

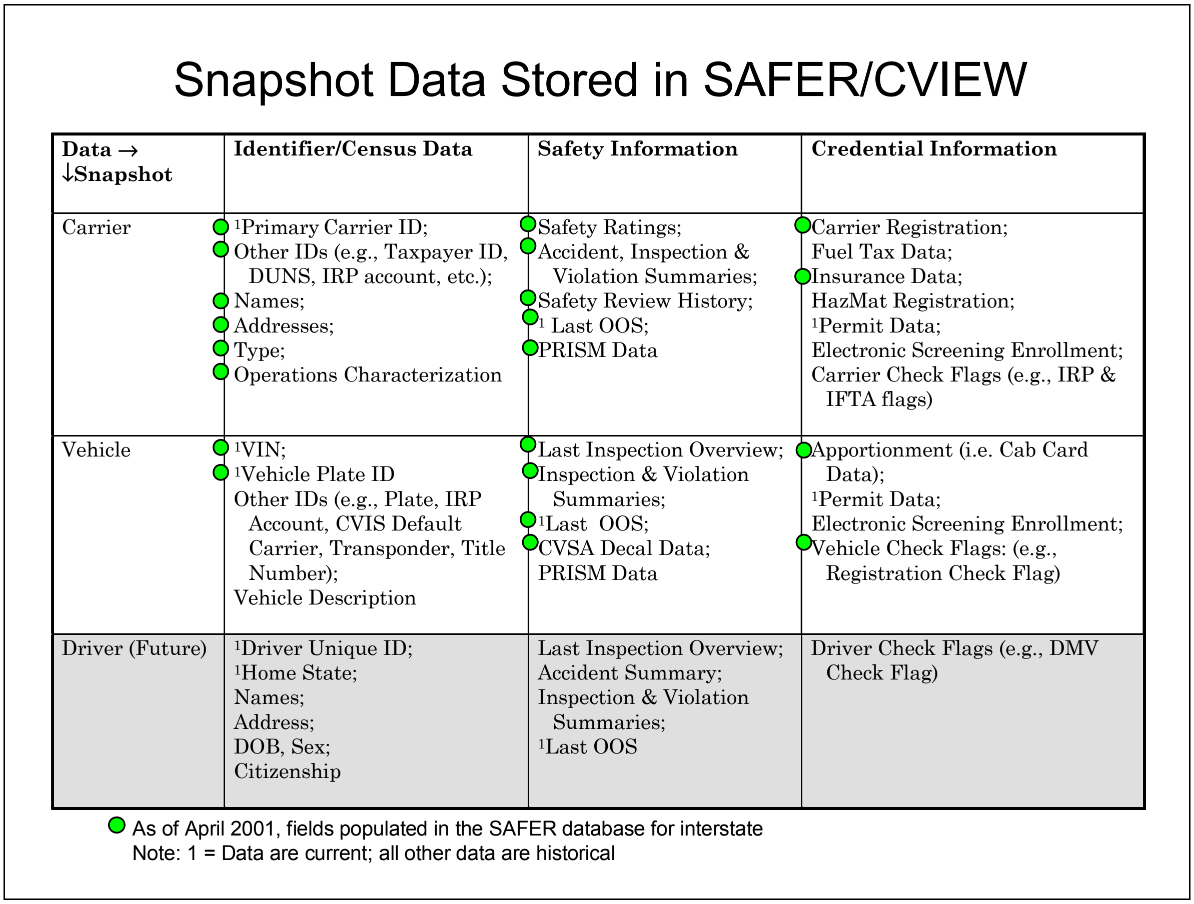
SAFER/CVIEW snapshots contain three general categories of information: identification/ census, safety, and credential. The identification/census section of the snapshot provides identifying numbers, names, addresses and other information that establishes the identity of the carrier or vehicle. The safety information includes selected statistics related to accidents, violations and inspections, as well as safety ratings, if they exist. The credential information is equivalent to the decals and paper documents carried today on commercial vehicles. The information included in the snapshots has undergone a process of review and refinement; additions are still possible as new uses are identified for snapshots.

The original purpose for the SAFER/CVIEW snapshots was to support electronic screening of vehicles at commercial vehicle check stations. In one operational scenario, on approach to the check station, identification information is read from the vehicle's transponder, and the vehicle is weighed. The identifiers are correlated with the SAFER/CVIEW snapshots: safety history, registration and authority data are checked, credentials check flags are examined, and weight is checked against legal limits. A decision then is made as to whether or not the vehicle should be pulled in. As the SAFER and CVIEW or equivalent systems are implemented, the value of snapshots for administrative processes becomes clear. Today, programs such as PRISM also plan to use snapshots to evaluate safety history in connection with vehicle registration.

4.2.1 Fundamental Principles Related to Snapshots

These principles guided the approach to the development of the SAFER and CVIEW or equivalent systems, and drove the contents proposed for snapshots.

There are three types of snapshots: carrier, vehicle, and driver (future).
These represent the three key entities in commercial vehicle operations. They are summarized in Figure 4–1.



Snapshot Data Stored in SAFER/CVIEW

Data → **↓Snapshot**	**Identifier/Census Data**	**Safety Information**	**Credential Information**

Carrier	● [1]Primary Carrier ID;
	● Other IDs (e.g., Taxpayer ID, DUNS, IRP account, etc.);
	● Names;
	● Addresses;
	● Type;
	● Operations Characterization
		● Safety Ratings;
		● Accident, Inspection & Violation Summaries;
		● Safety Review History;
		● [1] Last OOS;
		● PRISM Data
			● Carrier Registration;
			Fuel Tax Data;
			● Insurance Data;
			HazMat Registration;
			[1]Permit Data;
			Electronic Screening Enrollment;
			Carrier Check Flags (e.g., IRP & IFTA flags)

Vehicle	● [1]VIN;
	● [1]Vehicle Plate ID
	Other IDs (e.g., Plate, IRP Account, CVIS Default Carrier, Transponder, Title Number);
	Vehicle Description
		● Last Inspection Overview;
		● Inspection & Violation Summaries;
		● [1]Last OOS;
		● CVSA Decal Data;
		PRISM Data
			● Apportionment (i.e. Cab Card Data);
			[1]Permit Data;
			Electronic Screening Enrollment;
			● Vehicle Check Flags: (e.g., Registration Check Flag)

Driver (Future)	[1]Driver Unique ID;
	[1]Home State;
	Names;
	Address;
	DOB, Sex;
	Citizenship
		Last Inspection Overview;
		Accident Summary;
		Inspection & Violation Summaries;
		[1]Last OOS
			Driver Check Flags (e.g., DMV Check Flag)

● As of April 2001, fields populated in the SAFER database for interstate
Note: 1 = Data are current; all other data are historical

Figure 4-1. Snapshot Data Stored in SAFER/CVIEW

SAFER manages interstate snapshots.
The SAFER system was created to facilitate the exchange of carrier safety information among jurisdictions. The system has been extended to also provide credential summaries for interstate carriers, and to provide safety and credential summaries for interstate vehicles and drivers.

As part of ongoing efforts to improve SAFER, the SAFER Option Working Group (SOWG) is looking at ways to include intrastate data as well as interstate data as an alternative to developing and maintaining CVIEWs in individual states.

The state CVIEW (or equivalent) assembles and maintains the credentials portion of interstate snapshots and assembles and stores intrastate snapshots. The CVIEW or equivalent system provides for the electronic exchange of:

- interstate carrier and vehicle credential data between state source systems and SAFER
- intrastate carrier and vehicle safety and credential data between state source systems and users

Snapshots were primarily designed to support roadside electronic screening; many other uses have emerged. Congress mandated that carrier safety information be provided to roadside check stations as part of an initiative to improve safety in commercial vehicle operations. As snapshots were extended to include credentials information, their utility for other applications also grew. For example, PRISM states intend to use snapshots to check the carrier's safety status before renewing vehicle registration.

While carrier and vehicle snapshots are currently well defined and being used in many ways, driver snapshots remain conceptual. Administrative concerns, particularly regarding privacy, along with the technology currently in use, such as transponders and the communications infrastructure supporting roadside users, limit the availability of driver data. However, screening based on the driver may prove to be effective in improving safety. CVISN will continue to evaluate whether roadside screening based on driver license status can provide a cost-effective benefit when used in addition to screening based on the vehicle and carrier.

Snapshots are routinely distributed according to subscription criteria. A subscriber may set snapshot content-driven criteria for which snapshots should be provided by SAFER/CVIEW to that user. For example, a roadside site in Kentucky may choose to receive snapshots for all carriers based in Kentucky, plus those based in Tennessee, Virginia, Ohio, Indiana, Missouri, Illinois, North Carolina, and West Virginia.

Snapshots are also available for near-immediate response to a query. An occasional user of snapshots may request them one at a time. Or, a regular subscriber system may request a snapshot that is not covered by its subscription criteria.

Authoritative sources contribute specific segments of data proactively to snapshots, sometimes via indirect source systems. So that snapshots contain accurate information, sources of record (a.k.a. "authoritative sources") provide snapshot inputs to SAFER and CVIEW. Not all authoritative sources must be connected directly to SAFER/CVIEW to feed information to the snapshots.

Snapshots contain summary safety data, plus the equivalent of decals and paper documents carried on commercial vehicles today. As technology allows movement away from paper documents and towards paperless vehicles, snapshots provide information equivalent to the "papers" carried on commercial vehicles today, but in electronic form that computers can process. These electronic equivalents to documents will allow mainline electronic screening for safe and properly credentialed vehicles.

Snapshot data are stored in SAFER and CVIEW. SAFER and CVIEW store snapshot data for two reasons: to provide immediate response to a query, and to prevent SAFER/CVIEW from imposing undue data access/refresh burdens on authoritative sources. The design goal for a query response is ten seconds or less, 90 percent of the time; this goal does not account for dial-up time assuming that communication mode is selected. This also assumes that a single record is returned as opposed to an aggregate response. If SAFER/CVIEW had to construct a complete snapshot from scratch every time any data in the snapshot changed, then all of the data source systems for that snapshot would be queried every time any item in the snapshot changed. The underlying motivation for the snapshot concept is that data from a variety of sources should be made available to other systems to support near-real-time processing demands. To allow such quick response, snapshots are stored by the systems that provide them.

SAFER and CVIEW do not store copies of data readily available to SAFER/CVIEW users from other on-line systems. Replication of data is undesirable, and should be avoided unless the information is not readily available (i.e., when needed and according to user timeliness requirements) to those authorized users who need the data.

4.2.2 Operational Concepts Related to Snapshots

The snapshot user and snapshot builder perspectives imply these operational concepts:

Carriers, vehicles, and drivers may operate as intrastate or interstate entities. When carriers and vehicles are registered, the jurisdictions in which they intend to operate are specified.

SAFER provides snapshots on interstate operators to authorized users. SAFER is responsible for managing the snapshot data for interstate carriers, vehicles, and drivers (future), and for providing the data only to authorized users.

SAFER snapshots are provided to users based upon subscription or interactive request. Each user sets subscription criteria. The normal means of snapshot distribution is based on the subscription lists. Subscription criteria are based on certain data contained in the snapshots. Subscribers can also define the change criteria that cause an updated version of a snapshot to be sent to them. For instance, some roadside site may choose not to use stolen and junked vehicle flags from the snapshots because it has some other means to access that information. In that case, the subscription criteria for that site could filter out any snapshot updates that might occur only because of changes in those flags. Carrier subscriptions may be established to generate all carriers in a given state or states, all active carriers nationally or by specific USDOT number. The subscription is filled when the snapshot is updated. Vehicle subscriptions may be established for vehicles registered in a given state or states.

By including the data equivalent to the decals and paper documents carried on commercial vehicles today as part of the snapshots, SAFER supports the notion of the paperless vehicle. Under the “paperless vehicle” concept, drivers will no longer have to carry “hardcopy” evidence of the credentials for themselves, their vehicle, or the associated carrier. Instead, roadside enforcement officers will be able to check their credentials by a look-up in the infrastructure, based on some standard identifiers. Snapshots are an early step towards providing rapid access to basic credentialing information electronically.

MCMIS provides safety data to SAFER for interstate carriers. MCMIS is the primary source of safety data about interstate carriers today, and will continue to be so. State SAFETYNET systems update MCMIS with safety information collected at roadside sites. Since MCMIS is not set up to handle a large volume of requests for specific data, SAFER will provide summaries of the data stored in MCMIS to authorized users as part of the carrier snapshots.

The state CVIEW usually acts as the single point of contact within the state for providing interstate snapshot segment inputs to SAFER, and for retrieving interstate snapshots from SAFER for users within the state. State information systems are usually the authoritative sources for data contained in snapshots. Each state’s information systems are configured uniquely. To make the connection between states and SAFER simple, the recommended implementation option is to have the CVIEW collect inputs from the state systems and forward those snapshot segments to SAFER. Likewise, the state CVIEW will subscribe to SAFER (based on criteria that cover all of the state’s snapshot needs) to receive snapshots for interstate operators. The snapshot views CVIEW gets from SAFER must cover all the data items needed by in-state systems.

Some authoritative sources not equipped to handle a high volume of information requests send check flags to CVIEW/SAFER. The check flags are based on criteria that are common across jurisdictions. Each authoritative source sets their flag proactively. Check flags are used to indicate recent activity, especially negative actions regarding credentials. Instead of trying to maintain the latest credentials status in the SAFER snapshot, source systems send CVIEW/SAFER a check flag that acts as a warning to the receiving snapshot user to check with the authoritative source. The authoritative sources that choose to use this approach are responsible for sending check flag updates to CVIEW/SAFER proactively. Updating proactively means that the source system determines when it is necessary to send CVIEW/SAFER new information, and only updates the records that have changed. Generally, previously existing records in CVIEW/SAFER that have been updated are replaced.

The state CVIEW assembles and stores snapshots for intrastate carriers, vehicles, and drivers. As SAFER does for interstate carriers, vehicles, and drivers (future), the state CVIEW assembles and stores snapshots for intrastate operators. This implies that the state CVIEW interacts with all information systems in the state that are associated with commercial vehicle intrastate safety and credentialing activities. If all those systems connect to CVIEW, then they can exchange information with each other via the CVIEW snapshots.

The state CVIEW provides snapshots to roadside sites and other users within the state. As the source of intrastate snapshots, it is natural for CVIEW to be the distribution agent for intrastate snapshots. Since CVIEW also acts as the interface between the state and SAFER, it is a natural distribution agent for the snapshots that SAFER provides (i.e., interstate snapshots). The state CVIEW will distribute snapshots to state subscribers according to their unique criteria. If a user system within the state needs another snapshot, it will make the request to CVIEW, which will pass the request to SAFER, if necessary, and return the desired snapshot to the requesting system.

SAFER will provide support for retrieving recent inspection reports. If a SAFER/CVIEW user needs inspection information beyond that provided in the snapshot, a "past inspection query (PIQ)" may be issued to SAFER or CVIEW. SAFER retains inspection reports for 60 days; inspection reports are not stored in CVIEW. The state CVIEW or equivalent will pass the request for an inspection report on to SAFER. Authorized personnel could choose to go directly to the source system (MCMIS) for the information rather than to CVIEW or SAFER, in cases where this capability exists.

Snapshot users should always check with the authoritative source prior to any enforcement action. SAFER and CVIEW are not authoritative sources for any information. They are systems that provide information from a variety of sources to streamline roadside (and other) operations. Whenever enforcement action is to be taken, users should check with the authoritative source to verify the accuracy of the information on which the action is to be based.

4.3 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 updating snapshots with credential data are included in the *CVISN Guide to Credentials Administration*, Reference 6.

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 in Section 4.3.1 is presented in Figure 4–2 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 lines labeled numerically represent a set of flows that occur in the order indicated; the lines labeled with letters represent flows that are periodic in nature and have no specific precedence. 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 using SAFER, ASPEN V2, and SAFETYNET 2000. In this example, the state has a CVIEW that serves as the within-state interface to SAFER and ASPEN.

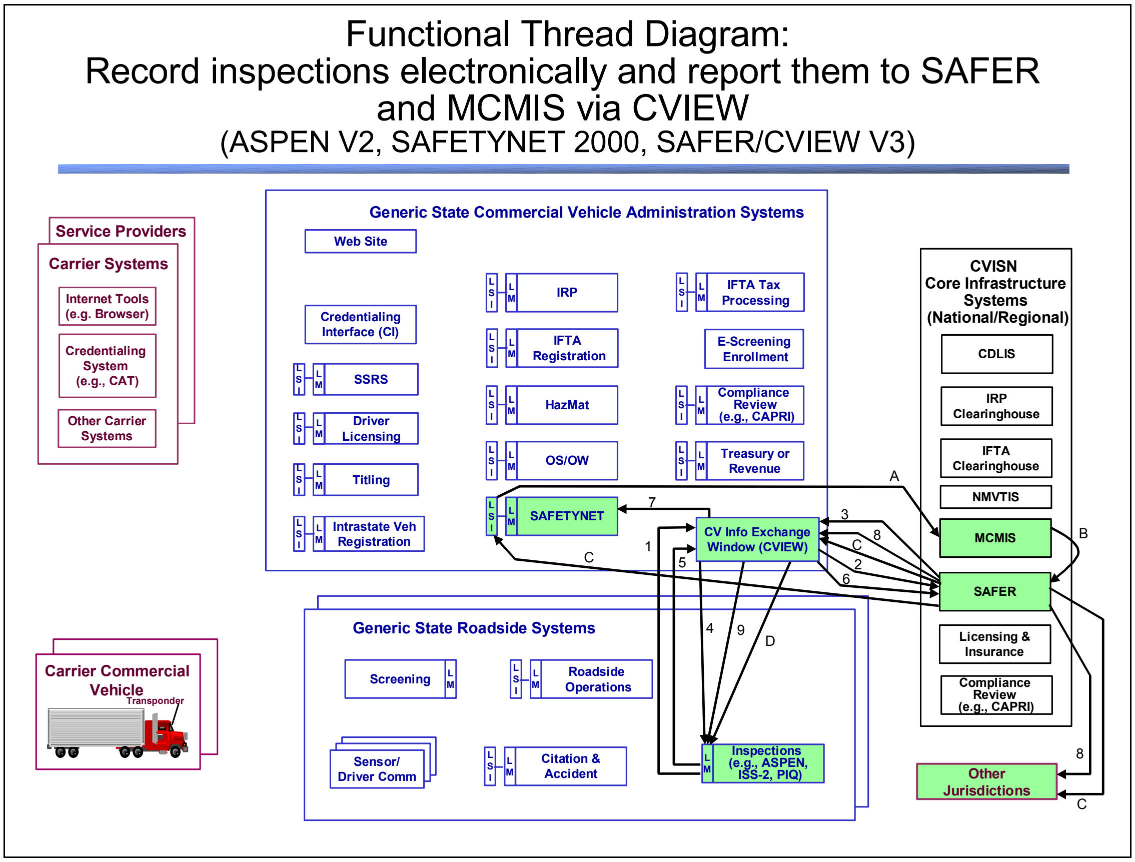

Functional Thread Diagram:
Record inspections electronically and report them to SAFER and MCMIS via CVIEW
(ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Generic State Commercial Vehicle Administration Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
CV Info Exchange Window (CVIEW)
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
Other Jurisdictions
Carrier Commercial Vehicle
Transponder
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
L S I
L M
1
2
3
4
5
6
7
8
9
A
B
C
D

Figure 4-2. Functional Thread Diagram: Record Inspections

4.3.1 Example Operational Scenario: Record Inspections Electronically and Report Them to SAFER and MCMIS (ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)

1. An enforcement officer, using the PIQ, issues a query to CVIEW’s input mailbox in the CDM, for all inspection reports relating to a particular carrier. The PIQ is in AFF.

2. CVIEW passes the query to SAFER, via a Remote Procedure Call (RPC).

   Note: All queries are passed to SAFER where inspection reports are stored for a 60-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.

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 in AFF to CVIEW's input mailbox in the CDM.

6. The CVIEW passes the inspection report to SAFER, via RPC, for 60-day storage.

7. CVIEW sends the inspection report in AFF to SAFETYNET 2000 via Blizzard mailbox in the CDM. Blizzard retrieves the inspection report from its CDM mailbox and passes it to SAFETYNET 2000.

8. 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.

9. CVIEW forwards vehicle snapshots in AFF to ISS-2 via their subscription mailboxes in the CDM.

A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the MCMIS/SAFETYNET Gateway.

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 to CVIEWs, and in AFF to SAFETYNET).

D. CVIEW updates its stored snapshots with carrier snapshot segments it receives from SAFER. CVIEW forwards carrier snapshot views in AFF to ISS-2 via their subscription mailboxes in the CDM.

> 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 scenarios are grouped in terms of safety information exchange CVISN Level 1 capabilities. 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. FMCSA has developed a set of interoperability tests that address most of the scenarios listed. Please see the interoperability testing documents (References 7, 8, 9, 10, 11) for more information.

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

Report inspections using ASPEN or equivalent; ASPEN data sent to SAFER directly or indirectly
ASPEN sends inspection report to SAFER
ASPEN sends inspection report to SAFER via CVIEW
SAFER processes carrier snapshot request from ASPEN
ASPEN sends request for inspection report to SAFER
ASPEN sends request for inspection report to SAFER via CVIEW
CVIEW processes carrier snapshot request from ASPEN
Implementation of CVIEW or equivalent for connection to SAFER to exchange interstate carrier and vehicle snapshots among states
CVIEW processes carrier snapshot updates from SAFER
CVIEW processes vehicle snapshot updates from SAFER
CVIEW processes carrier snapshot updates to SAFER
CVIEW processes vehicle snapshot updates to SAFER
Implementation of CVIEW or equivalent for exchange of intrastate and interstate data within the state
CVIEW processes carrier snapshot updates to Roadside Operations
CVIEW processes vehicle snapshot updates to Roadside Operations
CVIEW processes vehicle snapshot update from legacy credential product
CVIEW processes carrier snapshot update from legacy credential product
CVIEW processes vehicle snapshot request from legacy credential product
CVIEW processes carrier snapshot request from legacy credential product
CVIEW processes vehicle snapshot request from Roadside Operations
CVIEW processes carrier snapshot request from Roadside Operations

This Page Intentionally Blank

5. CRITICAL DECISIONS

In this chapter, some of the decisions critical to successful implementation of CVISN Level 1 safety information exchange are identified. The chapter is intended to serve as a checklist to remind states about some of the major planning and design issues that should be settled as early in the process as possible. Other decisions may be just as critical as these for a given state.

5.1 Design Decisions

The decisions listed below are categorized as "design" because they affect the design approach significantly. These decisions also affect planning, but to a lesser extent.

Which CVIEW development approach will the state pursue? Will the state implement the FMCSA-developed CVIEW or an equivalent system?

CVIEW is a distributed version of the federally-developed SAFER system. It is owned by and located in a state that chooses to use CVIEW as a data exchange mechanism. The state has the following options for implementing CVIEW functionality:

- Develop a CVIEW for the state
  - Adapt the Oracle-based FMCSA CVIEW software developed by JHU/APL and used by Maryland and Kentucky
  - Adapt the Oracle-based CVIEW software developed by a vendor for Minnesota
  - Adapt the Microsoft SQL-based CVIEW software under development by the State of Washington
  - Contract with a third party to provide the functionality of CVIEW
- Join other states in developing a "regional CVIEW"
- Use SAFER, and its future capability of receiving and exchanging intrastate data from MCMIS, instead of CVIEW

Will the state start with the generic FMCSA-developed model?

The FMCSA-developed model CVIEW 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 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 CVIEW model has the advantage of building on 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. Note that the FMCSA-developed model will not be updated after the release of SAFER/CVIEW Version 3, which is planned for Spring 2002. Future updates to a state's CVIEW based on this model will be the responsibility of the state. For available CVIEW documentation, visit the JHU/APL CVISN Web site at http://www.jhuapl.edu/cvisn

Another alternative would be to use a "CVIEW-like" system developed by another state (by starting with the FMCSA-developed model and modifying it) as the base and modifying it to satisfy state-specific needs. Minnesota and Washington have CVIEW systems that may be available for other states to use.

Implementing a "regional CVIEW" could be the most cost effective solution for a group of states. But it still requires one state in a region to implement a CVIEW. This approach also requires a way to replicate a copy of the CVIEW database to each of the subscribing states. Washington is currently implementing a regional CVIEW to support Idaho, Utah, and others. However, this is seen to be an interim solution until flat file and XML interfaces are supported by SAFER and the participating states can interface with SAFER directly via "xCVIEW", a Washington-developed version of CVIEW that supports flat file and XML interfaces.

Will the state use SAFER instead of implementing a CVIEW?

The state could decide to have its state-specific systems interface directly with SAFER, rather than incurring the expense of building a CVIEW. The state should take into consideration the following:

- Interfaces between a state's legacy system and SAFER would be limited to EDI and, potentially, a limited set of other selected standardized data definitions, file exchange formats and protocols.
- SAFER identifies carriers using the USDOT number. If the state wishes to store intrastate data in SAFER, the state would have to issue USDOT numbers to its intrastate carriers.
- SAFER does not have fields to support intrastate-specific data.

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 credentials data between state source/legacy systems, users, and SAFER
- Provide for the electronic exchange of intrastate carrier and vehicle safety and credentials data between state source systems and users
- Serve as the repository for a state-selected subset of interstate carrier and vehicle safety and credentials data
- Serve as the repository for a state-selected subset of intrastate carrier and vehicle safety and credentials data
- Provide inter- and intrastate carrier and vehicle safety and credentials 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.

What data formats will the state use in interfacing with SAFER?

Currently, EDI is the data format used for interfacing state systems to SAFER. However, flat file and XML interfaces are currently being prototyped as part of the SOWG efforts. A flat file or XML interface specification for uploading IRP and IFTA data to SAFER, and an XML interface specification for downloading carrier and vehicle snapshots from SAFER to a state system are being planned, with a target delivery date of the first quarter of 2003. The interface from ASPEN to SAFER is AFF and is not being changed. The interface from CVIEW to SAFER is expected to become Web-based in the future.

Does the state use or intend to use ASPEN for inspections?

ASPEN is a client system deployed in over 40 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 PIQ, allows any inspector throughout the country to retrieve inspections previously stored in the SAFER system for the most recent 60-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-2 algorithm and to upload electronically captured inspection reports. Although CVIEW Version 2 supports the download function, the upload function along with inspection retrieval capability via PIQ will not be supported until CVIEW Version 3. With Version 3 of CVIEW, ASPEN clients could interface exclusively with their state's CVIEW system to perform all of the functions now performed via the link to SAFER.

What systems in the state will provide snapshot segment updates?

This decision will be based on the types of information a state can and is willing to provide as segment updates to the snapshot data stored in its CVIEW or equivalent system. It will also depend on what information will be required at roadside sites within the state to support electronic screening, inspections, and other enforcement activities. An example of such a decision is as follows:

> 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 are transferred to an internal Maryland IRP workstation and then transmitted to and stored in their CVIEW system via an LSI using a flat file data exchange method. Upon receiving the data via the IRP LSI, CVIEW is configured to update the appropriate IRP data element in the vehicle snapshot for which the state is the authoritative source.

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

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 a 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 ISS-2 would require data to be sent to them using the “ISS-2 view.” The ISS-2 view supplies ASPEN clients only those data elements that are needed by the ISS-2 algorithm. See the Snapshot White Paper (Reference 3) for more detailed information about snapshot views. (Note that this white paper will be replaced by the View Summary Report, View Definition Report, and Schema Definition Report that will be available on the CVIEW V3 CD when it is released.)

5.2 Planning Decisions

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

Build or Buy?

One of the most important decisions the project team must make is the “build or buy” decision. The identification of what should be built and what should be purchased (hopefully “off the shelf”) is one of the first questions to be addressed in the planning process for the development of a system. This issue needs to be resolved 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 COTS products.

Will the state update current legacy systems or recompete/redevelop?

Sometimes a major project like implementing CVISN is the catalyst to reevaluate 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 4 for contact information. In addition, the PRISM processes should be considered when the top-level CVISN design for the state is being established.

What are the priorities and sequence for implementing capabilities?

For every state, some priorities and sequences for implementation make more sense than others do. Both design and cost factors should be considered when establishing baseline schedules. The relationship of CVISN activities to other state activities must also be considered. Further, 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 or 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 for "system integration" 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 V&V 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. In some cases, sole source contracting may not be an option since many states require competition whenever possible.

5.3 Funding and Contracting Decisions

These issues 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 Requests for Proposals (RFPs) be written to assure architectural conformance and interoperability?

5.4 Development Decisions

These issues 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?

6. REQUIREMENTS AND DESIGN GUIDANCE

The U.S. Congress has mandated that the implementation of ITS using Highway Trust Funds authorized by the Transportation Equity Act for the 21st Century (TEA-21) must be in conformance with the National ITS Architecture and Standards. Chapter 7, "How Do States Assure Conformance with the National ITS Architecture?" of the *Introductory Guide to CVISN* (Reference 17) provides an overview of the "Conformance Assurance Process." Conformance with the National ITS Architecture means that states will:

- Implement TEA-21
- Support key federal priorities:
  - Integration
  - Interoperability
  - Use of the National ITS Architecture and applicable standards
- Incorporate ITS into existing transportation planning and project design procedures
- Provide flexibility to states by emphasizing architecture and systems engineering process, rather than mandating use of the National ITS Architecture.

Broadly stated, for safety information exchange, conforming to the architecture means:

- Agreeing with the principles and following the guidance in the COACH Part 1 (Reference 2),
- Using the EDI standards and common identifiers as explained in the COACH Part 4 (Reference 14), and
- Conducting interoperability tests to demonstrate the criteria defined in the COACH Part 5 (Reference 8).

The *CVISN System Design Description* (Reference 15) illustrates the top-level requirements for safety information exchange, and shows the generic CVISN state design approach. The COACH Part 3 (Reference 16) 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.

As stated in Reference 17, the high-level definition of CVISN Level 1 with respect to safety information exchange is:

- Use of ASPEN (or equivalent) at all major inspection sites
- Connection to the SAFER system to provide exchange of interstate carrier and vehicle snapshots among states
- Implementation of the CVIEW system, or equivalent, 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 to the Architecture

In this section, various approaches to safety information exchange are presented. The examples do not exhaust the possibilities, but do represent a variety of choices that have been considered by early implementers.

The use of open standards is a key architectural concept in CVISN. It is important that states support the use of standards for data exchange between state systems and systems external to the state. At this time, the only standard data exchange method is X12 EDI. In particular, data exchange operations from SAFER to the state CVIEW, or its equivalent, should employ the use of X12 EDI transactions.

The CVISN architecture may be updated to include the use of additional standards, if recommended by a consensus of the stakeholder community and approved by FMCSA. These may include and the use of alternate data formatting standards such as the eXtensible Markup Language (XML). XML and/or flat file formats may be an option in the 2003 time frame; however, states should plan on EDI data exchange between the state and SAFER if they plan to interface with SAFER before March of 2003.

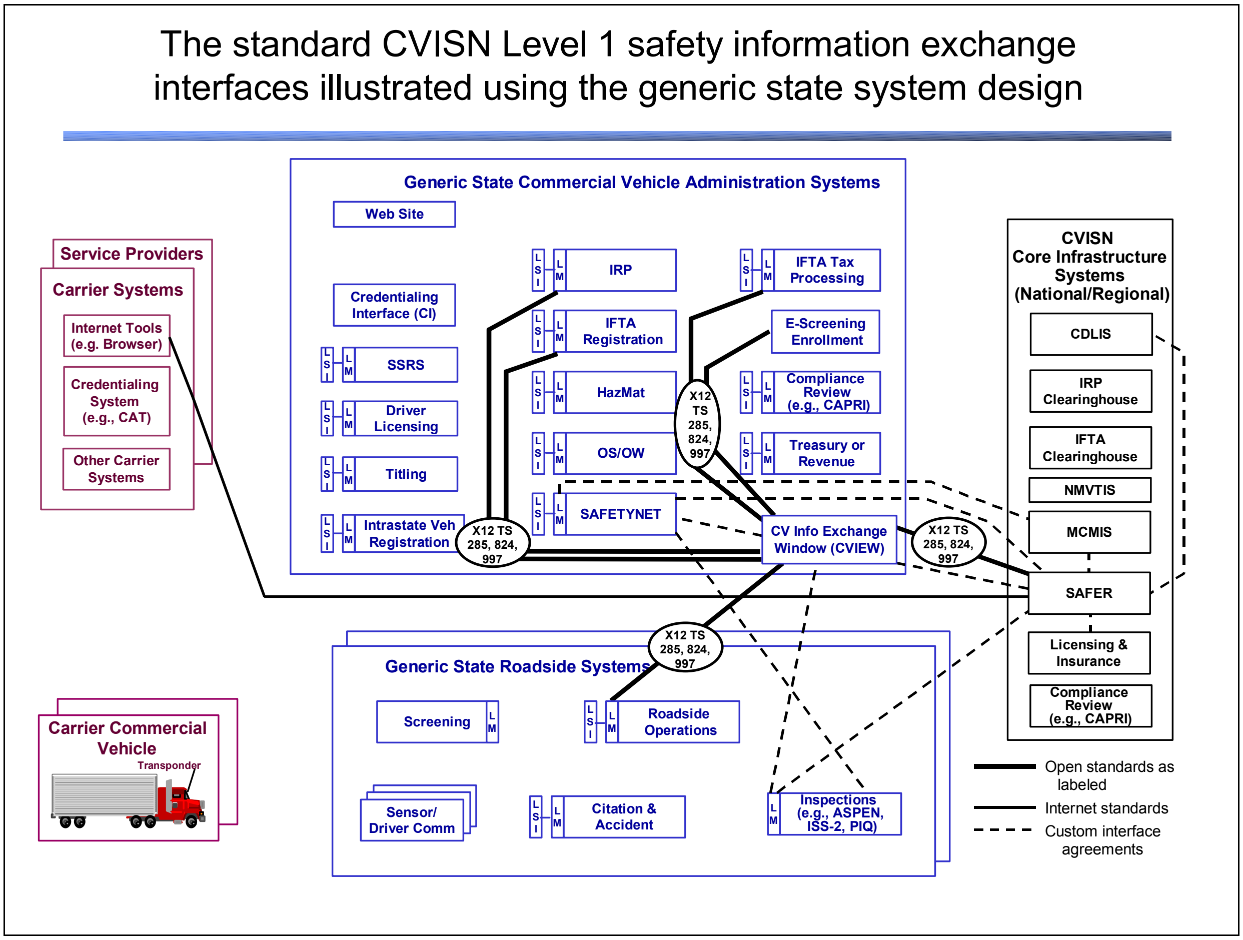
The EDI Transaction Sets (TS) associated with safety information exchange and supported by SAFER are:

- TS 285 Commercial Vehicle Safety & Credentials Information
- TS 824 Application Advice
- TS 997 Functional Acknowledgement.

Figure 6–1 and the following list summarize the interface requirements related to safety information exchange from the COACH Part 4 (Reference 14).

- 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 X12 EDI standard transactions (285, 824, 997). Alternatively, a state-specific flat file/LSI method could be used.
- To conform to 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 X12 EDI standard transactions (285, 824, 997).
- If a state chooses to use EDI internally to send snapshots to the roadside, a state's roadside system, e.g., a ROC, should be capable of requesting and receiving carrier and vehicle safety information from CVIEW, or its equivalent, via X12 EDI standard transactions (285, 824, 997). Alternatively, a state-specific flat file/LSI method could be used.

- To conform to 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 to the architecture, CVIEW or its equivalent, should be capable of submitting, requesting, and receiving inspection reports to/from SAFER via the existing CIA.



The standard CVISN Level 1 safety information exchange interfaces illustrated using the generic state system design

Generic State Commercial Vehicle Administration Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
CV Info Exchange Window (CVIEW)
X12 TS 285, 824, 997
LSI
LM
Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
Carrier Commercial Vehicle
Transponder
Open standards as labeled
Internet standards
Custom interface agreements

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

6.2 Design Guidance Related to ASPEN or Its Equivalent

Each state will have to decide whether to use the ASPEN client, developed by 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-2 algorithm (ISS-2), and for retrieving 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-2.

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 the 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 Transmission Control Protocol/Internet Protocol (TCP/IP) network communications
- The lag time the 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. 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 to/from SAFER, and downloads carrier ISS-2 subscription data to the ASPEN client, or its equivalent, via direct communications with the SAFER system. The inspection report, and carrier snapshot subscription and query transactions are performed using CIA and AFF data formatting methods, respectively. This approach is most suitable where:

- A state elects not to interface ASPEN with a CVIEW system, or its equivalent, and wants to support ASPEN data exchange with SAFER, or
- A state plans to interface ASPEN with a CVIEW system, or its equivalent, but the CVIEW is still in the process of being developed, and is not yet ready to provide data exchange support within the state.

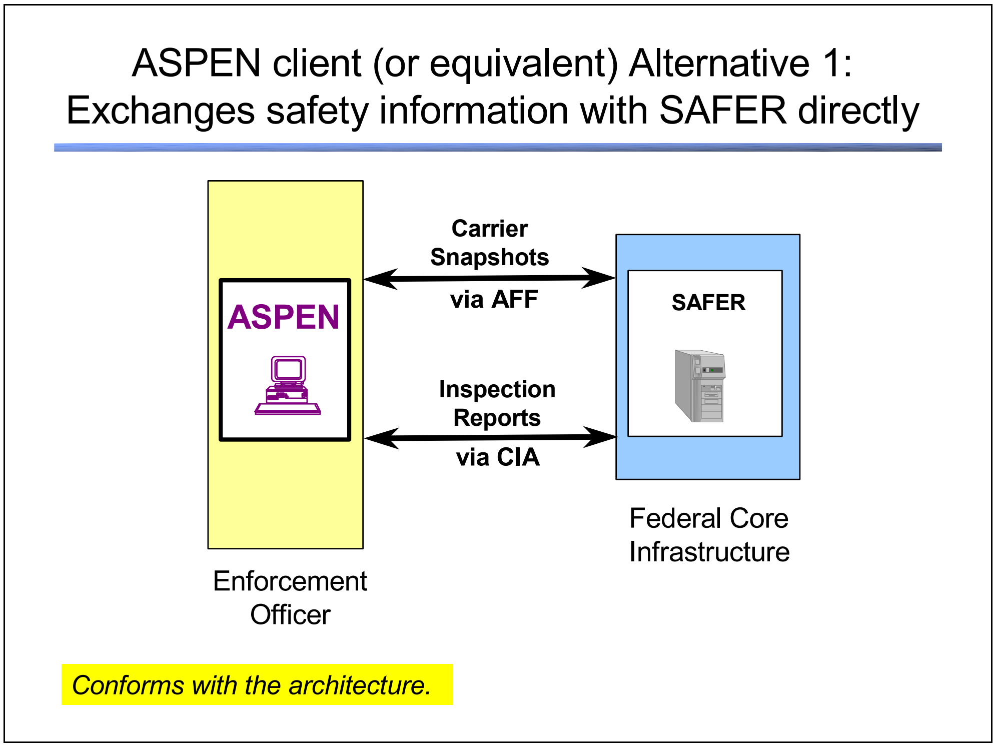
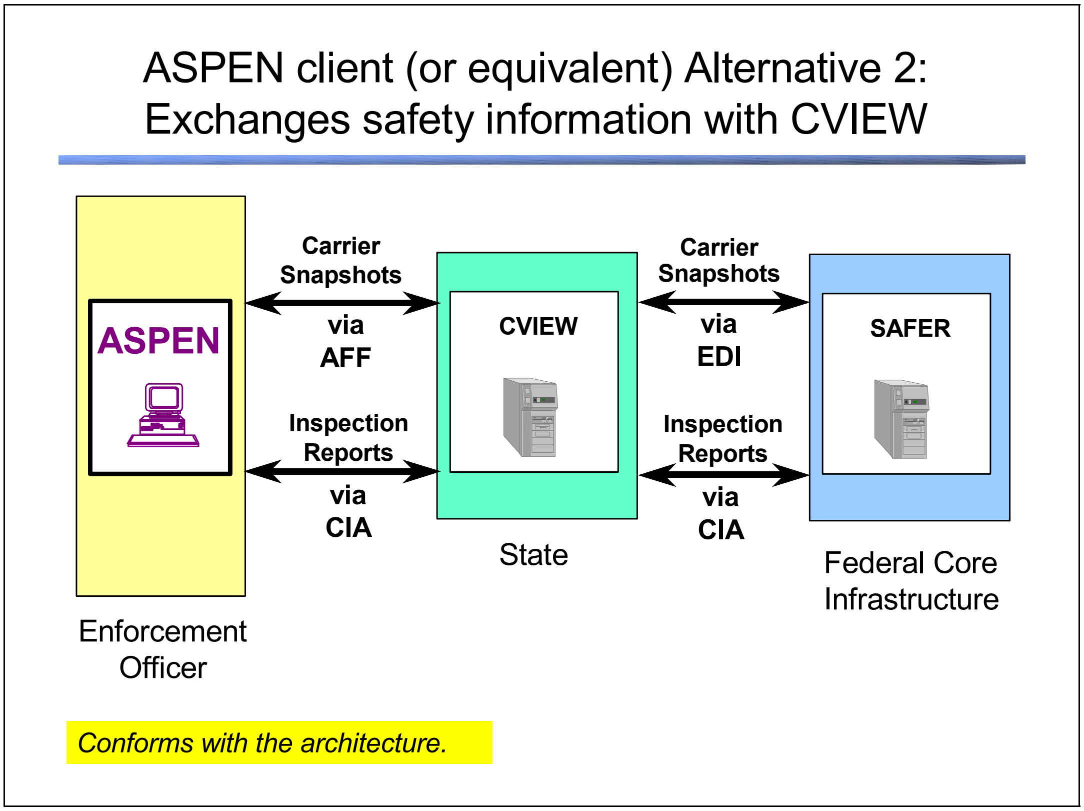

ASPEN client (or equivalent) Alternative 1:
Exchanges safety information with SAFER directly
ASPEN
Carrier Snapshots
via AFF
Inspection Reports
via CIA
SAFER
Enforcement Officer
Federal Core Infrastructure
Conforms with the architecture.

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-2 subscription data to 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 carrier subscription downloads and queries, are performed using CIA and AFF data formatting methods, respectively. Between CVIEW and SAFER, inspection report uploads and queries, and carrier subscription data, are exchanged using the existing CIA and EDI formatting methods, respectively.



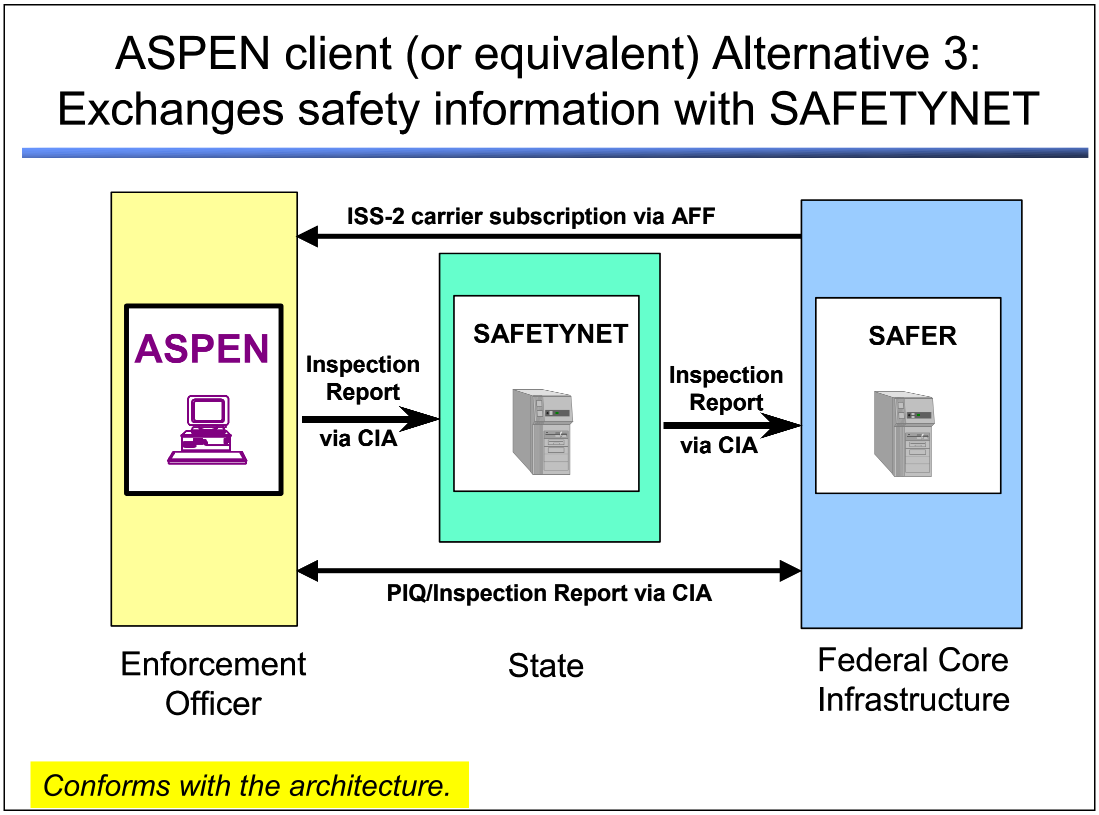
ASPEN client (or equivalent) Alternative 2:
Exchanges safety information with CVIEW

Conforms with the architecture.

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 of the SAFER and CVIEW software. Figure 6–3 represents the preferred architectural approach for uploading and downloading safety information from/to ASPEN or its equivalent. Note, however, that no federal support is planned for maintenance and/or upgrades to the FMCSA-developed CVIEW product after the delivery of Version 3.

In Figure 6–4, an enforcement officer, using ASPEN or its equivalent, sends inspection reports to the state's SAFETYNET 2000 system, which in turn uploads that information to SAFER using the existing CIA. The ISS-2 program (that is used in conjunction with ASPEN) allows the user to connect directly to SAFER to retrieve carrier snapshots from its SDM. The PIQ program (that is also used in conjunction with ASPEN) queries SAFER for previously completed inspections. Both ISS-2 and PIQ can be used independently of ASPEN, or work in tandem with ASPEN.



ASPEN client (or equivalent) Alternative 3:
Exchanges safety information with SAFETYNET

ISS-2 carrier subscription via AFF
ASPEN
Inspection Report via CIA
SAFETYNET
Inspection Report via CIA
SAFER
PIQ/Inspection Report via CIA
Enforcement Officer
State
Federal Core Infrastructure

Conforms with the architecture.

Figure 6–4. ASPEN Communicates with SAFER via SAFETYNET

6.2.2 Data Exchange Formats

ASPEN does not support safety data exchange via the use of 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 a CVIEW 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 18 for a detailed description of the SCAPI.

6.3 Design Guidance Related to CVIEW and State Systems

Each 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-2 algorithm via AFF and the upload and retrieval of inspection reports via the existing CIA to and from SAFER. (The FMCSA-developed CVIEW does not store inspection reports. Uploads and queries are passed to SAFER via RPC.)
- For the roadside operations computer, subscription download and online query of carrier and vehicle snapshots to support electronic screening operations via X12 EDI 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 X12 EDI standard transactions (285, 824, 997) or LSIs. XML or flat file interfaces with SAFER may be available in the CVISN Level 1 timeframe.

The choice of whether to use the existing FMCSA-developed CVIEW system, build/purchase an equivalent product, or use the SAFER option 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 and continuing maintenance efforts
- Assuming the work will be done in-house, the expertise of the state's IS staff in the areas of client/server software, relational database design and development, data formatting strategies, such as the use of X12 EDI, XML, and TCP/IP network communications
- The lag time the state is willing to tolerate before a CVIEW system is available to support the functions indicated 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 will exchange safety information with SAFER and other systems within the state. Aside from the issue of supporting all of the functions mentioned above, the state must make a design choice as to how to interface CVIEW with existing or new state systems, i.e., should CVIEW interface with state systems via EDI or the use of flat files via LSIs.

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 X12 EDI standard transactions (285, 824, 997). In many cases, this requires a modification to the state's legacy system(s) (shown as Legacy Modification or 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 those data via the subscription process using X12 EDI 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.

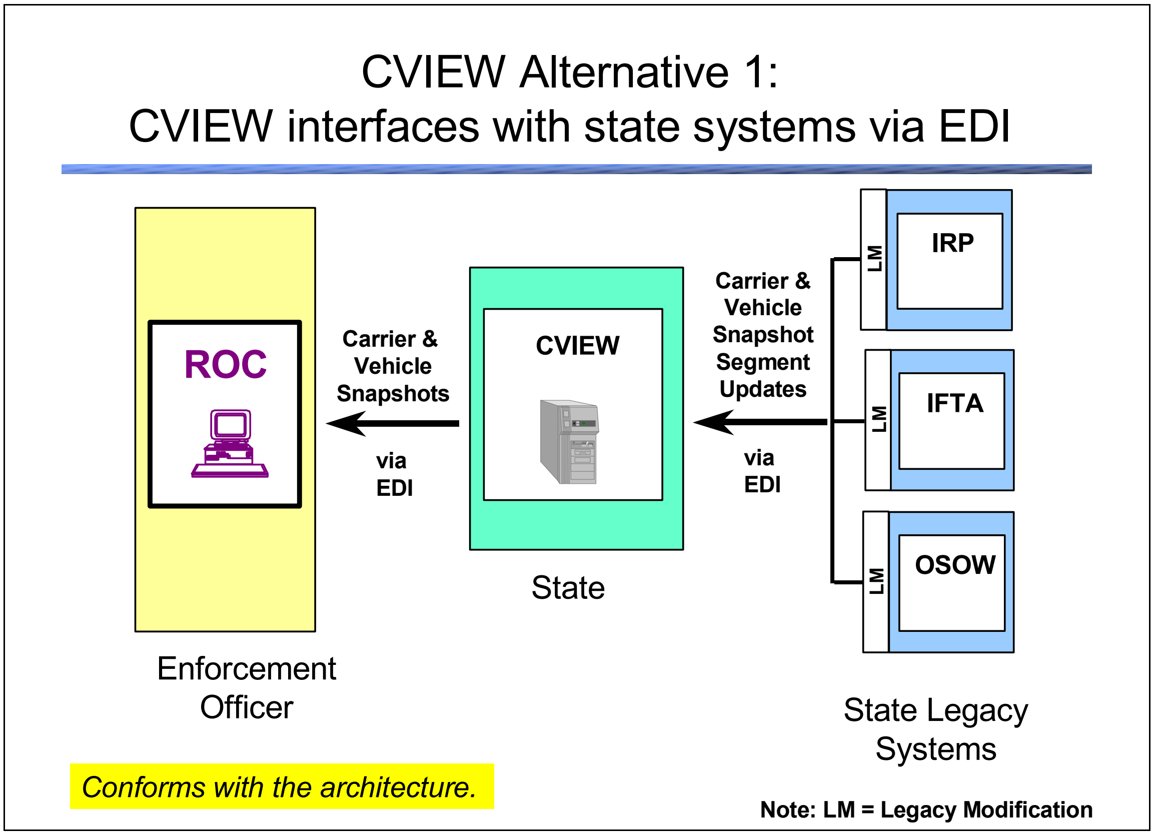
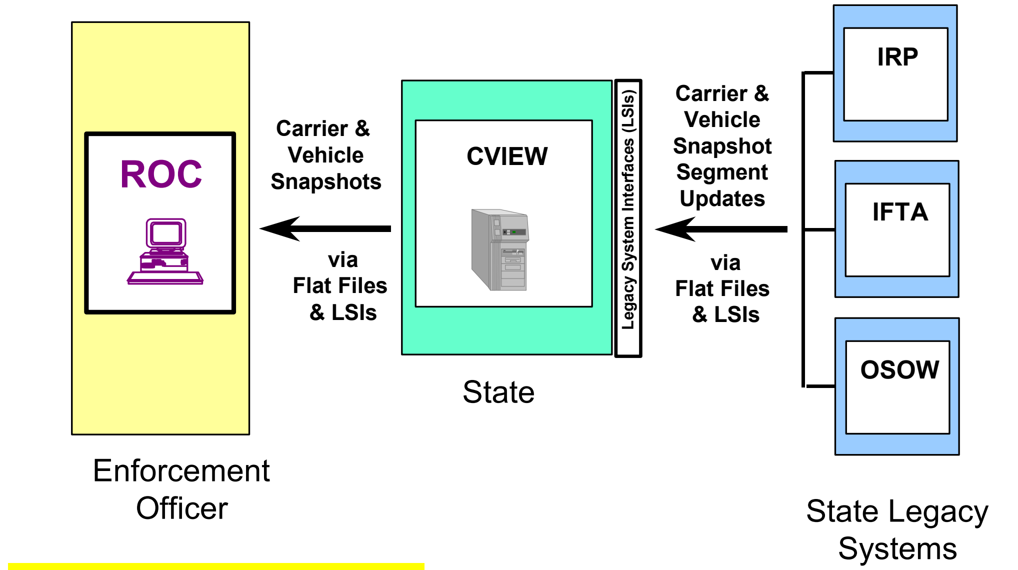

CVIEW Alternative 1:
CVIEW interfaces with state systems via EDI
ROC
Carrier & Vehicle Snapshots
via EDI
CVIEW
Carrier & Vehicle Snapshot Segment Updates
via EDI
LM
IRP
LM
IFTA
LM
OSOW
Enforcement Officer
State
State Legacy Systems
Conforms with the architecture.
Note: LM = Legacy Modification

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 LSIs. CVIEW, or its equivalent, updates its internal database and provides the new information to any client system, e.g., a ROC, that has requested that data via the subscription process. 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.

Some states have eliminated the CVIEW-roadside subscription step by replicating the CVIEW database at the roadside via FTP and updating it on a regular basis. In this case, there would be no need for query/response capabilities between the roadside and the CVIEW.

CVIEW Alternative 2:
CVIEW interfaces with state systems via LSIs



Conforms with the architecture.

Figure 6–6. CVIEW Communicates with State Systems via LSIs

6.3.2 Data Exchange Formats

The CVIEW system developed by FMCSA supports safety data exchange within the state via the use of EDI and LSIs. Again, the choice of 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. An additional data exchange option is the use of XML or flat file transfer between components.

The data exchange format between a state CVIEW and the SAFER system is EDI for carrier and vehicle snapshots and the existing CIA for inspection reports.

6.3.3 FMCSA Development and Maintenance Support for CVIEW

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.

FMCSA will continue to fund development and maintenance support of CVIEW through Version 3, which includes all of the capabilities required for CVISN Level 1 compatibility. States that elect to develop a CVIEW system based on the FMCSA-sponsored model will be required to assume responsibility for CVIEW enhancement and maintenance operations following release of CVIEW Version 3. Configuration control of carrier, vehicle, and, in the future, 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 definitions of the snapshot data elements are documented in Reference 3, which is available via the CVISN Web site at http://www.jhuapl.edu/cvisn/. Any planned changes to those definitions will be posted via the Web site. (Note that this white paper will be replaced by the View Summary Report, View Definition Report, and Schema Definition Report that will be available on the CVIEW V3 CD when it is released.)

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.

States that are interested in obtaining the FMCSA CVIEW product, or more information on the hardware and software requirements for its use, should contact FMCSA.

6.4 Design Guidance Related to Interfacing With SAFER

Each 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-2 algorithm via AFF and the upload and retrieval of inspection reports via the existing CIA, or via the state CVIEW
- 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 ROC, subscription download and online query of carrier and vehicle snapshots to support electronic screening operations via X12 EDI 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 X12 EDI standard transactions (285, 824, 997). XML or flat file interfaces may be available in the CVISN Level 1 timeframe.
- Electronic upload and download of inspection reports from/to CVIEW via existing CIAs, e.g., ASPEN-formatted inspection reports
- Subscription upload of carrier and vehicle snapshot segments from CVIEW via X12 EDI standard transactions (285, 824, 997). XML or flat file interfaces may be an alternative to EDI in the CVISN Level 1 timeframe.

Note: unlike CVIEW, SAFER does not support LSIs with state systems; it provides a standard interface for all state systems. FMCSA is currently exploring the option of providing an alternative standard interface for states to exchange data with SAFER using XML or flat file formats. This may be an option in the 2003 timeframe.

FMCSA is investigating allowing 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. It is planned that, in the 2003 timeframe, 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.

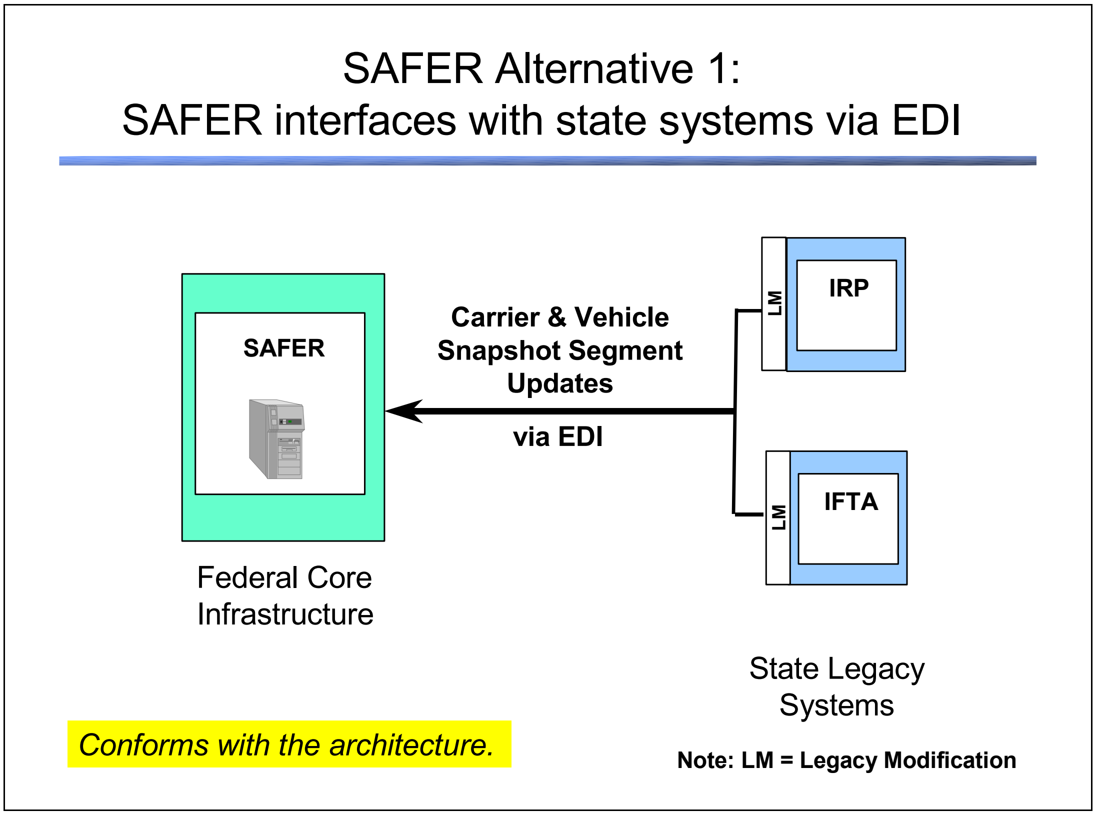
See the *SAFER System Interface Control Document* (Reference 20) for more information on current interface requirements.

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. Three alternative design options are provided below.

In Figure 6–7, IRP and IFTA legacy systems within the state send SAFER carrier and/or vehicle updates from each of their respective systems via X12 EDI standard transactions (285, 824, 997). SAFER updates its internal snapshot database and provides carrier and vehicle snapshots to states via the subscription process.

SAFER Alternative 1:
SAFER interfaces with state systems via EDI


SAFER
Carrier & Vehicle Snapshot Segment Updates
via EDI
LM
IRP
LM
IFTA
Federal Core Infrastructure
State Legacy Systems

Conforms with the architecture.

Note: LM = Legacy Modification

Figure 6–7. SAFER Communicates with State Systems via EDI

In Figure 6–8 below, a ROC performs subscription download functions and online queries for carrier and vehicle snapshots to support electronic screening operations via X12 EDI 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 via EDI. Currently there are no ROC subscriptions defined on SAFER.

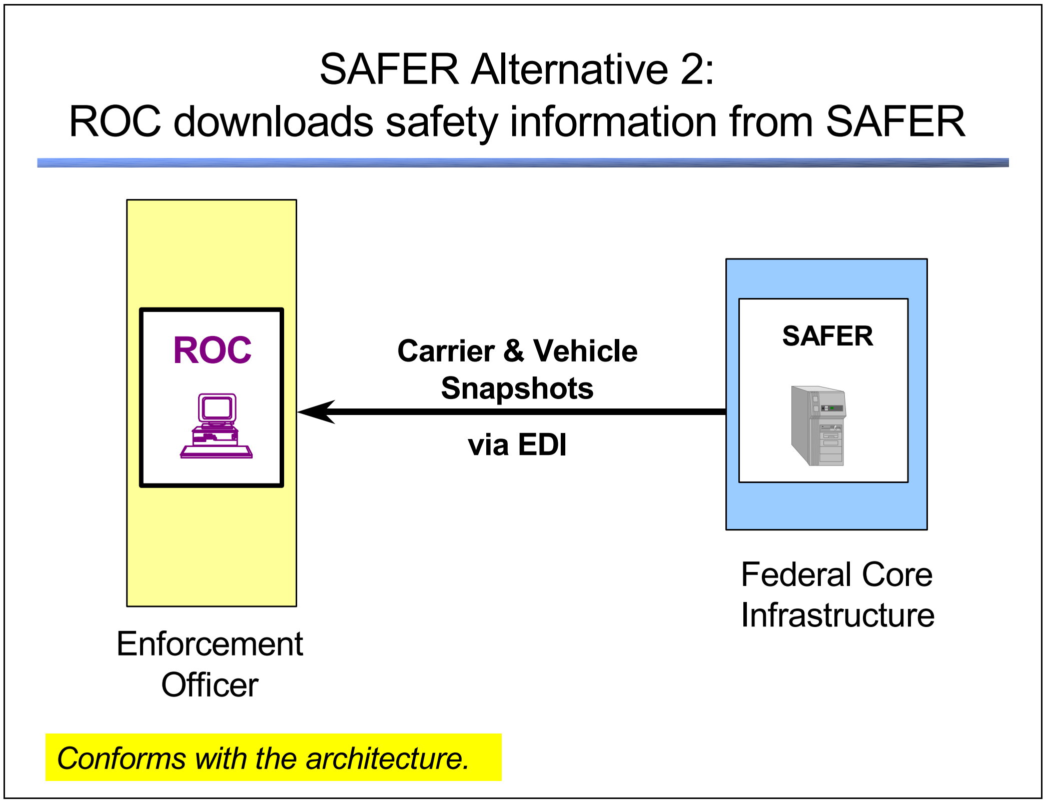
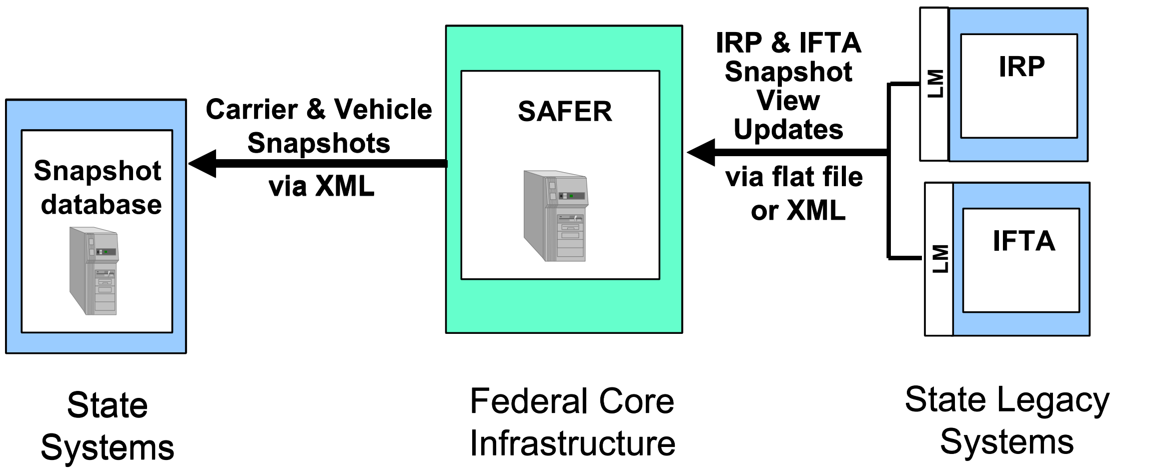

SAFER Alternative 2:
ROC downloads safety information from SAFER
ROC
Carrier & Vehicle Snapshots
via EDI
SAFER
Federal Core Infrastructure
Enforcement Officer
Conforms with the architecture.

Figure 6–8. SAFER Communicates with ROC Systems via EDI

Figure 6–9 depicts the configuration when a state chooses the (future) “SAFER Option” as an alternative design approach. Legacy systems would provide snapshot updates to SAFER via flat files or XML, and SAFER would provide snapshot updates to states via XML. This approach is not available at the present time; the SOWG is currently working on a prototype for this type of data exchange. The goal is to have this type of interface operational in the mid-2003 timeframe.

SAFER Alternative 3:
SAFER Option: SAFER interfaces
with state systems via XML and flat files


Snapshot database
Carrier & Vehicle Snapshots via XML
SAFER
IRP & IFTA Snapshot View Updates
via flat file or XML
LM
IRP
LM
IFTA
State Systems
Federal Core Infrastructure
State Legacy Systems

May conform with the architecture in the future.

Note: LM = Legacy Modification

Figure 6–9. SAFER Communicates with State Systems via Flat Files and XML

6.5 Design Guidance on Communications

Each 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

FMCSA has delegated responsibility for operation, maintenance and security of SAFER to the Volpe National Transportation Systems Center. The SAFER system currently supports the following TCP/IP-based WAN link options (See Reference 20):

- Internet
- AAMVAnet frame-relay
- FTS2000 frame-relay
- Verizon (formerly Bell Atlantic)

In addition, a digital modem bank providing toll-free access provides standard Public Switched 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 for non-web-based data exchange operations via the Internet requires establishing a virtual private network (VPN) link to SAFER that provides communications security between SAFER and the client by forcing the password and subsequent data transmissions to be encrypted.

IPSec (Internet Protocol Security) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of data packets at the IP layer. IPsec is expected to be deployed widely to implement VPNs. IPSec enables SAFER clients to connect to SAFER via the Internet through any private network that permits its traffic to be routed over the Internet via a secure IPSec tunnel environment. The FMCSA is utilizing the Cisco VPN/IPSec solution for allowing authorized FMCSA Field System application users to connect to SAFER over the Internet. The client version of this software can be provided (without charge) to authorized users of FMCSA applications. (See Appendix F and Reference 46 for more information.)

6.5.1.2 AAMVAnet Frame-relay

SAFER supports communications over the AAMVAnet, Inc., frame-relay WAN. This private network offers greater reliability and trouble-shooting diagnostics than the Internet solution but at a substantially higher cost. Maryland uses the AAMVAnet WAN to provide communications between its CVIEW system and SAFER. AAMVAnet also supports local PSTN and toll-free 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 FTS2001

FTS2001 is a frame-relay WAN that supports communications among federal systems. In the near-future, SAFER will use this WAN to communicate with the MCMIS for the exchange of weekly carrier census and safety information. Currently, this is being accomplished via the Internet. FTS2001 also supports local PSTN and toll-free 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 FMCSA directly.

6.5.1.4 Verizon

SAFER supports a connection to the Verizon (formerly 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 Verizon directly.

6.5.2 CVIEW Communications

A state that implements a 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 Subsection 6.5.1? If not, the state needs to either: 1) add an existing SAFER communications link to their CVIEW system, or 2) request FMCSA to add an additional communications link to SAFER to support their state's communication requirements.

See Appendix F for details on CVIEW-SAFER connectivity via AAMVAnet frame relay and VPN/IPSec.

6.5.3 SAFETYNET Communications

The current CVISN architecture specifies that SAFETYNET will not upload data to SAFER via 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 Subsection 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 ISS-2 and PIQ applications, needs to communicate with 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 Subsection 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 Subsection 6.5.1, could be used to facilitate communications among these systems.

6.5.5 ROC Communications

A 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 Subsection 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 Subsection 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.

7. 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 27) provides detailed guidance on establishing a workable approach.

7.1 Issues

How will safety-related identifiers be crossed-referenced to credentials-related identifiers?

The CVISN recommended primary carrier identifier (ID) for an interstate carrier is based on the USDOT number. The USDOT number is generally accepted as the main carrier ID for safety information exchange.

However, a number of different identifiers are associated with an interstate carrier for credentialing purposes. For the IFTA, the taxpayer ID is the main identifier. For the IRP, the IRP account number is used. The MCS-150 form captures many key identifiers (USDOT number, motor carrier operating authority number issued by FMCSA or Interstate Commerce Commission, Dun & Bradstreet business number, taxpayer identifier). Information from the MCS-150 form is entered into the MCMIS database, and this data is sent to SAFER for inclusion in SAFER snapshots.

Under the 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 each year. 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 number 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.

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. At the present time, only inspections for carriers with USDOT numbers can be stored in SAFER. To report and access intrastate inspections, either the systems involved (ASPEN, CVIEW, SAFER, SAFETYNET) must be modified to handle the identifiers used by the states for intrastate carriers, or the intrastate carriers must be assigned USDOT numbers. There is currently no plan to modify SAFER to handle state-specific identifiers. At this point in time, there is no federal legislation that requires intrastate carriers to have USDOT numbers; however, many states are beginning to assign USDOT numbers for their intrastate carriers.

7.2 Interoperability Tests

Interoperability tests for safety information exchange functions were defined according to the criteria in the *CVISN Operational and Architectural Compatibility Handbook (COACH) Part 5, Interoperability Test Criteria* (Reference 8). The *CVISN Interoperability Test Suite Package* (References 9, 10,11) 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).

APPENDIX A.
REFERENCES

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 Commercial Vehicle Information Systems and Networks (CVISN) Glossary*, POR-96-6997 V2.0, December 2000. (Delivered via SSD-PL-00-0751, 16 February 2001.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].
2. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1 – Operational Concept and Top-Level Design Checklists*, POR-97-7067 V2.0, August 2000. (Delivered via SSD/PL-00-0528, 30 August 2000.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].
3. JHU/APL, *Safety and Fitness Electronic Records (SAFER) System and Commercial Vehicle Information Exchange Window (CVIEW) Carrier, Vehicle, and Driver Snapshots*, V1.0, August 2001. (Delivered via SSD-PL-01-0258, 6 August 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-White Papers]. (Note that this white paper will be replaced by the View Summary Report, View Definition Report, and Schema Definition Report that will be available on the CVIEW V3 CD when it is released.)
4. FMCSA, *PRISM Overview*, published on the World Wide Web at http://www.fmcsa.dot.gov/factsfigs/prism.htm.
5. FMCSA - Field Systems Group (FSG) in Lakewood, CO, http://www.inspector.org/fhwafsg1.htm, a site maintained by the International Inspector's Competition.
6. JHU/APL, *CVISN Guide to Credentials Administration*, POR-99-7192 P.2, August 2000. (Delivered via SSD/PL-00-0015, 10 March 2000.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].
7. JHU/APL, *ITS/CVO Architecture Conformance: Interoperability Testing Strategy*, POR-98-7076 P.2, June 1999. (Delivered via SSD-PL-99-0467, 30 July 1999.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-Interoperability Testing].
8. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 5 – Interoperability Test Criteria*, POR-98-7126 V1.0, July 2001. (Delivered via SSD-PL-01-0444, 21 September 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].

9. JHU/APL, *CVISN Interoperability Test Suite Package, Part 1 - Test Specifications*, POR-98-7122 V1.0, July 2001. (Delivered via SSD-PL-01-0168, 21 September 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-Interoperability Testing].

10. JHU/APL, *CVISN Interoperability Test Suite Package, Part 2 - Test Cases and Procedures*, POR-98-7123 V1.0, July 2001. (Delivered via SSD-PL-01-0454, 12 September 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-Interoperability Testing].

11. JHU/APL, *CVISN Interoperability Test Suite Package, Part 4 - Test Data*, POR-98-7125 D.0, June 1998. (Delivered via SSD/PL-98-0399, 3 July 1998.) [Note: This document is scheduled for a significant update in 2002.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-Interoperability Testing].

12. Intelligent Transportation Society of America, *ITS CVO Guiding Principles*, published on the World Wide Web at http://www.itsa.org/frontpage.html, last updated 27 March 1998. [Site Resources-Search-document title.]

13. Intelligent Transportation Society of America, *Fair Information Principles for ITS/CVO*, published on the World Wide Web at http://www.itsa.org/frontpage.html, last updated 22 August 2000. [Site Resources-Search-document title.]

14. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 4 – Interface Specification Checklists*, POR-97-7067 P2.0, October 2000. (Delivered via SSD-PL-00-0633, 1 December 2000.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].

15. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V2.0, August 2000. (Delivered via SSD-PL-00-0553, 13 September 2000.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].

16. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists*, POR-97-7067 V1.0, October 2000. (Delivered via SSD-PL-00-0618, 1 December 2000.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].

17. JHU/APL, *Introductory Guide to CVISN*, POR-99-7186 P.2, February 2000. (Delivered via SSD/PL-00-0010, 21 January 2000.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

18. JHU/APL, *SAFER-CVIEW Application Programming Interface for Win32 (SCAPI32).* [Available from Alan Mick, (240) 228-7386 (Alan.Mick@jhuapl.edu)].

19. Reference deleted.

20. JHU/APL, *Safety and Fitness Electronic Records (SAFER) Interface Control Document (ICD),* POR-99-7129 V1.0, June 2001. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [SAFER].

21. JHU/APL, *CVISN Guide to Program and Project Planning*, POR-99-7188 V1.0, November 2001. (Delivered via SSD-PL-01-0620, 20 December 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

22. JHU/APL, *CVISN Guide to Phase Planning and Tracking*, POR-99-7189 V1.0, November 2001. (Delivered via SSD-PL-01-0626, 19 December 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

23. JHU/APL, *CVISN Guide to Top-Level Design*, POR-99-7187 V1.0, February 2001. (Delivered via SSD-PL-01-0070, 26 February 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

24. ANSI/IEEE Std 1042-1987 (R1993), *An American National Standard IEEE Guide to Software Configuration Management*, 1988.

25. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), State of Maryland, Credentials Administration Requirements Specifications (CARS)*, D.1. (Delivered via SSD/PL-96-0613, November 1997.)

26. JHU/APL, *Intelligent Transportation Systems (ITS) Commercial Vehicle Information Systems and Networks (CVISN), Commonwealth of Virginia, Credentials Administration Requirements Specifications (CARS)*, V2.0. (Delivered via SSD/PL-98-0485, September 1998.)

27. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Recommendations for Primary Identifiers*, P1.0, 23 June 1999. (Delivered via SSD-PL-99-0388, 13 July 1999.) [Note: This document is scheduled for update in 2001.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-White Papers].

28. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 2 – Project Management Checklists*, POR-97-7067 P2.0, September 1999. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Architecture and Standards].

29. JHU/APL, *CVISN Guide to Electronic Screening*, POR-99-7193 D.1, October 1999. (Delivered via SSD/PL-00-0016, 10 March 2000.) [Note: This document is scheduled for update in 2002.] The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

30. ANSI ASC X12, *Electronic Data Interchange X12 Standards*, Draft Version 4, Release 4, (a.k.a. Release 4040), December 2000.

31. JHU/APL, *Electronic Data Interchange (EDI) Implementation Guide for Commercial Vehicle Safety and Credentials Information Exchange (Transaction Set 285), ANSI ASC X12 Version 4 Release 4*, POR-96-6995 V1.0, March 2001. (Delivered via SSD-PL-01-0052, 12 April 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-EDI and XML].

32. Reference deleted.

33. Reference deleted.

34. JHU/APL, *The Maryland Commercial Vehicle Information Systems and Networks (CVISN) Prototype Top-Level Design Description*, POR-99-7235, proposed Baseline Issue, November 1999.

35. Intelligent Transportation Society of America, *ITS/CVO Interoperability Guiding Principles*. Published on the World Wide Web at http://www.itsa.org/frontpage.html, last updated August 26, 1999. [Site Resources-Search-document title.]

36. JHU/APL, *Introduction to ITS/CVO Training Material*, version 2.2, August 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].

37. 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].

38. ASC X12D/W456, *ASC X12 Guideline for Electronic Data Interchange, EDI Implementation Reference Manual Guidelines*, Data Interchange Standards Association (DISA), February 1991.

39. Data Interchange Standards Association (DISA) Home Page: http://www.disa.org/.

40. JHU/APL, *CVISN Scope Workshop Notebook*. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents – All Workshop Materials].

41. JHU/APL, *CVISN Guide to Integration and Test*, POR-99-7194 D.1, May 2001. (Delivered via SSD-PL-01-0230, 7 August 2001.) The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVISN Guides].

42. Notice of Proposed Rulemaking, Statewide Transportation Planning, Metropolitan Transportation Planning; US DOT Federal Highway Administration 23 CFR parts 450 and 1410; Federal Transit Administration 23 CFR Part 1410, 49 CFR Parts 613 and 621; FHWA Docket No. FHWA A-99-5933, FHWA RIN 2125-AE62; FTA RIN 2132-AA66; published in the Federal Register Volume 65, No. 102, Thursday May 25, 2000; Proposed Rules.

43. Washington State Department of Transportation, *SAFER Option Working Group Proposed State – SAFER Flat File and XML Interfaces Control Document*, Draft, July 2001.

44. JHU/APL, *Commercial Vehicle Information Exchange Window (CVIEW) Interface Control Document (ICD)*, POR-99-7195 V1.0, June 2001. The latest version will be available on the JHU/APL CVISN Web site http://www.jhuapl.edu/cvisn/ [Documents-CVIEW].

45. *Alternative Architectures for the PRISM Program*, Baseline V1.0, October 2001.

46. JHU/APL, *Secure Network Communications to Support SAFER and CDLIS Data Exchange*. (Delivered via SSD-PL-00-0723, December 2000.

This Page Intentionally Blank

APPENDIX B.

PRISM AND CVISN – EXPLAINING THE RELATIONSHIP

This Page Intentionally Blank

APPENDIX B. PRISM AND CVISN: EXPLAINING THE RELATIONSHIP

Performance and Registration Information Systems Management (PRISM) and CVISN share key concepts in that they both:

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

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

PRISM - An 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 its safety rating (see Motor Carrier Safety Improvement Program, below).

PRISM is a comprehensive program of motor carrier safety assessment, enforcement and improvement. The core concept of PRISM is the linking of <u>vehicle registration</u> at the state level to acceptable <u>carrier safety performance</u>. 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 the vehicle registration process, participating states ensure that motor carriers are registered and meet 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 if the state implements an interface from the registration system to roadside operations and screening systems. Twenty states (Iowa, Colorado, Indiana, Oregon, Minnesota, Pennsylvania, Maine, Rhode Island, Connecticut, Tennessee, Kentucky, Georgia, South Carolina, Arizona, New Mexico, Utah, South Dakota, Louisiana, New Jersey, and Vermont) currently participate in the PRISM program. Participation is expected to increase by four or five states annually.

The other major process in PRISM is the **Motor Carrier Safety Improvement Program (MCSIP)**. MCSIP is a process in which carrier safety is systematically tracked and improved. The intent is to improve safety performance of carriers through identification and performance monitoring of carriers with demonstrated poor safety performance. Under MCSIP, carriers that do not improve their safety performance face progressively more stringent penalties that may culminate in a Federal imminent hazard determination and possible suspension of vehicle registrations by the state.

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 an 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 can also be made available at the roadside for use in screening algorithms if the appropriate interfaces are in place. The SafeStat values are updated by MCMIS periodically for each carrier, and weekly updates of the SafeStat files are sent to the PRISM Central Site maintained by FMCSA. The PRISM Central Site provides vehicle registrations and any updated SafeStat values to the state registration offices via a proprietary flat file format on a daily basis.

Commercial Vehicle Information Systems and Networks (CVISN) - 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 and 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.

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 (e.g., SAFER, SAFETYNET, MCMIS, ASPEN, CAPRI) provide that access.

- To facilitate information exchange, several systems are being developed under CVISN. One of those systems is **Safety and Fitness Electronic Records (SAFER)**. SAFER and other information systems (e.g., SAFETYNET, MCMIS, ASPEN, CAPRI) are used to supply data for the PRISM processes. SAFER also provides PRISM Central Site data exchange support for the participating PRISM states.
- The values generated by the SafeStat algorithm are included in SAFER data snapshots that are used by the CVISN states. Snapshots are used in roadside screening and inspection activities to focus resources on high-risk operators. Snapshots are available to CVISN states on a daily basis with SafeStat updates provided by MCMIS via SAFER on a weekly basis.

Thus, the PRISM program concepts and approach are compatible with and utilize components of the CVISN Architecture. The CVISN Architecture facilitates the transmission of safety data (SafeStat scores) to the roadside via data snapshots from SAFER, and the SAFER system supports data exchange for the PRISM states.

The PRISM operational concepts are illustrated in Figure B-1.

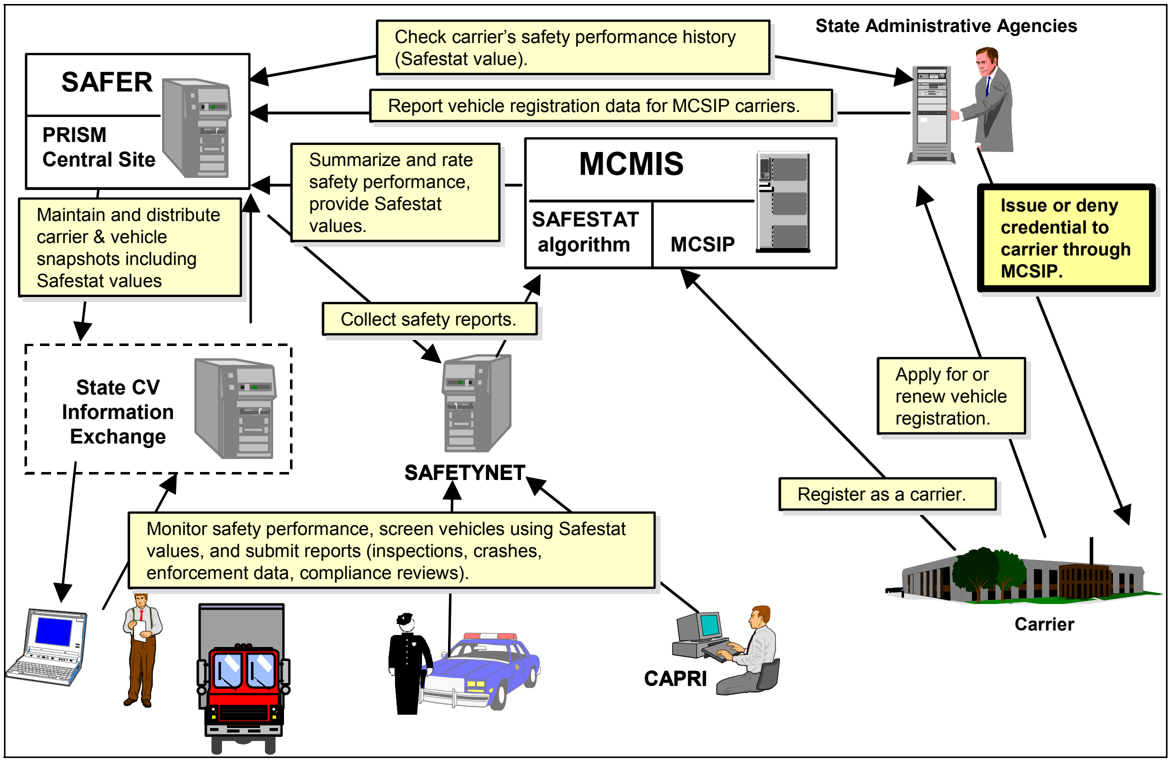

State Administrative Agencies
Check carrier's safety performance history (Safestat value).
Report vehicle registration data for MCSIP carriers.
SAFER
PRISM Central Site
Summarize and rate safety performance, provide Safestat values.
MCMIS
SAFESTAT algorithm
MCSIP
Issue or deny credential to carrier through MCSIP.
Maintain and distribute carrier & vehicle snapshots including Safestat values
Collect safety reports.
State CV Information Exchange
SAFETYNET
Apply for or renew vehicle registration.
Register as a carrier.
Monitor safety performance, screen vehicles using Safestat values, and submit reports (inspections, crashes, enforcement data, compliance reviews).
Carrier
CAPRI

Figure B–1. PRISM Operation Concepts

In order to more completely support PRISM operations, 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.

When originally established, the PRISM program supported a single data exchange and networking architecture for interactions between the PRISM states and the PRISM Central site. Since that time, several new data exchange and telecommunications technologies and methods have become available. At the same time, the PRISM Central site has been reengineered and combined with the SAFER system to form the SAFER-PRISM Central site (SPCS). Because the SPCS now supports a variety of data exchange and networking options, the PRISM states have more choices regarding program implementation. See Reference 45, *Alternative Architectures for the PRISM Program*.

This Page Intentionally Blank

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.

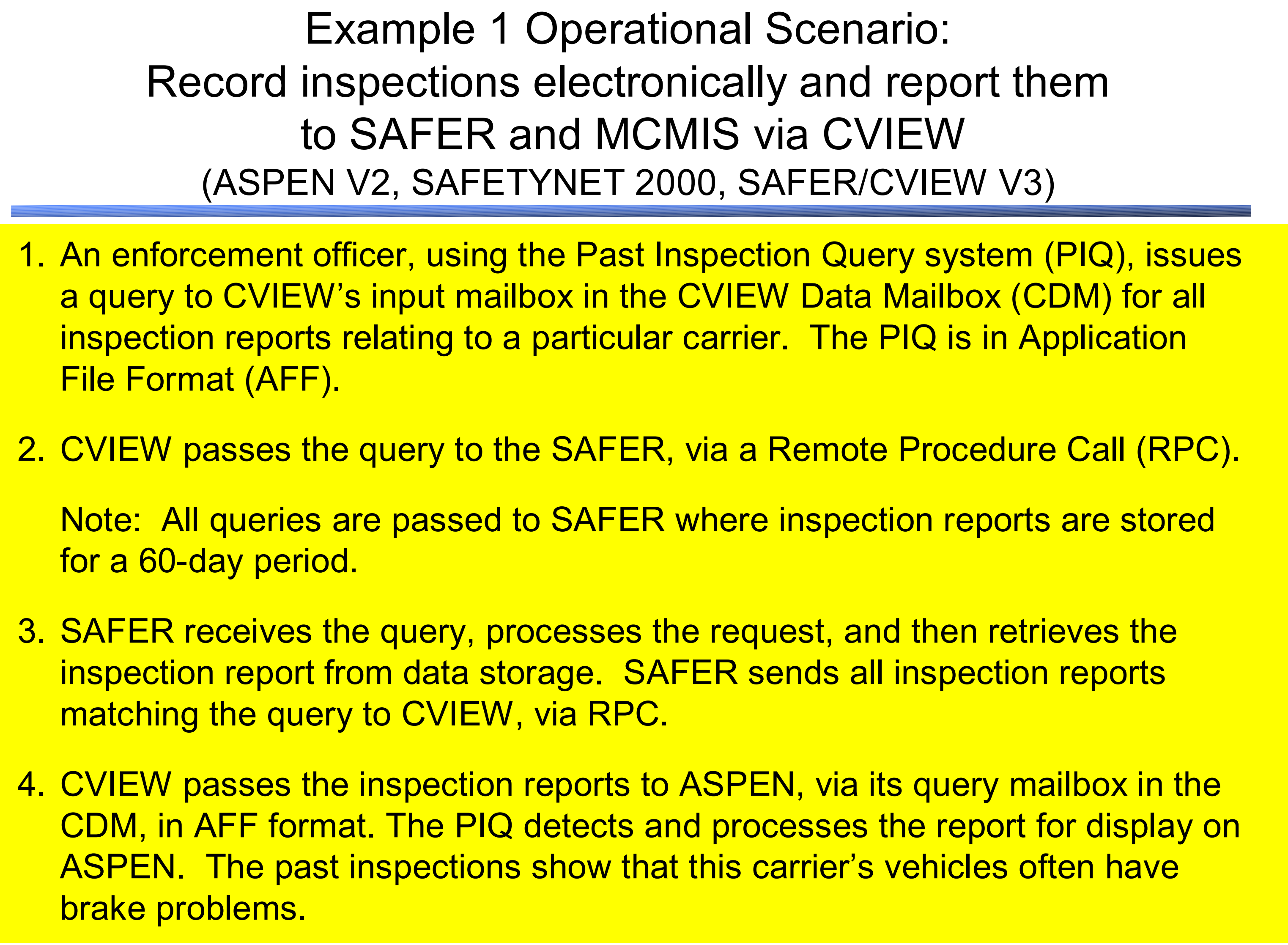
CVISN Level 1 Safety Information Exchange Key Operational Scenarios

- Record inspections electronically and report them to SAFER and MCMIS
  - ***Example 1:*** Operational Scenario: Record inspections electronically and report them to SAFER and MCMIS via CVIEW
    (ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)*
  - ***Example 2:*** Operational Scenario: Record inspections electronically and report them to SAFER and MCMIS
    (ASPEN V2, SAFETYNET 2000, SAFER 3 (No CVIEW))
- Queries
  - ***Example 3:*** Operational Scenario: Past inspection report query to SAFER via CVIEW
    (ASPEN V2, SAFER/CVIEW V3)*
  - ***Example 4:*** Operational Scenario for today: Past inspection report query to SAFER
  - ***Example 5:*** Operational Scenario: Carrier snapshot query to SAFER via CVIEW
    (ASPEN V2, SAFER/CVIEW V3)*

* planned for 2002

Operational Scenario Examples 1-2

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



Example 1 Operational Scenario: Record inspections electronically and report them to SAFER and MCMIS via CVIEW (ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)

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).

2. CVIEW passes the query to the SAFER, via a Remote Procedure Call (RPC).

   Note: All queries are passed to SAFER where inspection reports are stored for a 60-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:
Record inspections electronically and report them to SAFER and MCMIS via CVIEW
(ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)

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 in AFF to CVIEW’s input mailbox in the CDM.

6. The CVIEW passes the inspection report to SAFER, via RPC, for 60-day storage.

7. CVIEW sends the inspection report in AFF to SAFETYNET 2000 via Blizzard mailbox in the CDM. Blizzard retrieves the inspection report from its CDM mailbox and passes it to SAFETYNET 2000.

8. 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.

9. CVIEW forwards carrier snapshot views in AFF to ISS-2 via their subscription mailboxes in the CDM.

Example 1 Operational Scenario:
Record inspections electronically and report them to SAFER and MCMIS via CVIEW
(ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)

A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the MCMIS/SAFETYNET Gateway.

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.

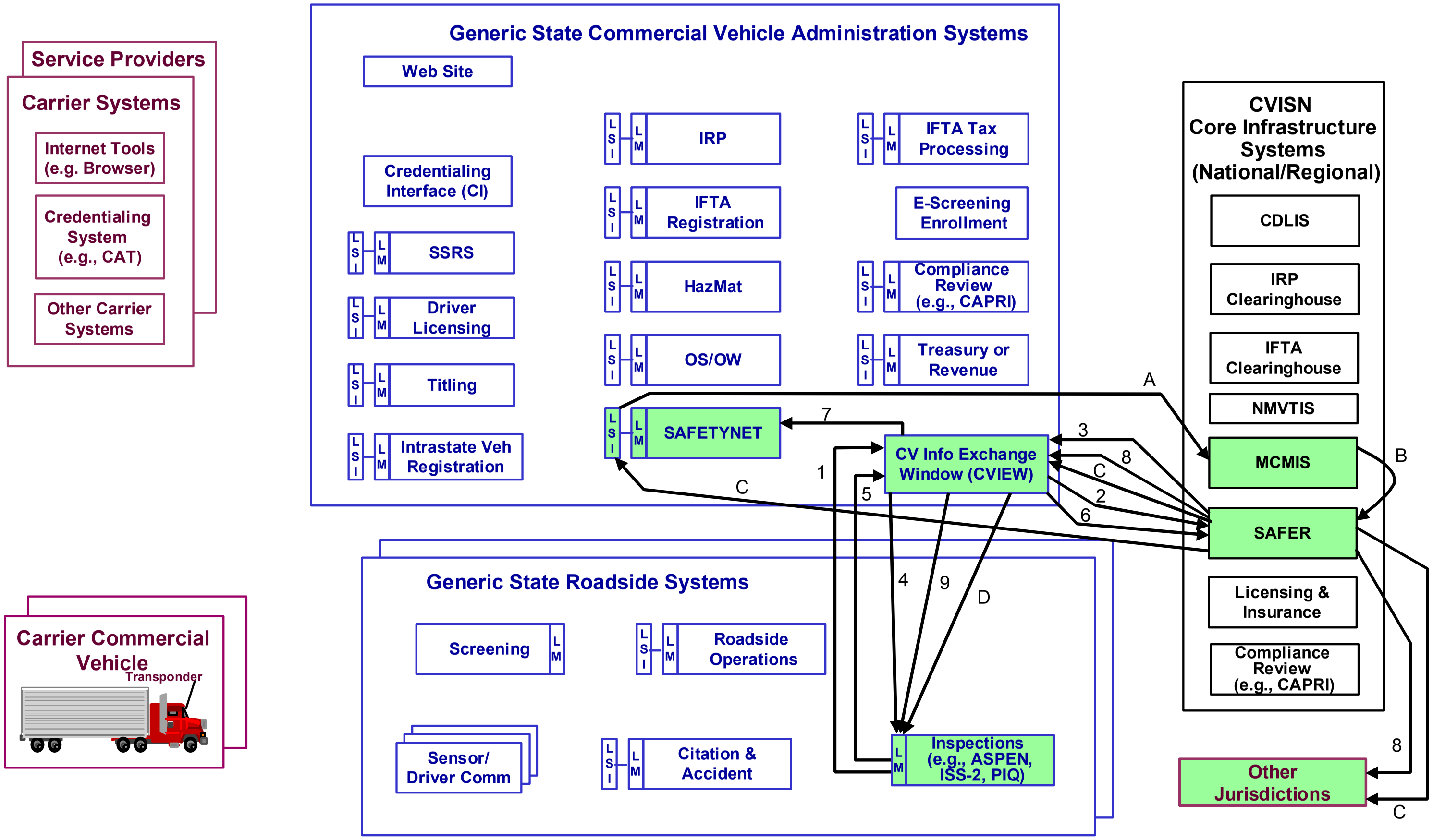
C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM (in EDI X12 TS 285 format to CVIEWs, and in AFF to SAFETYNET).

D. CVIEW updates its stored snapshots with carrier snapshot segments it receives from SAFER. CVIEW forwards carrier snapshot views in AFF to ISS-2 via their subscription mailboxes in the CDM.

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: Record inspections electronically and report them to SAFER and MCMIS via CVIEW

(ASPEN V2, SAFETYNET 2000, SAFER/CVIEW V3)



Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

Generic State Commercial Vehicle Administration Systems

Web Site

Credentialing Interface (CI)

SSRS

Driver Licensing

Titling

Intrastate Veh Registration

IRP

IFTA Registration

HazMat

OS/OW

SAFETYNET

IFTA Tax Processing

E-Screening Enrollment

Compliance Review (e.g., CAPRI)

Treasury or Revenue

CV Info Exchange Window (CVIEW)

CVISN Core Infrastructure Systems (National/Regional)

CDLIS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

Other Jurisdictions

Carrier Commercial Vehicle

Transponder

Generic State Roadside Systems

Screening

Roadside Operations

Sensor/ Driver Comm

Citation & Accident

Inspections (e.g., ASPEN, ISS-2, PIQ)

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

(ASPEN V2, SAFETYNET 2000, SAFER (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).

   Note: SAFER stores Intrastate and Interstate Inspection Reports for a 60-day period.

2. SAFER receives, processes, and sends all inspection reports matching the query to ASPEN in AFF 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: Record inspections electronically and report them to SAFER and MCMIS

(ASPEN V2, SAFETYNET 2000, SAFER (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 in AFF to SAFER’s input mailbox and the state’s input mailbox in the SDM.

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 (via Blizzard) retrieves the inspection report in AFF format from the state’s mailbox on the SDM.

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

(ASPEN V2, SAFETYNET 2000, SAFER (No CVIEW))

A. The SAFETYNET 2000 staff member reviews the inspection report and sends it to MCMIS, in AFF, via the MCMIS/SAFETYNET Gateway at Volpe.

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.

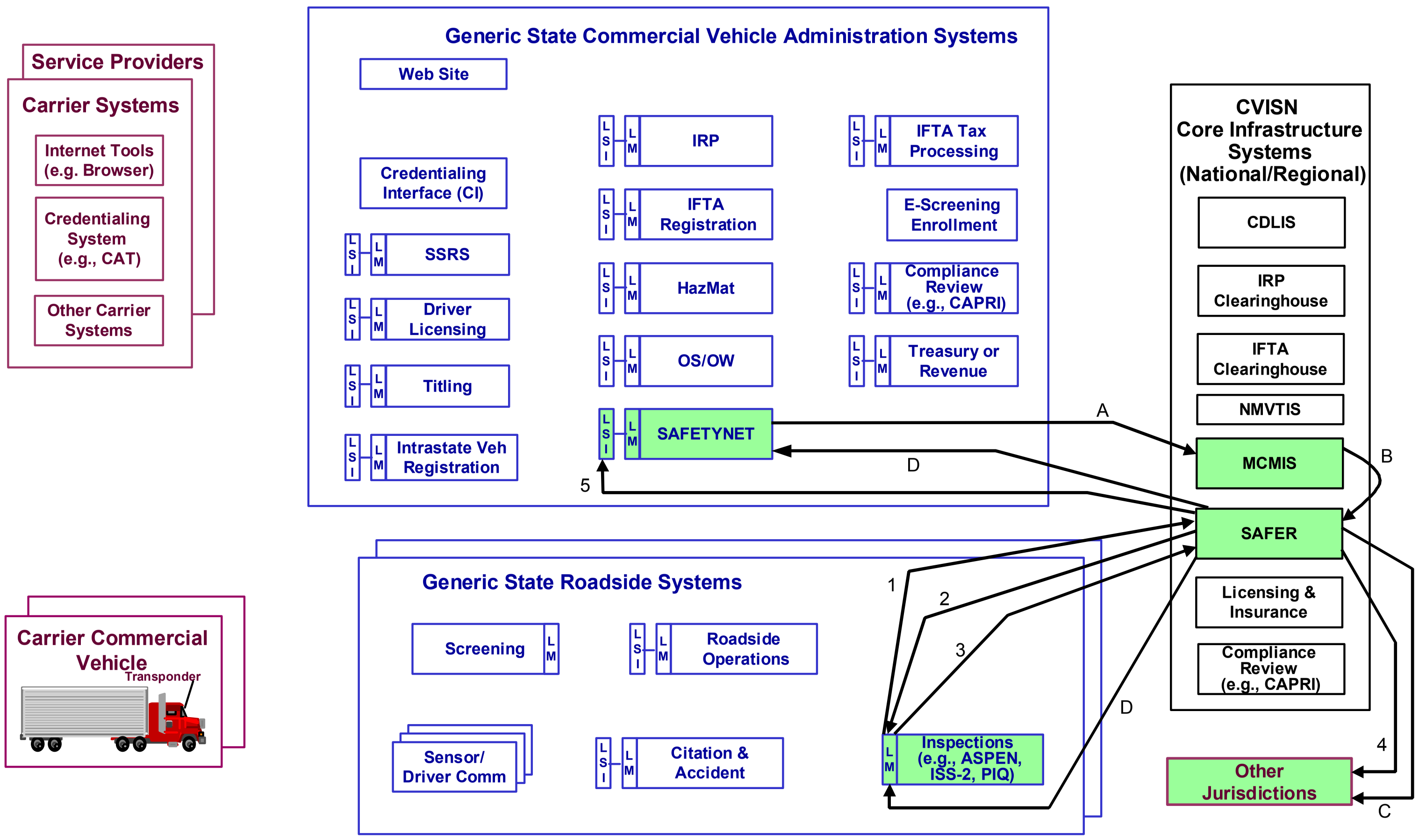
C. SAFER updates its stored snapshots with carrier snapshot segments it receives from MCMIS. SAFER forwards snapshot views to subscribers via their subscription mailboxes in the SDM in EDI X12 TS 285 format.

D. SAFER then forwards carrier snapshot views to ASPEN and SAFETYNET subscribers in AFF 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: Record inspections electronically and report them to SAFER and MCMIS

(ASPEN V2, SAFETYNET 2000, SAFER (No CVIEW))


Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Carrier Commercial Vehicle
Transponder
Generic State Commercial Vehicle Administration Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
L S I
L M
5
A
D
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
1
2
3
D
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
B
4
C
Other Jurisdictions

Example 3 Operational Scenario: Past inspection report query to SAFER via CVIEW

(ASPEN V2, SAFER/CVIEW V3)

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).

2. CVIEW passes the query to the SAFER, via a Remote Procedure Call (RPC).

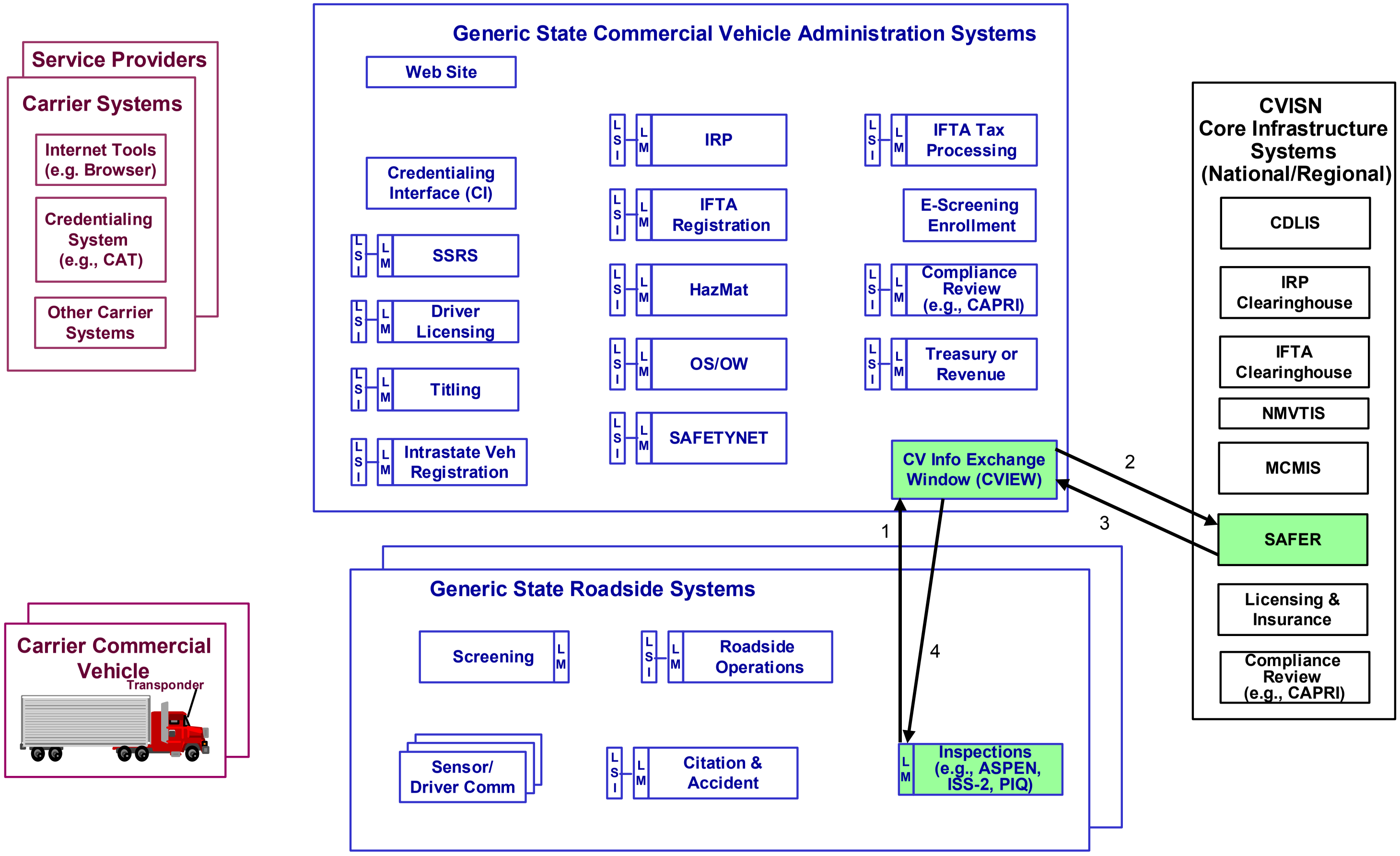
   Note: All queries are passed to SAFER where inspection reports are stored for a 60-day period.

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 in AFF to ASPEN via its query mailbox in the CDM. The PIQ detects and processes the report for display on ASPEN.

Example 3 Functional Thread Diagram: Past inspection report query to SAFER via CVIEW

(ASPEN V2, SAFER/CVIEW V3)



Service Providers

Carrier Systems

Internet Tools (e.g. Browser)

Credentialing System (e.g., CAT)

Other Carrier Systems

Carrier Commercial Vehicle

Transponder

Generic State Commercial Vehicle Administration Systems

Web Site

Credentialing Interface (CI)

SSRS

Driver Licensing

Titling

Intrastate Veh Registration

IRP

IFTA Registration

HazMat

OS/OW

SAFETYNET

IFTA Tax Processing

E-Screening Enrollment

Compliance Review (e.g., CAPRI)

Treasury or Revenue

CV Info Exchange Window (CVIEW)

Generic State Roadside Systems

Screening

Roadside Operations

Sensor/ Driver Comm

Citation & Accident

Inspections (e.g., ASPEN, ISS-2, PIQ)

CVISN Core Infrastructure Systems (National/Regional)

CDLIS

IRP Clearinghouse

IFTA Clearinghouse

NMVTIS

MCMIS

SAFER

Licensing & Insurance

Compliance Review (e.g., CAPRI)

Example 4 Operational Scenario for today: Past inspection report query to SAFER

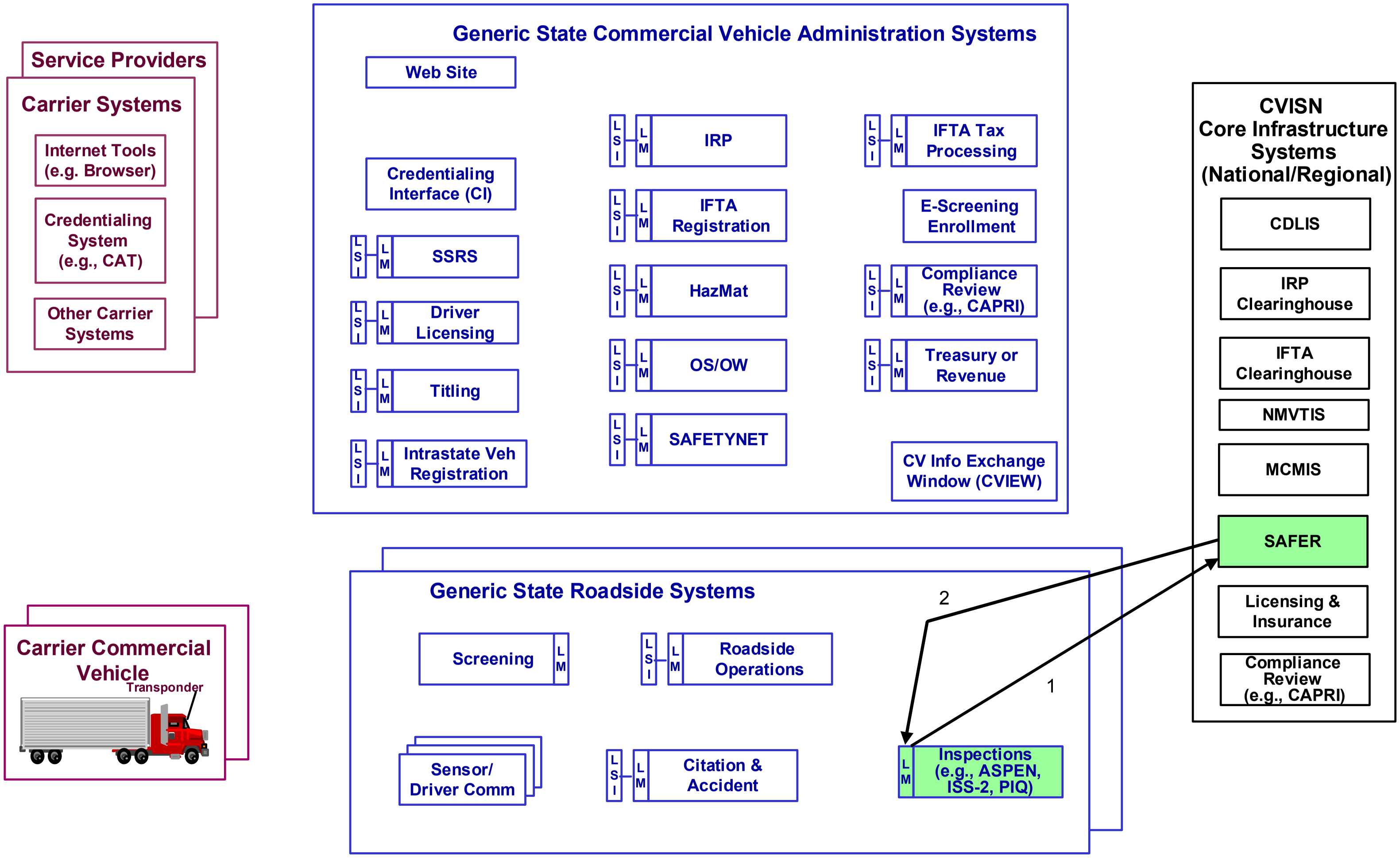
1. An enforcement officer, using the Past Inspection Query system (PIQ), issues a query to SAFER’s input mailbox in the SAFER Data Mailbox (SDM) for all inspection reports relating to a particular carrier in AFF format.

   Note: Inspection reports are stored in SAFER for 60 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 4 Functional Thread Diagram for today: Past inspection report query to SAFER


Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Generic State Commercial Vehicle Administration Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
CV Info Exchange Window (CVIEW)
L
S
I
L
M
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
Carrier Commercial Vehicle
Transponder
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
1
2

Example 5 Operational Scenario: Carrier snapshot query to SAFER via CVIEW

(ASPEN V2, SAFER/CVIEW V3)

1. While performing an inspection, the enforcement officer, using ASPEN’s Inspection Selection System (ISS-2), issues a query in Application File Format (AFF) to CVIEW’s Data Mailbox (CDM) for a carrier snapshot to check the carrier’s SafeStat values.

   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).

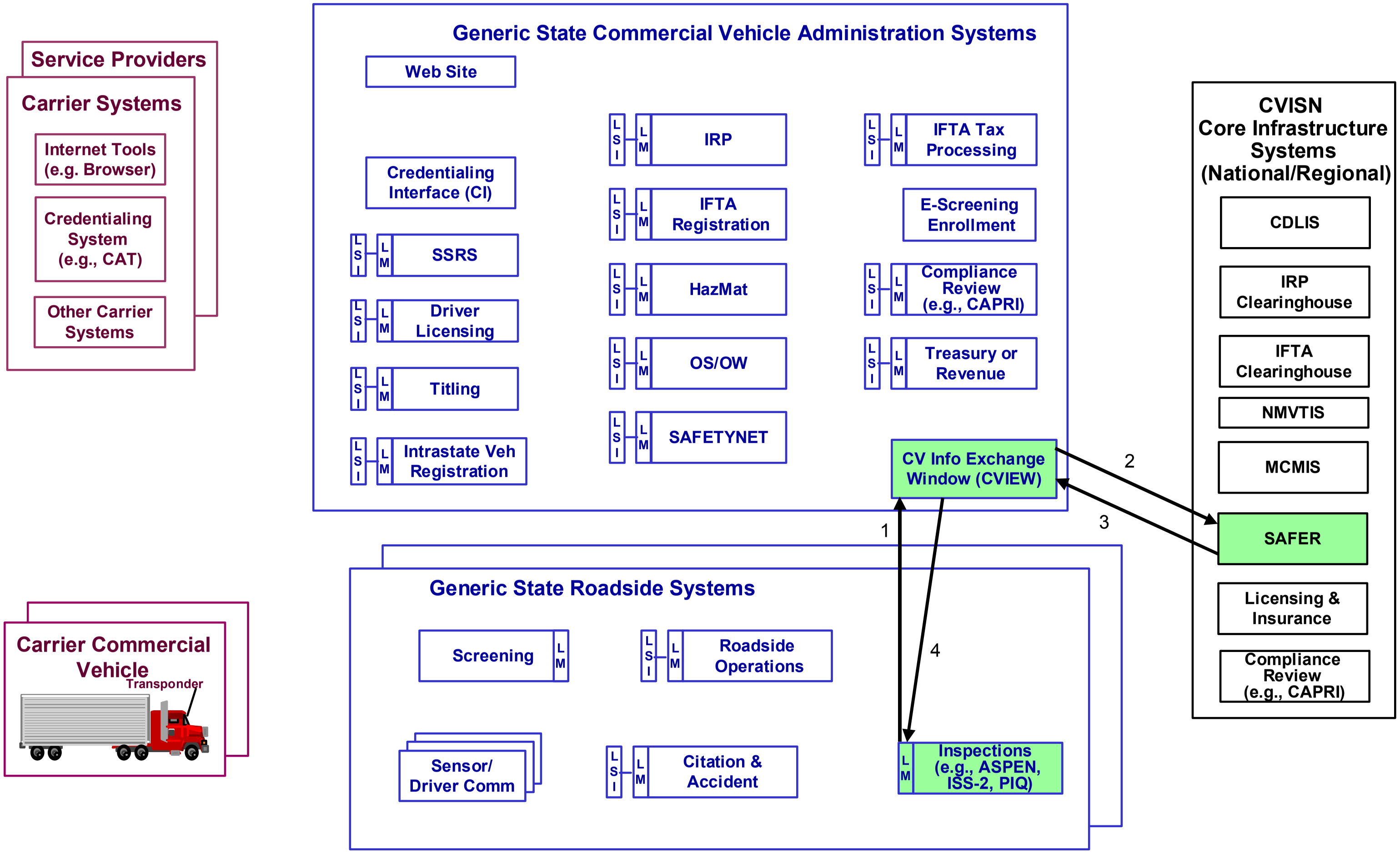
3. SAFER receives, processes, and sends the carrier snapshot matching the query to CVIEW, via RPC.

4. CVIEW passes the carrier snapshot to ASPEN’s ISS-2 in AFF format.

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

Example 5 Functional Thread Diagram: Carrier snapshot query to SAFER via CVIEW

(ASPEN V2, SAFER/CVIEW V3)


Service Providers
Carrier Systems
Internet Tools (e.g. Browser)
Credentialing System (e.g., CAT)
Other Carrier Systems
Carrier Commercial Vehicle
Transponder
Generic State Commercial Vehicle Administration Systems
Web Site
Credentialing Interface (CI)
SSRS
Driver Licensing
Titling
Intrastate Veh Registration
IRP
IFTA Registration
HazMat
OS/OW
SAFETYNET
IFTA Tax Processing
E-Screening Enrollment
Compliance Review (e.g., CAPRI)
Treasury or Revenue
CV Info Exchange Window (CVIEW)
L S I
L M
Generic State Roadside Systems
Screening
Roadside Operations
Sensor/ Driver Comm
Citation & Accident
Inspections (e.g., ASPEN, ISS-2, PIQ)
CVISN Core Infrastructure Systems (National/Regional)
CDLIS
IRP Clearinghouse
IFTA Clearinghouse
NMVTIS
MCMIS
SAFER
Licensing & Insurance
Compliance Review (e.g., CAPRI)
1
2
3
4

This Page Intentionally Blank

APPENDIX D.

RECOMMENDED DEVELOPMENT PROCESS

This Page Intentionally Blank

The *CVISN Guide to Top-Level Design* (Reference 23) and the *CVISN Guide to Program and Project Planning* (Reference 21) 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 are not 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 requirement specification, a topic that influences all phases.

Development Process Overview

The *Introductory Guide to CVISN* (Reference 17) outlined a model development process for implementing CVISN capabilities. Figure D-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, feedback, and visibility into project progress.

Figure D-1 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 21) and the *CVISN Guide to Phase Planning and Tracking* (Reference 22).

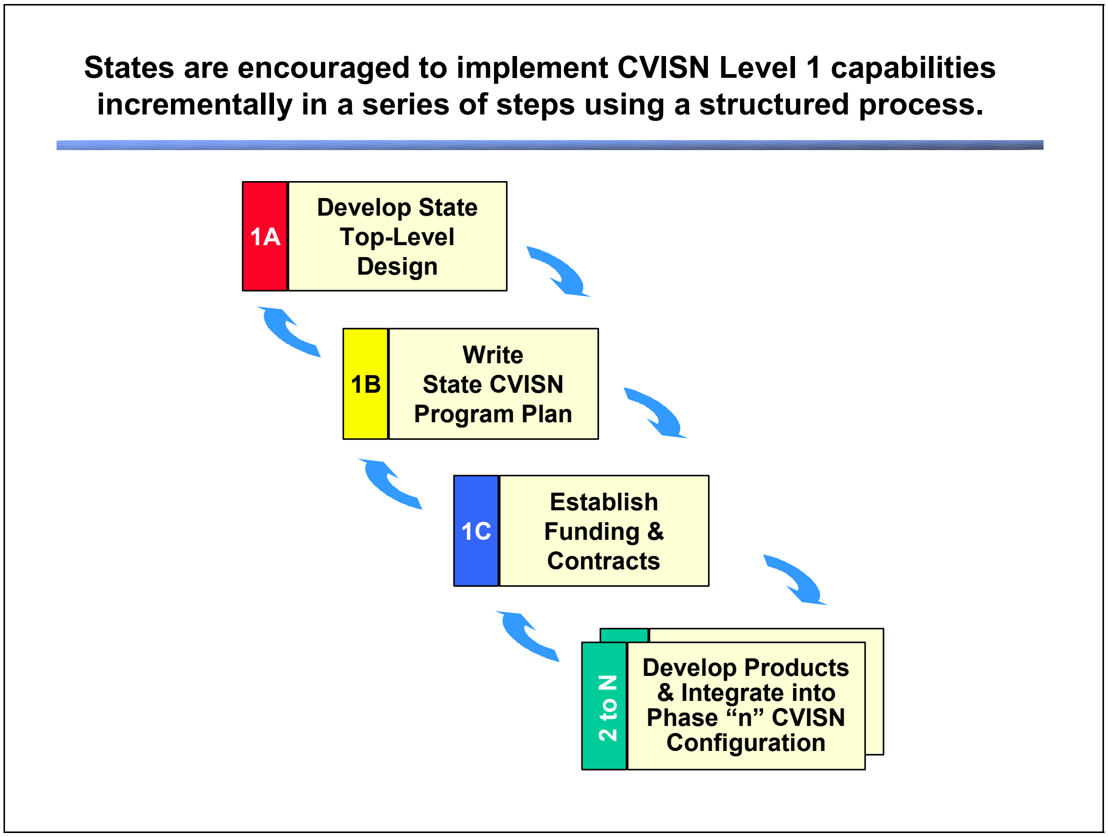

States are encouraged to implement CVISN Level 1 capabilities incrementally in a series of steps using a structured process.
1A
Develop State Top-Level Design
1B
Write State CVISN Program Plan
1C
Establish Funding & Contracts
2 to N
Develop Products & Integrate into Phase "n" CVISN Configuration

Figure D–1. Overview of CVISN Deployment Process

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 a state presently uses both ASPEN and SAFETYNET and intends to continue using them, two key elements are already in place. If USDOT numbers are assigned to both interstate and intrastate carriers and the FMCSA-developed CVIEW developed for other states is being used, the CVISN Level 1 requirements can be met with a relatively modest effort.

The approach defined herein assumes that a state is providing some level of system integration. If the role of system integrator is subcontracted, the detailed steps outlined herein might not be followed. Most likely, a system integrator will propose an approach based on their methodology. Nevertheless, the material herein can aid in understanding what a system integrator must accomplish.

D.1 Top-Level Design Phase

Top-Level Design Phase Process

The *CVISN Guide to Top Level Design* (Reference 23) describes the general process for developing a top-level design. Figure D-2 describing this process is repeated below as a reminder.

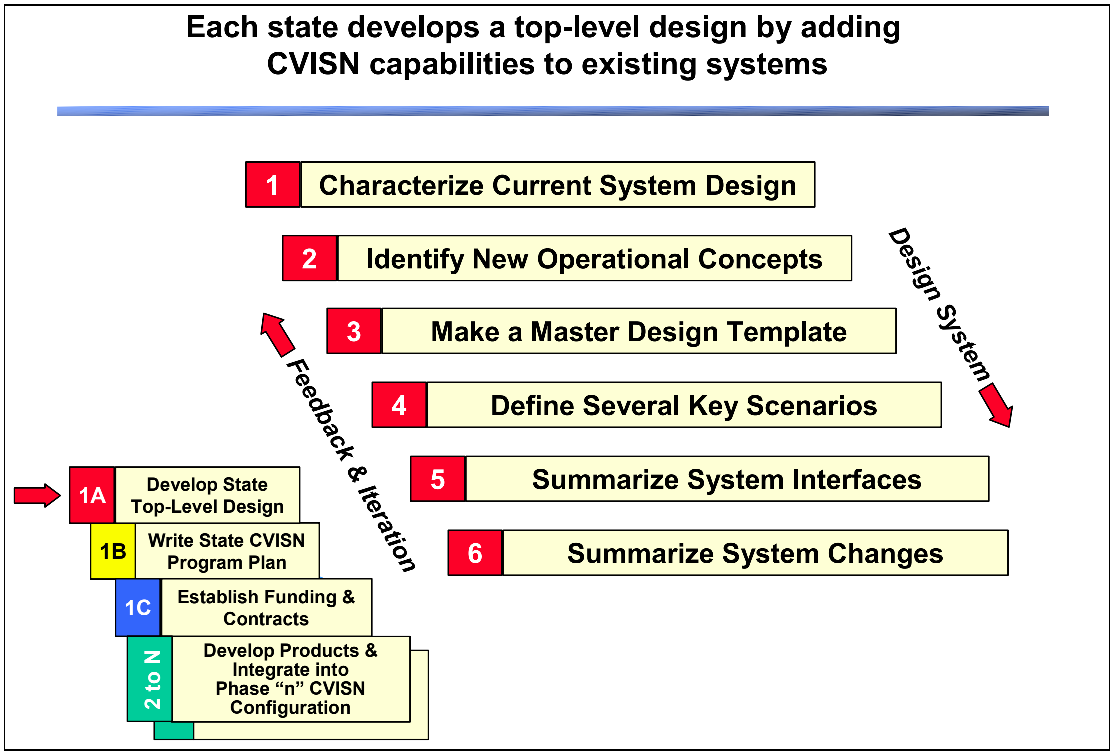

Each state develops a top-level design by adding CVISN capabilities to existing systems
1 Characterize Current System Design
2 Identify New Operational Concepts
3 Make a Master Design Template
4 Define Several Key Scenarios
5 Summarize System Interfaces
6 Summarize System Changes
Design System
Feedback & Iteration
1A Develop State Top-Level Design
1B Write State CVISN Program Plan
1C Establish Funding & Contracts
2 to N Develop Products & Integrate into Phase "n" CVISN Configuration

Figure D–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, a 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* shows how safety information exchange fits into the statewide CVISN design. It should include:
  - System Requirements
    - State-specific goals
    - COACH Part 1 tables from Chapters 2, 3, 4, 5, 6 (Reference 2)
    - COACH Part 4 tables (Reference 14)
    - Other state requirements.
  - System Design
    - Allocation of requirements to system components
      - COACH Part 3 tables, tailored as needed (Reference 16)
      - 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*, each state may want to prepare a separate, more detailed specification for CVIEW and any other new systems.

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 the FMCSA-developed CVIEW, or will it implement an 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?
- Will the state use SAFER instead of implementing a CVIEW?
- What data formats will the state use in interfacing with SAFER?
- 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?
- What systems in the state will provide snapshot segment updates?
- What snapshot views will be used where?
- 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 Subsection D.6, Requirements Specification, for more discussion.)
- Within the state, the use of a CVIEW to serve as a single interface node 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 LSIs.

D.2 Program and Project Planning Phase

Program and Project Planning Phase Process

The *CVISN Guide to Program and Project Planning* (Reference 21) describes the general process for developing a project plan and organizing the project. Figure D-3 that portrays this process is repeated below as a reminder.

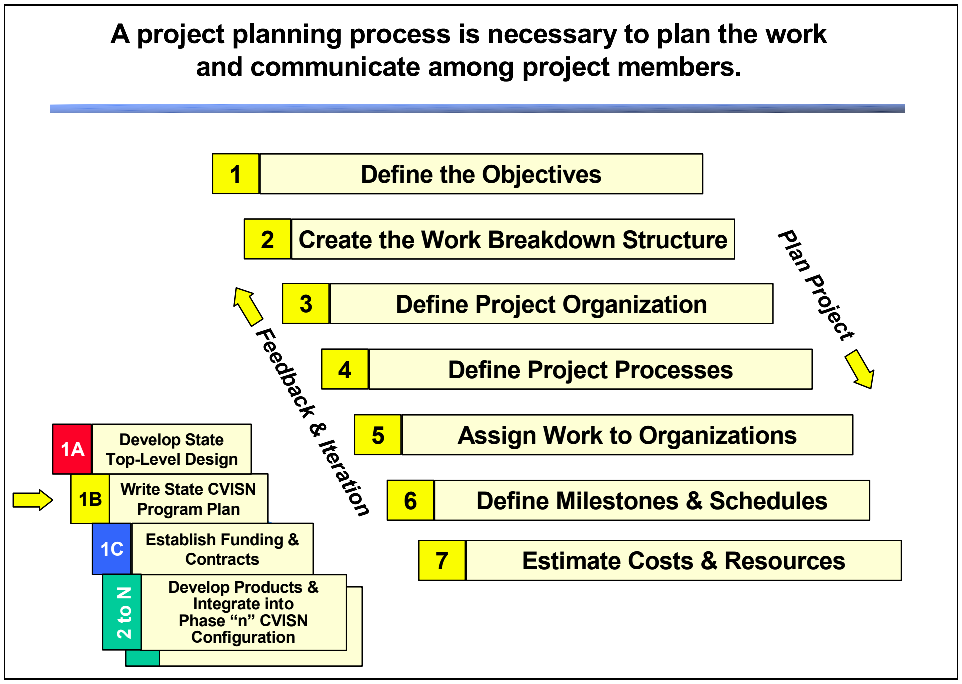

A project planning process is necessary to plan the work and communicate among project members.
1 Define the Objectives
2 Create the Work Breakdown Structure
3 Define Project Organization
4 Define Project Processes
5 Assign Work to Organizations
6 Define Milestones & Schedules
7 Estimate Costs & Resources
Plan Project
Feedback & Iteration
1A Develop State Top-Level Design
1B Write State CVISN Program Plan
1C Establish Funding & Contracts
2 to N Develop Products & Integrate into Phase "n" CVISN Configuration

Figure D–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

- Other projects are going on in the state that may affect 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 the 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 existing systems are being modified 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 the state have on the use of the Web? Is there a program in the state to actively promote “electronic government” and deliver more services over the Web and the Internet? Can development leverage on these programs?
- What type of internal methodology has the 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 the 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? Is it possible to leverage on their progress, 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 recompete/redevelop?
- When will the state connect to SAFER?
- Will the state participate in the 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?

D.3 Funding and Contracts Phase

Funding and Contracts Phase Process

The *CVISN Guide to Program and Project Planning* (Reference 21) describes the general process for the funding and contracting phase. Figure D-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. A specific process should be developed that meets the needs of each individual state.

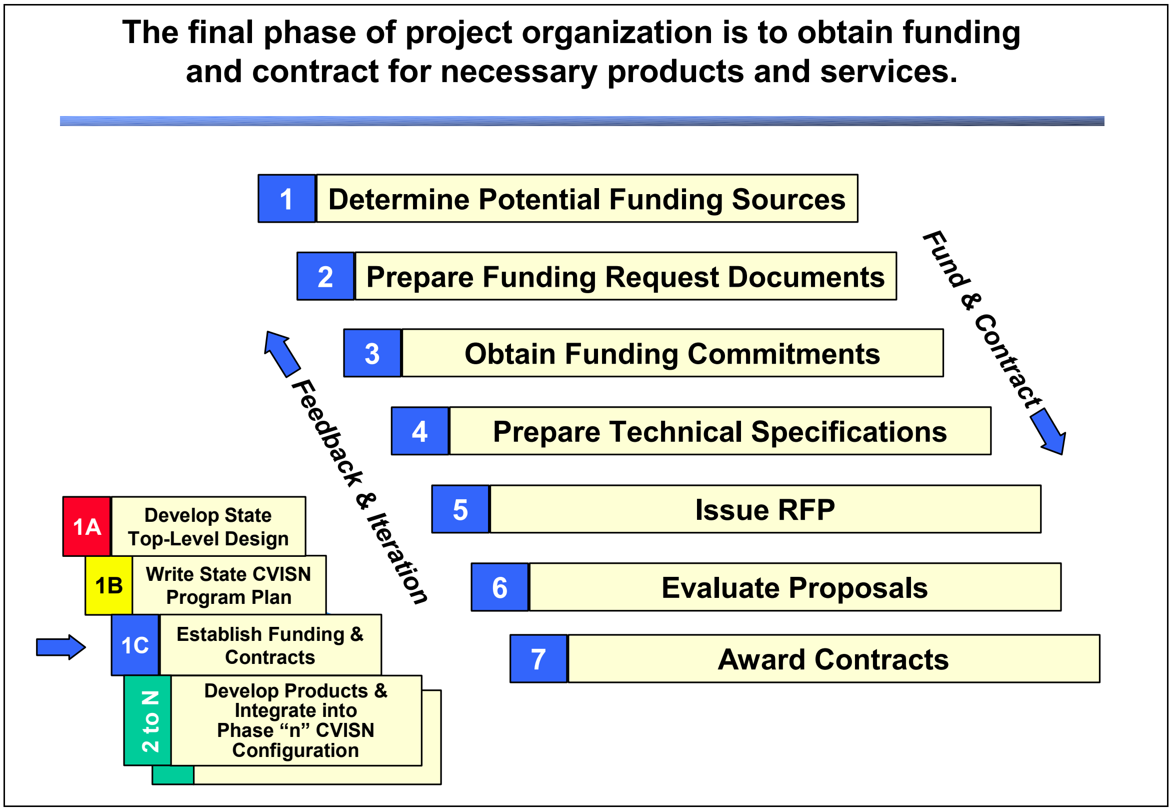

The final phase of project organization is to obtain funding and contract for necessary products and services.
1 Determine Potential Funding Sources
2 Prepare Funding Request Documents
3 Obtain Funding Commitments
4 Prepare Technical Specifications
5 Issue RFP
6 Evaluate Proposals
7 Award Contracts
Fund & Contract
Feedback & Iteration
1A Develop State Top-Level Design
1B Write State CVISN Program Plan
1C Establish Funding & Contracts
2 to N Develop Products & Integrate into Phase "n" CVISN Configuration

Figure D–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., 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 from FMCSA that can be used as a starting point (although customization and operations and maintenance support will be required). Several states have developed their own versions of CVIEW, which may be available from the states or their vendors.
- 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 nonperformance 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 COTS packages:* The requirements analysis approach is required, but not as critical as with custom development. This is a case of buying what vendors already have. In this case, an opportunity to “try before you buy” is very important. Consider including a preliminary demonstration phase in the contract that allows 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 the systems integration agent and software services vendors. This allows definition of 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 a state purchases an existing CVIEW, it is likely to require substantial modification and customization to fit in that state's Information Technology (IT) environment. It may need custom legacy system interfaces. That state may have slightly different processes than other states using the product, or it 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.

D.4 Development Phase "n"

Development Phase "n" Process

The *CVISN Guide to Phase Planning and Tracking* (Reference 22) describes the general process for developing and maintaining a Phase Plan and tracking progress as the phase proceeds. Figure D-5, which portrays this process, is repeated below as a reminder.

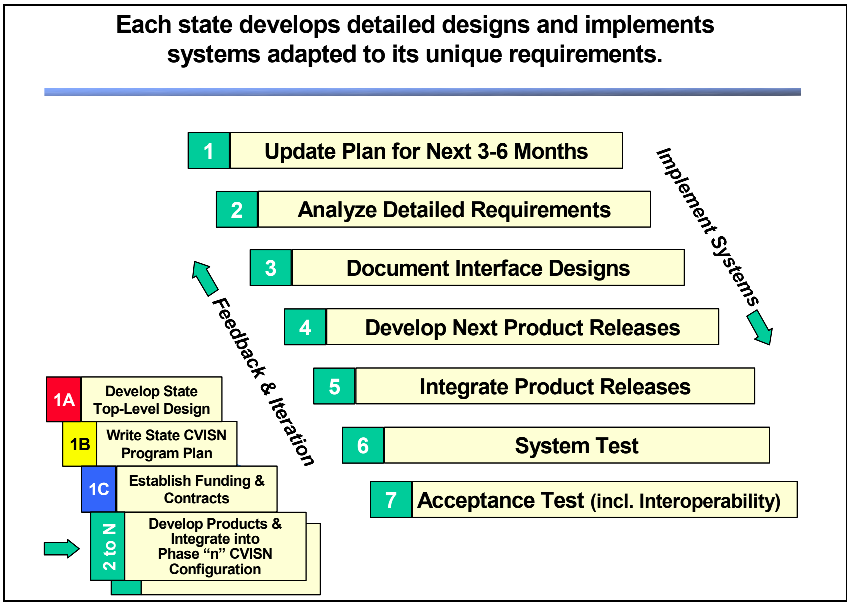

Each state develops detailed designs and implements systems adapted to its unique requirements.
1 Update Plan for Next 3-6 Months
2 Analyze Detailed Requirements
3 Document Interface Designs
4 Develop Next Product Releases
5 Integrate Product Releases
6 System Test
7 Acceptance Test (incl. Interoperability)
Implement Systems
Feedback & Iteration
1A Develop State Top-Level Design
1B Write State CVISN Program Plan
1C Establish Funding & Contracts
2 to N Develop Products & Integrate into Phase "n" CVISN Configuration

Figure D–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”

- It is important 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 requirements should be published in a *State of ___ Motor Carrier Safety Information Exchange 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 (CM) 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.
- If an incremental development process is being used, 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. A strong system integrator and problem resolution process is required to deal with this.
- An early indicator of a vendor's ability to perform is provided by checking 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 about their other assignments. Step back and perform a "sanity check" on staffing levels. Ask yourself if it is realistic to expect the desired work to be accomplished with the effort being applied.
- Hopefully, careful planning will allow things to go well with vendors. Nevertheless, be sure to have contractual remedies in place just in case they do not. 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*, References 9-11) when possible. An absence of test data can cause insufficient testing and allow problems to go undetected until after systems are put into production.
- Changes in requirements can kill project schedules and cause cost overruns. An effective 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 24.

D.5 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 a 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 results and leaves the details to be developed as part of the phased development process is more likely to succeed. Remember that the objective is to produce a top-level requirements specification that limits the project scope, is concise, testable, and provides a basis for establishing and managing a contract.

One suggested approach is to use the *State CVISN System Design Description* as the basic source of requirements for 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 (Reference 2)
- COACH Part 3, Detailed System Checklists (Reference 16)
- COACH Part 4, Interface Specification Checklists (Reference 14).

Review and edit these, filling them out and customizing them as required to meet state-specific needs.

An 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. Refer to the COACH Part 5 (Reference 8) and the *CVISN Interoperability Test Suite Package* (References 9, 10, 11) 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 the state team to develop these detailed process designs.

Alternative B: Delta Requirements

If a state is using a largely COTS approach, it may want to consider a variation on Alternative A. Create a simplified requirements specification based on the 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) requirement specification that describes what changes are desired to their product. The contractor may use checklists, JAD sessions, focus groups, interviews and other techniques to collect these "delta" requirements.

Preparation of delta requirements is in lieu of a detailed description of each scenario or business process. If the product comes very close to satisfying the needs, 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 are not the ones developing the system, much of the investment remains locked in the heads of the analysts who wrote the specs. Thus, this information is not transferred to the developers. As a result, it is likely that the developers will want to redo this work themselves and get the users' perspective first hand.
- User personnel often do not 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 requirements documents and actually understand what they are getting. When they finally see the system, they will realize that there were many things they wanted that did not occur to them when reviewing the specs.

However, if a state has worked successfully with comprehensive, detailed requirements specifications before and this is what is desired for this project, consider issuing a partial draft of the requirements specification as part of the 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 25 and 26) 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.

APPENDIX E.

CVIEW-SAFER CONNECTIVITY VIA VPN/IPSEC

This Page Intentionally Blank

APPENDIX E. CVIEW-SAFER CONNECTIVITY VIA VPN/IPSEC

INTEROFFICE MEMORANDUM
TO: CVIEW SITE PRIMARY POINT OF CONTACT (POC)
FROM: FMCSA TECHNICAL SUPPORT
SUBJECT: VPN/IPSEC CONNECTIVITY TO SAFER
DATE: NOVEMBER 21, 2001

1. PURPOSE

Coordinate the exchange of information and procedures for establishing a persistent, secure, LAN-to-LAN VPN/IPSec connection between state CVIEW System sites and SAFER.

2. BACKGROUND

CVIEW systems have been designed to send and receive information from the Safety and Fitness Electronic Records (SAFER) system. As SAFER can also independently "push" information to the CVIEW sites, a persistent secure network connection is needed between the CVIEW sites and SAFER.

Two options are currently available for establishing this type of connection:
AAMVAnet Frame Relay, IP based network connection; LAN-to-LAN, VPN IPSec based Internet connection (persistent VPN connection).

The AAMVAnet point of contact for establishing a Frame Relay, IP based network connection to SAFER is Patrice L. Aasmo (paasmo@aamva.org or 703-908-5787).

Secure 2-way connectivity with SAFER can also be accomplished over the Internet by establishing a persistent virtual private network (VPN) LAN-to-LAN connection between an appropriate firewall attached to the State's network, and the SAFER VPN Concentrator located at Volpe. This method is presently used between Volpe and the Johns Hopkins University Applied Physics Laboratory (JHU/APL). The appropriate State's firewall would protect the state network(s) from unauthorized Internet access, and would need to be capable of being configured for the VPN/IPSec LAN-to-LAN connection.

The FMCSA is utilizing the Cisco VPN/IPSec solution for allowing authorized FMCSA Field System application users to connect to SAFER over the Internet. The client version of this software can be provided (without charge) to authorized users of FMCSA applications.

Once the described VPN/IPSec LAN-to-LAN persistent connection is established, other users of FMCSA Field Systems applications (PIQ, SAFETYNET 2000, etc.) connected to the same LAN as the CVIEW system can also connect to SAFER.

This memorandum provides the process and general procedures for setting up this connection.

3. GENERAL PROCEDURES

FMCSA has delegated responsibility for operation, maintenance and security of SAFER to the Volpe National Transportation Systems Center. To establish a persistent secure VPN/IPSec connection from state CVIEW sites, the following steps must be taken:

- The **CVIEW primary point of contact (POC)** will first have to provide Volpe with limited network topography information, a primary point of contact (POC) and individual points of contact for application users, network, firewall, and security administration.

- **Volpe** network administration and security personnel will then contact the primary POC to coordinate the configuration of both the State firewall and Volpe VPN Concentrator to accommodate the connection. **Volpe** will provide the user and/or their local network, firewall, and security administrators with requirements to open specific firewall ports needed to support the VPN/IPSec connectivity. These configuration changes should be made on the highest-level firewall within the state's network topography that exists between the CVIEW server and the Internet. In this manner the state network administration and security officials can control access and use of the VPN tunnel between the state and SAFER. When ready, the **CVIEW POC** will also be provided user names and passwords for authenticating on the Volpe VPN Concentrator.

- Finally, the **CVIEW POC** and **Volpe** teams will coordinate a test of the connectivity.

4. NEXT STEPS:

If you are interested in utilizing the VPN/IPSec solution for connectively with SAFER, please provide the following information to FMCSA Technical Support:

- General system topography information (i.e. a one line drawing-depiction with text notations) describing the proposed network path between the CVIEW server and SAFER. Include operating systems, firewall applications, and router hardware used. (Example: CVIEW is set up on a WinNT 4.0 Server, connected to a Cisco Catalyst 2900 switch, connected to a Cisco 7513 Router, connected to a Cisco Catalyst 5500 switch, connected to a WinNT 4.0 Server running Microsoft Proxy Server. The firewall is at the Proxy server, no firewalls in between.)
- Primary point of contact (POC) within your organization that is responsible for CVIEW connectivity to SAFER. This is to provide a centralized point of contact for coordination of the installation and future questions that may arise.
- Contact information for person to receive User Account and Password information.
- Contact information for person to contact regarding firewall activities.
- Contact information for local Network Engineer, if available.

The above information will be used by Volpe system administration, firewall, and security personnel to assist the requesting agency establish a reliable VPN/IPSec connection to SAFER, and to diagnose and rectify problems once the connection is deemed operational.

The requested information should be sent to FMCSA Technical Support via phone to (617) 374-5090 (Roadside Inspection Systems Group), Fax to (617) 374-2336, or email to FMCTechSup@volpe.dot.gov (Subject VPN/IPSec Connectivity).

This Page Intentionally Blank