Multi-Modal Traveler Information System

Gateway Design Options
Working Paper # 19220.01

De Leuw, Cather & Co mpany

ue Date: May 19, 1997

in association with:
JHK & Associates

Gateway Design Options
Working Paper # 19220.01

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this working paper is to provide insight into the options that are available from which to design the Gateway Traveler Information System (TIS). This working paper will discuss each option in a general manner without becoming overly technical. It allows for an in-depth look at all of the available technologies and their potential applicability in the Gateway. The Gateway design options will be combined with the Gateway user needs and lessons learned from other similar Intelligent Transportation Systems (ITS) projects to produce the Gateway System Definition Document and the Gateway Functional Requirements Document.

1.1.1 Goals of this Working Paper

The goals of this working paper are as follows:

- To present the possible ways to implement the overall architecture and specific components of the Gateway TIS.
- To provide a solid research base from which the final Gateway TIS design will be chosen.

It should be noted that this Working Paper will not address recommendations on a specific architecture or Gateway structure, recommendations will be addressed in the System Definition Document, Working Paper # 17150.

1.1.2 Intended Audience

This working paper is intended to serve as a resource and a guide to the members of the Gary-Chicago-Milwaukee (GCM) Deployment Committee, Architecture, Communications and Infrastructure (ACI) Work Group, project managers, system designers, system developers and system integrators.

1.1.3 Working Paper Organization

This working paper is organized in the following manner. Section 1 provides an introduction and describes the overall goals of this paper. Section 2 discusses the National Architecture for ITS. Section 3 discusses three different architectures that can be used for the Gateway. Sections 4 and 5 discuss hardware and software respectively. Section 6 presents different networking options. Section 7 describes options for interfaces to other systems in terms of national standards, along with options for collection and distribution methods. Section 8 provides a summary of the Gateway Design Options Working Paper.

1.2 PROJECT OVERVIEW

The Multi-Modal Traveler Information System (MMTIS) project involves research in the areas of ITS systems in the corridor which are currently deployed and proposed systems identified in regional strategic plans or early deployment studies. This information is used to develop a corridor architecture which best suits the characteristics of the diverse resources within the corridor. Along with the corridor architecture, a corridor strategic plan will be developed. Another key component of the MMTIS project is the design of the Gateway Traveler Information System. The Gateway will be the collection and distribution hub for traveler information

in the GCM Corridor. Specific tasks identified in the MMTIS project include developing the following documents for the Gateway: System Definition Document, Functional Requirements Document and Interface Control Requirements Document.

1.3 DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Document #17100-1, MMTIS Project Glossary, contains all definitions, acronyms and abbreviations associated with this project, as well as pertinent ITS, communications, computer programming and other standards in general.

1.4 RELATED DOCUMENTS

This working paper is part of a series of documents and working papers produced to support the design of the GCM Corridor Multi-Modal Traveler Information System.

Related documents and working papers include:

- Document #17100-1 - MMTIS Project Glossary
- Document #17150 - Gateway TIS System Definition Document
- Document #17200 - GCM Corridor Architecture Functional Requirements
- Document #17250 - Gateway TIS Functional Requirements
- Document #17300 - GCM Corridor Architecture Interface Control Requirements
- Document #17350 - Gateway TIS Interface Control Requirements
- Working Paper #18250 - Cellular 911 - State of the Practice
- Working Paper #18380 - GCM Corridor User Needs and Data Exchange Requirements
- Working Paper #18400 - Summary of Regional Strategic Plans
- Working Paper #18500 - GCM Corridor Strategic Plan
- Working Paper #18520 - Performance Criteria for Evaluating GCM Corridor Strategies and Technologies
- Working Paper #18550 - Alternative GCM Corridor Technologies
- Working Paper #18555 - Alternative GCM Corridor Strategies
- Working Paper #18600 - System Interfaces and Information Exchange
- Working Paper #18700 - Information Clearinghouse - Initial Administrative Network
- Working Paper #18790 - Information Clearinghouse - Final Network
- Working Paper #18830 - Weather Detection System Standard Message Sets
- Working Paper #19140 - Gateway TIS Phased Implementation Plan
- Working Paper #19210 - Lessons Learned
- Working Paper #19840 - Variable Message Signs (VMS)/Highway Advisory Radio (HAR) State of the Practice
- Working Paper #19845 - VMS/HAR Suggested Guidelines.

2.0 NATIONAL ITS ARCHITECTURE

A National Intelligent Transportation System (ITS) Architecture provides a framework for the design of ITS by defining the interfaces and communications requirements for the information flows between physical subsystems. The National ITS Architecture Project was recently completed by the U.S. Department of Transportation and Federal Highway Administration. This National ITS Architecture is the key to providing a base for the standards needed to support national and regional interoperability. The National ITS Architecture was specifically designed to allow multiple design approaches to be used for specific environments and individual needs of the user by defining only required interfaces and their communications.

The National ITS Architecture goals, objectives, definitions and its evaluation and deployment are documented in extensive volumes. The specific documents that are directly related to this project are the architecture definition documents which consist of:

- "ITS Logical Architecture," January 1997, United States Department of Transportation (USDOT), Federal Highway Administration (FHWA). This document represents a functional review of the ITS user services. It defines the functions or process specifications that are required to perform the ITS user services.

- "ITS Architecture Definition Theory of Operations," March 1996, USDOT, FHWA. This document defines the data flows that need to be created to provide the functions defined by the logical architecture. This document also identifies those interface standards that are supported by the national architecture.

- "ITS Architecture Implementation Strategy," April 1996, USDOT, FHWA. This document defines a series of steps to encourage efficient deployment of architecture-compatible ITS systems.

The MMTIS project will be designed to maximize compliance with the National ITS Architecture. Full compliance may not be possible at this point in time due to the large number of existing systems in the Corridor. Additionally, the National ITS Architecture is continuing to evolve.

Hence, as the National ITS Architecture is a very major input to the MMTIS project, the following sections are devoted to describing the Physical Architecture in a way that presents all the fixed relationships, data flows and interfaces which can be accommodated by the architecture. A two level approach will be used, presenting first the architecture for the subsystems (implementation level) and then the architecture for the user services (operational level). The interface standards which are supported by the National ITS Architecture will also be described in the sections that follow.

2.1 IMPLEMENTATION LEVEL PHYSICAL ARCHITECTURE

2.1.1 Subsystems

The National ITS Architecture has identified 19 different subsystems that can exist within an ITS. A subsystem is a set of functions which represent the smallest units of ITS that can be purchased and deployed. Each function necessary for the present to 20-year time frame is covered within the 19 subsystems. An ITS deployment may consist of one or more subsystems and within each subsystem one or more functions based on local deployment choices. Each subsystem is grouped into either Center Subsystems, Roadside Subsystems,

Remote Access Subsystems, or Vehicle Subsystems as defined below:
Center Subsystems - These subsystems are grouped together because of their dependence on wireline communications. Center Subsystems can be located anywhere as long as there is communications media available.

- Emergency Management Subsystems - enable coordination of emergency response crews.
- Emissions Management Subsystems - perform data collection on vehicle emissions and the environment and transfer this data to any subsystem that may require it.
- Planning Subsystems - model an ITS, using data collected from other subsystems. Transportation planners use the output from the planning subsystems for evaluation and other planning efforts.
- Transit Management Subsystems - collect and analyze data from the transit fleets and provide real-time management strategies as well as evaluate operations.
- Toll Administration Subsystems (TAS) - collect and process data from the toll collection subsystem for audit purposes and evaluate operations.
- Traffic Management Subsystems (TMS) - analyze data received from various field equipment and provide real-time traffic management and incident management. TMS also provides real-time control for transit signal priority and emergency vehicle signal preemption.
- Fleet and Freight Management Subsystems - collect and analyze data from commercial fleets and provide real-time management strategies, coordination with intermodal depots and shippers and evaluate operations.
- Information Service Provider (ISP) Subsystems - typically, a private enterprise collects and processes data from a combination of Transit Management Subsystems, Traffic Management Subsystems, Emergency Management Subsystems, Parking Management Subsystems and Commercial Vehicle Administration Subsystems. These subsystems then provide data to travelers for pre-trip travel information, route guidance, demand-responsive transit, ride matching and other traveler information services. The ISPs may also utilize their private clients (data recipients) to collect probe data which may in turn be shared with the Traffic Management Subsystem. In the case of the GCM Corridor, an ISP could receive information from the C-TIC or the Gateway. Additionally, the C-TIC/Gateway can also be thought of as an ISP based on the definition used in the national system architecture which does not specify that the ISP is public or private.
- Commercial Vehicle Administration (CVO) Subsystems - interface between CVO Information Requestors and CVO fleets. They sell credentials, administer taxes, keep safety records, provide credential check data and exchange information with other Commercial Vehicle Administration Subsystems.

Roadside Subsystems - This group of subsystems also relies on wireline communications or at least some form of point-to-point communications, but they must be co-located with a roadside transportation system to enable access to sensors, signals, programmable signs, or interfaces with travelers, vehicles and fleet operators.

- Roadway Subsystems - provide traffic management surveillance, signals and signage for traveler information.

- Toll Collection Subsystems - collect tolls and identify violators.

- Parking Management Subsystems - collect parking fees and inform users of parking lot occupancy.

- Commercial Vehicle Check Subsystems - collect credential and safety data from the vehicles, determine conformance to requirements, inform driver of results (and/or carrier) and provide results to the Commercial Vehicle Administration Subsystem.

Remote Access Subsystems - These subsystems provide data to travelers or carriers in support of multi-modal traveling. The manner in which data are provided could be through a fixed terminal, a portable terminal or other means.

- Remote Traveler Support Subsystems - include an electronic kiosk located in a public location to provide traveler information as well as security functions.

- Personal Information Access Subsystems - include a home/office/portable computer for traveler information and emergency requests.

Vehicle Subsystems - All of these subsystems reside in a vehicle and support vehicle-to-roadside communications, vehicle-to-center communications and vehicle-to-vehicle communications.

- Vehicle Subsystems - are equipment and functions that are common across all vehicle types (navigation and tolls), including advanced vehicle safety and operations systems.

- Transit Vehicle Subsystems - provide operational data to the Transit Management Center, receive transit network status, provide en route traveler information to travelers and provide passenger and driver security functions.

- Commercial Vehicle Subsystems - store safety data, identification numbers (driver, vehicle and carrier) and last-check event data as well as provide in-vehicle signage for driver pass/pull-in messages.

- Emergency Vehicle Subsystems - provide vehicle and incident status to the Emergency Management Subsystem.

A graphical representation of the subsystems is presented in Figure 2-1.

2.1.2 Architecture Layers

Figure 2-1 also reveals the layering scheme the Architecture uses on the implementation level. Implied, but not shown, the layering scheme includes an institutional layer, communications layer and the transportation infrastructure layer. The institutional layer is inferred only by the various center subsystems that will need to be coordinated as shown by the communications links. The communications layer is shown by the lines

connecting the subsystems with various communications media. The transportation infrastructure is represented by the subsystem rectangles. These three layers allow a separation between institutional issues, functional issues and communications issues. In this way, subsystem functionality remains separate and independent of communications media and institutional issues and relationships. This means the system deployer may provide unique institutional arrangements, as long as they facilitate the functions of the subsystem.

2.2 OPERATIONAL LEVEL PHYSICAL ARCHITECTURE

It is by looking at the operational level that the National ITS Architecture is able to provide a complete definition of an ITS. At the operational level, the National ITS Architecture defines data interfaces and communications requirements for a complete ITS deployment for all of the 30 user services defined by the Federal Highway Administration (FHWA). A user service is the very smallest component of an ITS system that is still independent of technologies or implementation strategies. User services provide a wide range of functions that could be required within an ITS. The FHWA has identified 29 user services. One additional user service is in the process of being defined; the 30th user service will be Railroad Grade Crossings. More user services may be added in the future. A listing of these 30 user services is provided in Table 2-1.

Table 2-1 User Services

	USER SERVICE	DESCRIPTION
1	En-Route Driver Information	Provides driver advisories and in-vehicle signing for convenience and safety.
2	Route Guidance	Provides travelers with simple instructions on how to best reach their destinations.
3	Traveler Services Information	Provides a business directory, or "yellow pages," of service information.
4	Traffic Control	Manages the movement of traffic on streets and highways.
5	Incident Management	Helps public and private organizations quickly identify incidents and implement a response to minimize their effects on traffic.
6	Emissions Testing and Mitigation	Provides information for monitoring air quality and developing air quality improvement strategies.
7	Demand Management and Operations	Supports policies and regulations designed to mitigate the environmental and social impacts of traffic congestion.
8	Pre-Trip Travel Information	Provides information for selecting the best transportation mode, departure time and route.
9	Ride Matching and Reservation	Makes ride sharing easier and more convenient.

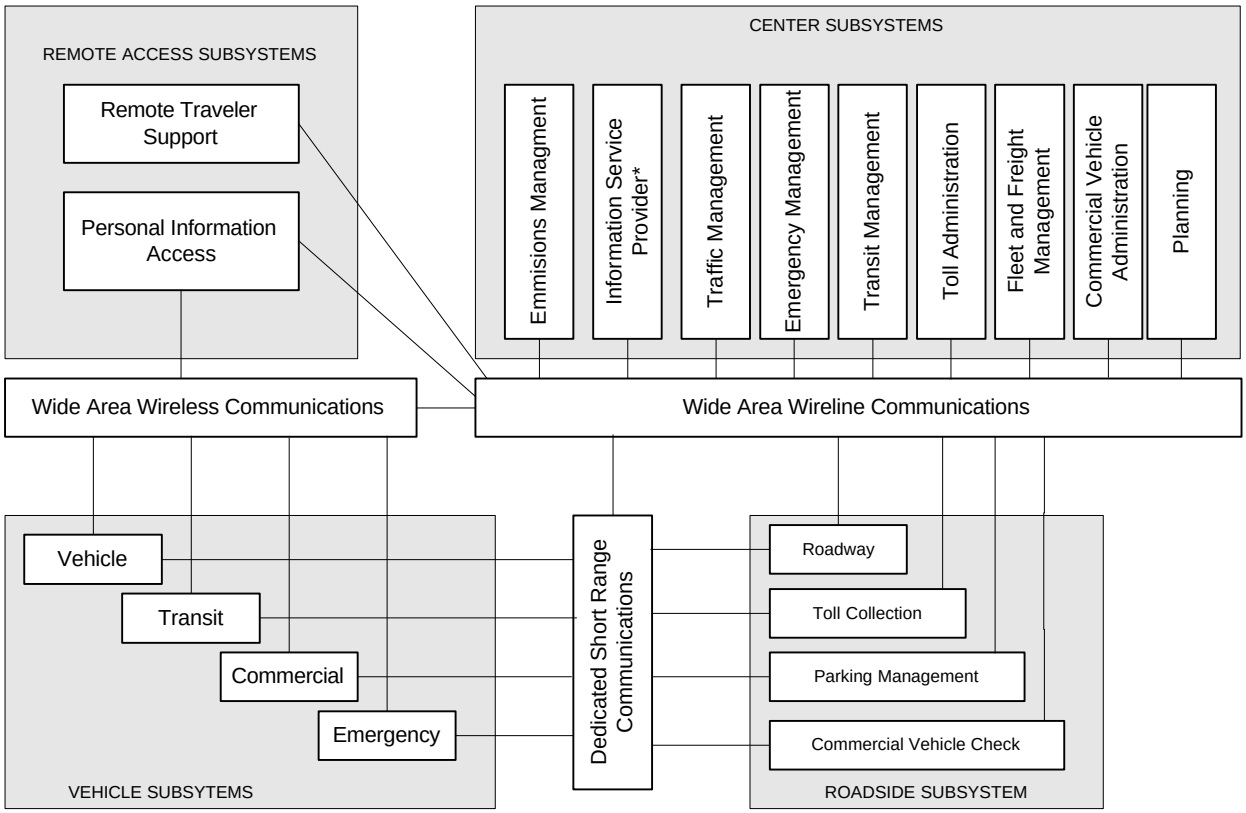
	USER SERVICE	DESCRIPTION
10	Public Transportation Management	Automates operations, planning and management functions of public transit systems.
11	En-Route Transit Information	Provides information to travelers using public transportation after they begin their trips.
12	Personalized Public Transit	Provides flexibly-routed transit vehicles to offer more convenient customer service.
13	Public Travel Security	Creates a secure environment for public transportation patrons and operators.
14	Electronic Payment Services	Allows travelers to pay for transportation services electronically.
15	Commercial Vehicle Electronic Clearance	Facilitates domestic and international border clearance, minimizing stops.
16	Automated Roadside Safety Inspection	Facilitates roadside inspections.
17	On-board Safety Monitoring	Senses the safety status of a commercial vehicle, cargo and driver.
18	Commercial Vehicle Administrative Processes	Provides electronic purchasing of credentials and automated mileage and fuel reporting and auditing.
19	Hazardous Materials Incident Response	Provides immediate description of hazardous materials to emergency responders.
20	Freight Mobility	Provides communication between drivers, dispatchers and intermodal transportation providers.
21	Emergency Notification and Personal Security	Provides immediate notification of an incident and an immediate request for assistance.
22	Emergency Vehicle Management	Reduces the time it takes for emergency vehicles to respond to an incident.
23	Longitudinal Collision Avoidance	Helps prevent head-on, rear-end or backing collisions between vehicles, or between vehicles and other objects or pedestrians.
24	Lateral Collision Avoidance	Helps prevent collisions when vehicles leave their lane of travel.
25	Intersection Collision Avoidance	Helps prevent collisions at intersections.

	USER SERVICE	DESCRIPTION
26	Vision Enhancement for Crash Avoidance	Improves the driver's ability to see the roadway and objects that are on or along the roadway.
27	Safety Readiness	Provides warnings about the condition of the driver, the vehicle and the roadway.
28	Pre-Crash Restraint Deployment	Anticipates an imminent collision and activates passenger safety systems before the collision occurs, or much earlier in the crash than is currently feasible.
29	Automated Highway System	Provides a fully automated, "hands-off," operating environment.
30	Railroad Grade Crossings	Increases safety of at-grade railroad crossings by providing additional warnings and restraint systems.

An ITS could deploy just a few user services, all of them or even some additional local area specific user services. It is the National ITS Architecture that provides a roadmap to system deployers on what interconnections each user service or individual component requires to be fully functional. In so doing, the National ITS Architecture identifies all necessary data flows for each component.

Each interface must supply the components with their required data at their required functionality. In other words, the interface must be standard. The ITS Architecture supports open communications standards and requires that the interface is able to network with other communications media by utilizing open Internet working standards. The Architecture also requires that the communications media provide the necessary coverage for each component.

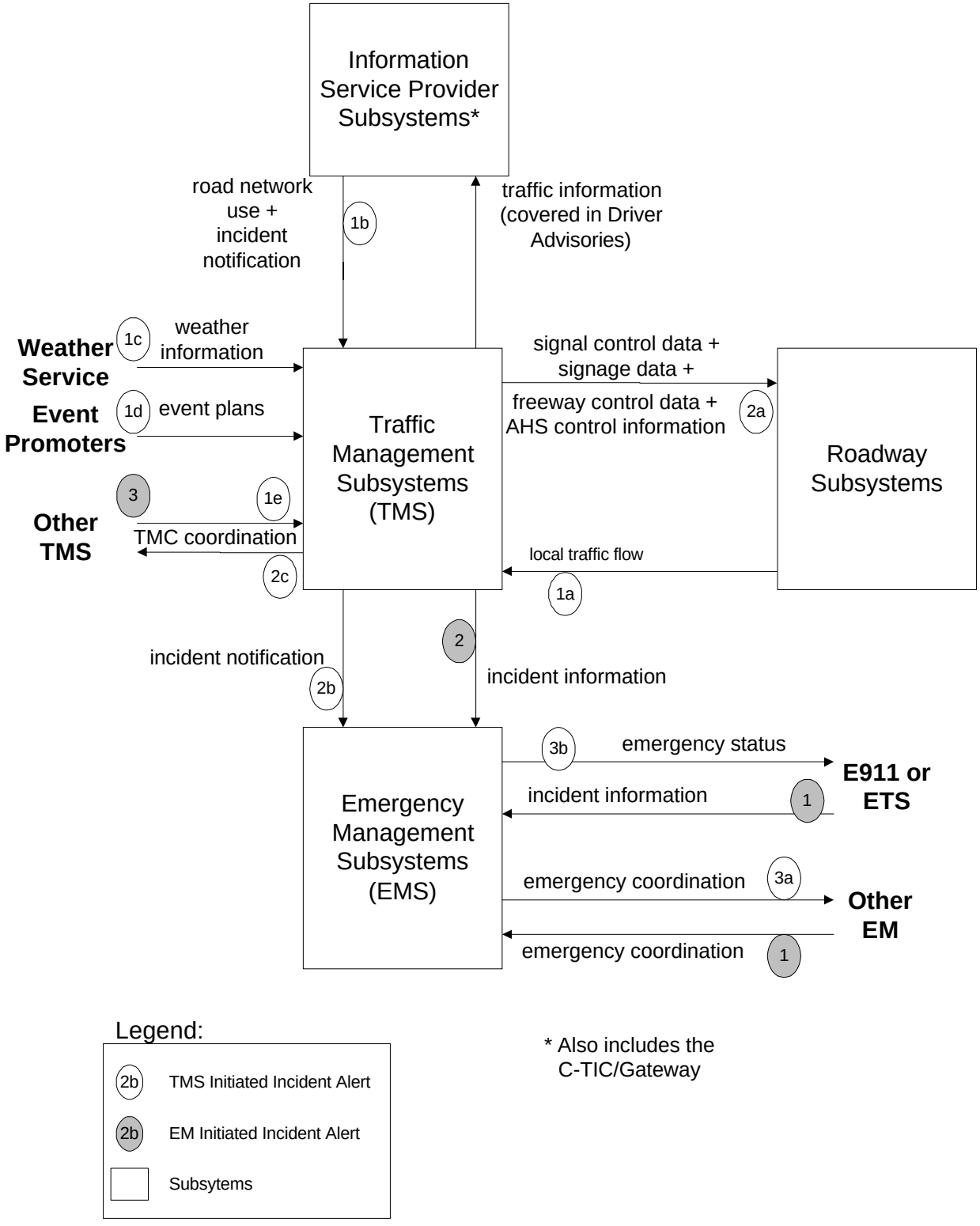
Figure 2-1 National ITS Physical Architecture



* Also includes the C-TIC/Gateway

Figure 2-2 shows an example of the physical architecture diagrams that were developed for each user service. These diagrams are used to describe the subsystems which are used to implement each user service. The arrows represent data flows between the subsystems and indicate originator and receiver by the direction of the arrow. The sequence of architectural processing is shown by the ordered numerical labels assigned to each data flow. Figure 2-2 and the text that follows have been included here to provide an example of the extent to which the National ITS Architecture details subsystem interfaces and describes data operations.

Figure 2-2 Physical Architecture for Incident Management



2.2.1 Input Data Flows and Processes

The data input streams for the Incident Detection User Service provide data that the Traffic Management Center processes to determine incident status. These input data streams are continuously polled for data. Input data flows include the Roadway Subsystem (1a) where local traffic flow data is collected by video surveillance and vehicle detector stations. The Information Service Provider Subsystem also can be a data source (1b) if probes are used to monitor road network usage and incidents. External data sources could be used which include weather information (1c) from a Weather Service provider and scheduled event plans from an event promoter (1d). Additionally, there are other Traffic Management Centers that could provide information on incidents within their jurisdiction (1e). Similarly, emergency service patrols could also provide data on an incident that is occurring within their jurisdiction and can coordinate directly with other Emergency Management Subsystems.

2.2.2 Output Data Flows and Processes

The Traffic Management Center (TMC) then processes the data to determine the possibility and/or impacts of an incident. The TMC then provides the appropriate control strategies to the traffic signal controllers, freeway control systems (variable message signs, ramp metering, etc.) and the Automated Highway System to facilitate real-time traffic control (2a). The Emergency Management Subsystem is notified (2b) as well as other TMCs (2c). The other TMCs respond with an incident alert message (3).

The next steps (3a, 3b) are carried out by the Emergency Management Subsystem to provide the emergency status to other E911 or emergency response systems and coordinate a response with other Emergency Management Subsystems.

As described above and shown on Figure 2-2, the data flows are identified and the relationships among messages are clearly defined. The National ITS Architecture has provided this framework for each user service (or group of similar user services) in the Theory of Operations Definition Document listed on page 2-1.

2.3 NATIONAL ITS ARCHITECTURE STANDARDS

The developers of the National ITS Architecture envisioned that ITS systems would be deployed in an ad-hoc manner with a variety of combinations of subsystems and functionality. To ensure national and regional compatibility, standards for the architecture's interfaces and data flows are necessary. Standardization insures a greater degree of manufacturer competition which will provide a wide range of product and service functionality at a competitive price. Standardization also allows for interoperability of components and subsystems.

Since the standards cannot be developed and imposed on manufacturers immediately, a Standards Development Plan (SDP) was created by the Federal Highway Administration. The SDP identifies potential standards based on the data flows and interfaces defined in the Physical Architecture.

According to the SDP, of the 125 interfaces defined in the Physical Architecture, 45 require nationwide compatibility. An example of this is the dedicated short range interface between a vehicle and the roadside. A nationwide standard for this interface will allow travelers and commercial vehicles to use their compliant equipment anywhere within the United States.

National interoperability is specified for all interfaces to mobile subsystems:

- Information Service Provider (ISP) to Personal Information Access Subsystem
- Toll Collection Subsystems to Vehicle Subsystems and
- Commercial Vehicle Subsystems to Commercial Vehicle Check Subsystems.

Regional interoperability is specified when the coordination issues are regional rather than national in scope:

- Traffic Management Subsystems to Transit Management Subsystems
- Traffic Management Subsystems to Information Service Provider and
- Traffic Management Subsystem to Traffic Management Subsystem.

It should be noted here that the MMTIS project requires communication between regional TMSs, thus, it should follow regional standards. There is nothing, however, to prevent the regional standard from following a national standard (e.g. NTCIP, see Section 7.1).

The SDP considers three types of standards as defined below:

- regulatory standards - are those established by a governmental agency for the welfare and safety of the public (e.g., a standard governing the integration of a route guidance driver's interface with an automobile).

- de facto standards - are those established by someone in industry who designs, builds, or establishes a product or service which then becomes an accepted industry practice.

- voluntary standards - are those established by a voluntary consensus among manufacturers, integrators, service providers and consumers.

Almost all ITS standards are voluntary standards, although the National ITS Architecture is flexible enough to support all types of standards.

The architecture identified sixteen key standards areas that are relatively independent. Each area covers specific interfaces that have common data elements. For example, map databases are used in several applications and have impact on several stakeholders, but each map database conforms to the same standard. Developers of the standards do not have to create totally new standards; there are several standards already in existence that can be incorporated into an ITS Standard.

Standards activities for each of these sixteen areas are in various stages of completion as shown in Table 2-2. Table 2-2 also lists the status of their activities summarized as well.

Table 2-2 Standards Development Status[1]

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
01	Dedicated Short Range Comm. (DSRC)	Advanced Traffic Controller 2070 (an open architecture standard for hardware, software and user interfaces).	Software documentation guidelines is being developed (due June 1997). ATC application program interface and data module definitions being developed (due June 1997).
		Advanced Traffic Management System (ATMS) Data Dictionary (DD) (Develop an ATMS DD including data elements for ATMS messages used within TMCs and communicated external to TMCs by ATMS).	ITE: Prototype completed, formal development begun.
		ASTM1 DSRC Protocol (Physical and data link standards for beacons).	ASTM - Standards for physical and data link layers under development. Both active and back scatter physical layers will be supported with a single data link layer.
		CVISN Architecture and Design (Develops EDI Standards for CVO Wireless).	ANSI - draft completed
		CVO-TS285 CVO Safety & Credentials Information Exchange (Form and Content of Messages).	IEEE/SAE - none
		Guidelines for vehicular radar.	IEEE Status unknown.
		IEEE1 Development of draft standards for DSRC Message Sets (IEEE Working Group P1455).	IEEE: draft to be completed 9/30/97
		IEEE2 Message Sets for DSRC for AVI.	Project plan under review by FHWA
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.

[1] *Standards Development Plan*, National ITS Architecture, FHWA and the *ITS America "Standards Link Page,"* http://www.itsa.org.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
02	Digital Map Data Exchange and Location Referencing	ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.
		ORNL Spatial Data Interchange (Develop an ITS profile to the Spatial Data Transfer Standard FIPS 173).	Project team has been assembled and are reviewing existing standards.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
03	Information Service Provider Wireless Interfaces	IEEE2 Message Sets for DSRC for AVI.	Project plan under review by FHWA.
		PCS for APTS.	Status Unknown.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
		SAE2 High Speed FM Subcarrier Protocol for EMS (Form and content of messages for real-time emergency notification from the Emergency Management Center to other centers.	A standard has been proposed.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		SAE6 Operational Guidelines for Navigation/Route Guidance Systems (To insure ease-of-learning and ease-of-use in operating Navigation and Route Guidance Systems and to minimize the visual and cognitive demands associated with the use of these systems).	Detailed work plan was presented at 1/30/97 meeting.
		SAE J2256 Navigation and ATIS Message Set Evaluation (Test and validation of two-way message set for ATIS to/from the vehicle).	Draft completed 9/30/97
04	Inter-Center Data Exchange for Commercial Vehicle Operations	CVISN Architecture and Design (Develops EDI Standards for CVO Wireless).	ANSI: draft completed
		CVO-TS285 CVO Safety & Credentials Information Exchange (Form and Content of Messages).	IEEE/SAE - Status: none
		CVO-TS286 Credential Application (Form and Content of Messages).	SAE - Status: none
		IEEE1 Message Sets for DSRC for ETTM & CVO.	IEEE: draft to be completed 9/30/97
05	Personal and HAZMAT Maydays	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		ORNL Spatial Data Interchange (Develop an ITS profile to the Spatial Data Transfer Standard FIPS 173).	Project team has been assembled and are reviewing existing standards.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
		SAE5 Message Set for Mayday Alert (Develop a specification which prescribes various protocol methods such that vendors with different communication methods may speak to response agencies in a standard format. The standard will also address the issue of message content).	Draft completed 3/30/97. Work plan for the Mayday Specification due.
06	Traffic Mgmnt. Subsystems to Other Centers (Except EM)	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		Advanced Traffic Management System Data Dictionary (Develop an ATMS DD including data elements for ATMS messages used within TMCs and communicated external to TMCs by ATMS.	ITE: Prototype completed, formal development begun.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.
		ORNL Spatial Data Interchange (Develop an ITS profile to the Spatial Data Transfer Standard FIPS 173).	Project team has been assembled and are reviewing existing standards.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
		SAE J2256 Navigation and ATIS Message Set Evaluation (Test and validation of two-way message set for ATIS to/from the vehicle).	Draft completed 9/30/97.
07	Traffic Mgmt. Subsystems to Roadway Devices and Emissions Sensing/ Mgmt.	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		Advanced Traffic Controller 2070 (an open architecture standard for hardware, software and user interfaces).	Software documentation guidelines is being developed (due June 1997). ATC application program interface and data module definitions being developed (due June 1997).
		Advanced Traffic Management System Data Dictionary (Develop an ATMS DD including data elements for ATMS messages used within TMCs and communicated external to TMCs by ATMS.	ITE: Prototype completed, formal development begun.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
08	Signal Priority for Transit and Emergency Vehicles	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		ASTM1 DSRC Protocol (Physical and data link standards for beacons).	ASTM - Standards for physical and data link layers under development. Both active and back scatter physical layers will be supported with a single data link layer.
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
09	Emergency Mgmt. to Other Centers	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		CVISN Architecture and Design (Develops EDI Standards for CVO Wireless).	ANSI: draft completed.
		CVOEDI2 HAZMAT Information Request.	Status: Unknown.
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		ITE-96-04 Message Set for External TMC Communications (Develop a standard message set for external communication between TMCs and other External National Architecture Subsystems).	Project has just begun, detailed program plan due.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
		SAE5 Message Set for Mayday Alert (Develop a specification which prescribes various protocol methods such that vendors with different communication methods may speak to response agencies in a standard format. The standard will also address the issue of message content).	Draft completed 3/30/97. Work plan for the Mayday Specification due.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		SAE J2256 Navigation and ATIS Message Set Evaluation (Test and validation of two-way message set for ATIS to/from the vehicle).	Draft completed 9/30/97.
10	Information Service Provider to Other Centers (except EM and TMS)	AASHTO 01- NTCIP (provides interoperability and interchangeability for traffic management devices within the same communications infrastructure and to support communications between TMCs).	Project plan approved 8/01/96. Twelve protocols identified for development. The Actuated Signal Controller was approved for ballot by AASHTO and ITE. Drafts for VMS and Environmental Stations are under user review. Ramp Meters, Highway Advisory Radio and TMC to TMC are under development.
		Advanced Traffic Management System Data Dictionary (Develop an ATMS DD including data elements for ATMS messages used within TMCs and communicated external to TMCs by ATMS.	ITE: Prototype completed, formal development begun.
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		SAE1 Location Reference Specification (Interoperable location identification information).	Development began 10/96. Test procedures and scenarios being developed for field test (March to July 1997). Local ITS datum for Santa Barbara being evaluated. Datum and LRMS documentation under revision, incorporating input from multiple sources. Draft standard due in August 1997.
		SAE2 High Speed FM Subcarrier Protocol for EMS (Form and content of messages for real-time emergency notification from the Emergency Management Center to other centers).	A standard has been proposed.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		SAE5 Message Set for Mayday Alert (Develop a specification which prescribes various protocol methods such that vendors with different communication methods may speak to response agencies in a standard format. The standard will also address the issue of message content).	Draft completed 3/30/97. Work plan for the Mayday Specification due.
11	Transit Mgmt. to Transit Vehicle	IEEE1 Message Sets for DSRC for ETTM & CVO.	Draft to be completed 9/30/97.
		IEEE2 Message Sets for DSRC for AVI.	Project plan under review by FHWA.
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
		Message Sets for Public Transit Electronic Fare Collection.	No status.
		ORNL Spatial Data Interchange (Develop an ITS profile to the Spatial Data Transfer Standard FIPS 173).	Project team has been assembled and are reviewing existing standards.
A	AHS Standards	Adaptive Cruise Control (ACC) Man Machine Interface and Operating Characteristics (Consistent ACC operating characteristics to improve safety).	Begin mid-1997. Completed mid-1999.
		Guidelines for vehicular radar.	IEEE Status unknown.
E	Existing Standards	IEEE2 Message Sets for DSRC for AVI.	Project plan under review by FHWA .
		ITE-96-02 - Transit Communications Interface Protocols (Protocols for user services, transit operations, maintenance, customer information, planning and management functions).	Contracts signed in early November 1996. Steering group and committees established, work beginning.
I	Internal and probably proprietary	Guidelines for vehicular radar.	IEEE Status unknown.

KEY AREA	STDS. REQMNTS PACKAGE	STANDARDS	STATUS
		SAE4 In-Vehicle Databus Interface (Standards that will permit plug and play integration of multiple ITS devices into a vehicle at any time during its life cycle, while ensuring that the safety and integrity of the vehicle and on-board systems is maintained).	J2355 - ITS Data Bus Architecture Reference Model J2366-1 - Physical Layer J2366-2 - Data Link Layer J2366-7 - Application Layer J2367 - Gateway (due 12/31/97) J2368 - Conformance Development of these standards is just beginning.
		SAE5 Message Set for Mayday Alert (Develop a specification which prescribes various protocol methods such that vendors with different communication methods may speak to response agencies in a standard format. The standard will also address the issue of message content).	Draft completed 3/30/97. Work plan for the Mayday Specification due.
P	Proprietary Standards	No known relevant standards activities.	N/A
H	Human Interfaces	No known relevant standards activities.	N/A

List of Abbreviations used in Table 2-2:

AASHTO - American Association of State Highway Transportation Officials
AHS - Automated Highway System
ANSI - American National Standards Institute
APTS - Advanced Public Transportation Systems
ASTM - American Society of Testing and Materials
ATC - Automatic Traffic Control
ATIS - Advanced Traveler Information Systems
AVI - Automatic Vehicle Identification
CVISN - Commercial Vehicle Information System Network
EDI - Early Deployment Initiative
ETTM - Electronic Toll and Traffic Management
IEEE - Institute of Electrical and Electronics Engineers
ISO - International Organization for Standardization.
ITE - Institute of Transportation Engineers
LRMS - Location Referencing Message Specifications
ORNL - Oak Ridge National Laboratories
SAE - Society of Automotive Engineers

<<This Page is Intentionally BLANK>>

3.0 SYSTEM ARCHITECTURE

This section will discuss the system architecture options that could be used in the design of the Gateway Traveler Information System (TIS). There are several architecture options for the overall Gateway System. These options range from having one large network connecting all participants in the GCM Corridor to having a stand-alone system with a rack of modem connections to individual external systems. There are certain tradeoffs which must be addressed when discussing the options for a system of the Gateway's proposed complexity.

3.1 CENTRALIZED

A centralized architecture for the Gateway centers around a computing platform (Gateway computer) that would provide all of the necessary processing power, data communications and data storage. This computer would then have the responsibility for handling all tasks associated with the operation of the system. The centralized system has evolved from the main-frame, to the mini-computer and even to the desktop PC or workstation. Figure 3-1 is a diagram of potential interconnections using a centralized Gateway architecture.

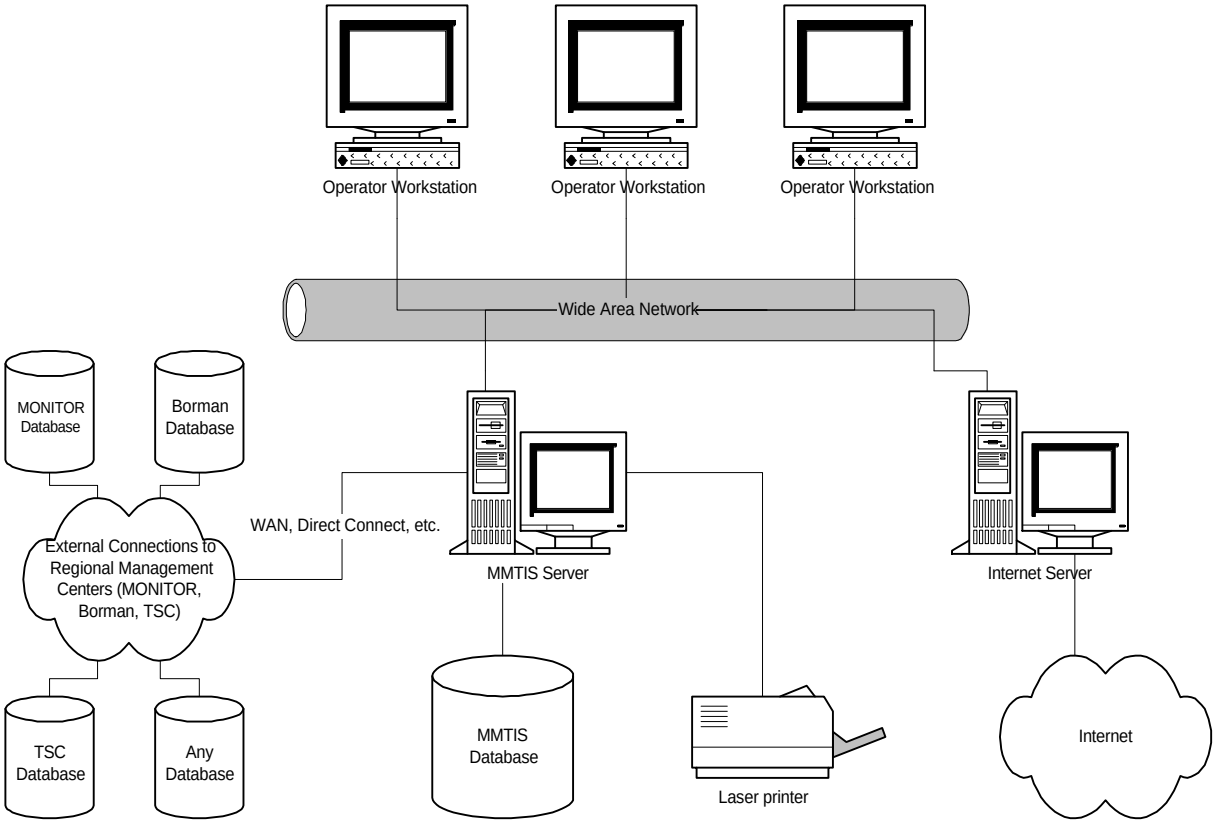


Figure 3-1 Gateway Centralized Architecture

By definition, a centralized system is not connected to external networks except for standard or customized modem connections. In this configuration it is extremely difficult to share large amounts of data in real-time. This type of configuration also limits flexibility in the acquisition of data and in the amount of data that can be received at the Gateway.

Since the centralized architecture revolves around a single computer, if the computer fails, then the entire system fails. If the system requires intensive user applications, then it can limit the processing resources for the non-user applications.

3.2 DISTRIBUTED

A distributed architecture for the Gateway could be thought of as a client/server system with multiple servers and clients. The physical Gateway hardware would only be a subset of the total network. This would be a network of computers that would provide the necessary computing power, data communications and data storage. There would be the ability to have databases located on different servers at different locations. As a result, however, when a change is made to one database, it may require changes in similar, remote databases. The Gateway application software would be able to access any server on the network that contains the applicable data through a data interface with standard network protocols. The data location is transparent to the users. In this type of an architecture, the Gateway would not own all of the information that is being distributed to users. Figure 3-2 is a diagram of potential interconnections using a distributed Gateway architecture.

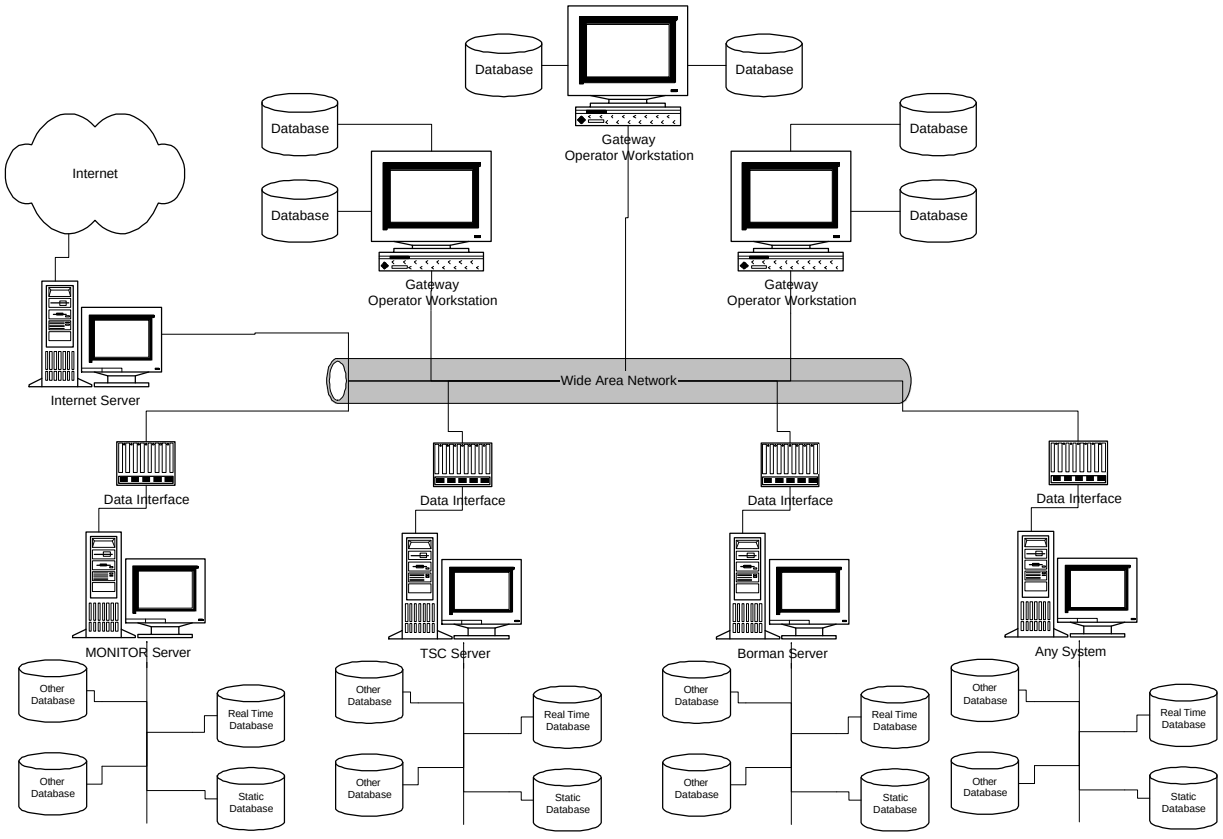


Figure 3-2 Distributed Gateway Architecture

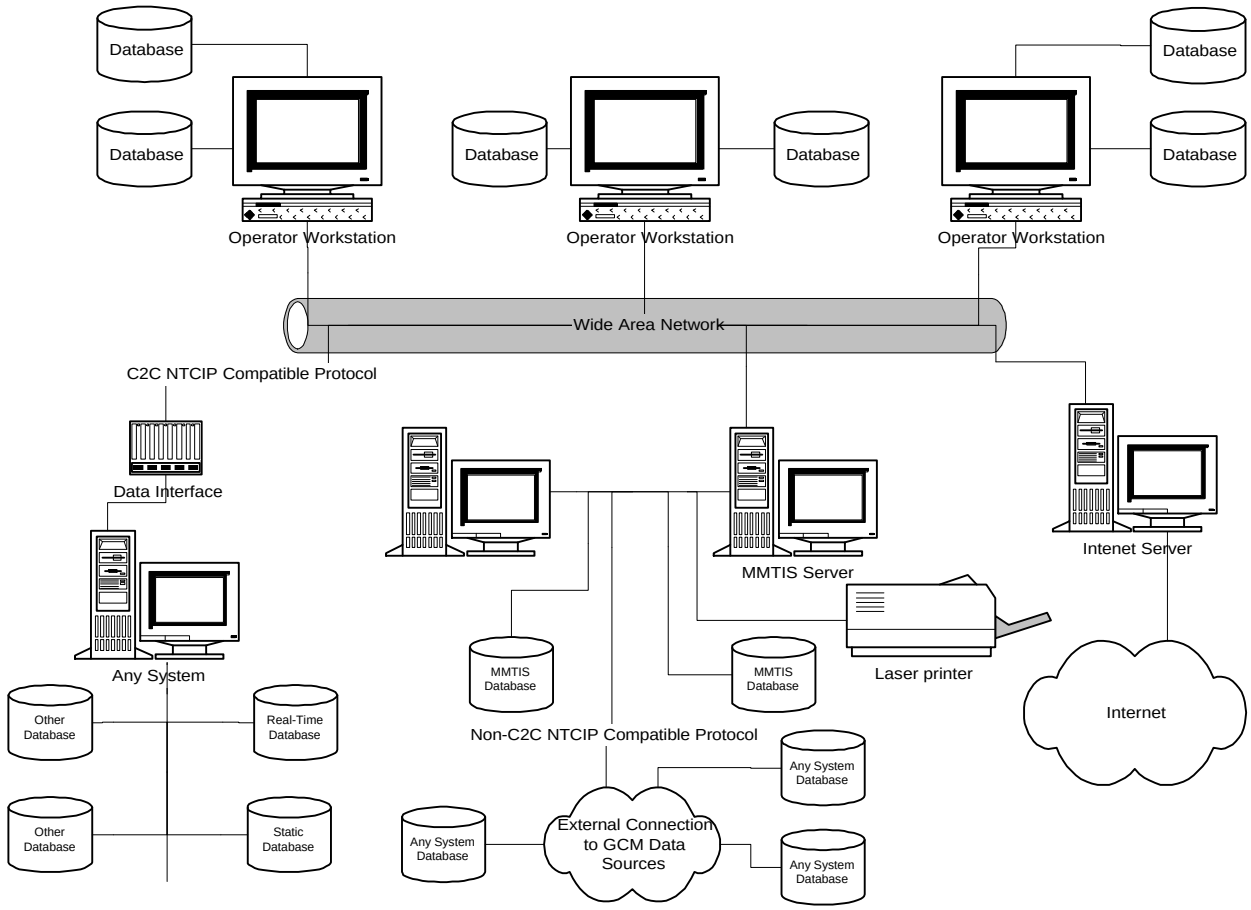
With this type of architecture, security would need to be built into the system to prevent unauthorized access to specific pieces of sensitive data. User passwords and access levels are necessary in this type of architecture.

A distributed architecture lends itself to easily accommodate additional servers and clients as they are needed. Additional networks can be set up and connected through bridges, routers and repeaters.

3.3 HYBRID

In the context of architecture for the Gateway, a hybrid contains features from both the centralized and decentralized architectures. In the hybrid architecture there would be the main processing performed by the Gateway computer with either workstations or dumb terminals for the Gateway operators. In addition, for agencies with strict network restrictions, modem connections could be used. For those agencies with more lenient networking policies, connections to the Gateway through data interfaces with standard network protocols could be used. The hybrid architecture allows the flexibility to connect to a vast array of agencies with differing data sharing policies. However, with the ability to connect using a variety of methods, an added level of complexity arises for development and maintenance of the interfaces. Figure 3-3 diagrams potential interconnections for a hybrid Gateway architecture.

Figure 3-3 Hybrid Gateway Architecture



<<This Page is Intentionally BLANK>>

4.0 HARDWARE

In the past, many traffic control systems, such as the Gateway System, relied on large mainframes or minicomputers for their central processing needs. Recent (within the past ten years) development of the microprocessor, however, has all but rendered these large machines obsolete. As more users found that they could have the same power on their desk that required a mainframe just a few years before, the PC revolution began. In time, however, the users found that they still wanted to share the data that was previously available to everyone on the mainframe. To deal with this, networks of computers were set up. The main repository of data became the "server," and the users the "clients." Thus client-server computing was born. This type of distributed processing allows the best of both worlds, with shared data and local control of what is done with the data.

4.1 SERVER HARDWARE

The Gateway System will likely use several servers to perform the various functions required. When selecting a computer system to use as a server, several factors must be considered. These are:

- Disk Capacity
- Memory Capacity
- Communications Capacity and
- Processor Type and Speed.

4.1.1 Disk Capacity

Most computers today can use two types of hard disk drives; integrated device electronics (IDE) or small computer system interface (SCSI). IDE was developed as a low cost means for small to medium capacity disks to be integrated into mostly desktop computers. It is relatively fast, but cannot handle more than two devices per interface and only one device can be active at any given time. SCSI is a broader interface standard, allowing not just medium-to high capacity disk drives, but also CD-ROMs, scanners and other peripherals to exist on the same "chain." SCSI also supports disk RAID arrays, which are a series of disks that duplicate the same information, so that a backup is always available if a primary disk fails. The SCSI interface also allows multiple devices to be accessed simultaneously, increasing speed in a multi-drive system.

In general, a server should include at least 5 Gigabytes (GB) of disk storage, but this size can be increased if necessary for backup or if data archiving purposes require it. Additionally, client machines should include at least 1 GB of disk storage to accommodate application software.

4.1.2 Memory Capacity

A computer uses Random-Access Memory (RAM) for the actual execution of all programs stored on its disk drives. The amount of RAM is closely tied to the performance of a given system. As RAM is increased, the less often the computer must access the hard disk drives, which are slow relative to memory access speed. RAM is available in different access times and this factor is system specific.

The minimum amount of RAM that should be considered for a server is 64 Megabytes, but this can quickly grow to 256 MB, or even a Gigabyte per server in some cases. Client machines should contain a minimum of 16 MB but 32 MB is preferred.

4.1.3 Communications Capacity

Servers will usually need two types of communications: network and serial. The serial needs are usually light, sometimes just a local terminal. In cases of a server acting as a communications processor however, the number of serial lines needed and the speeds needed to be supported usually dictate that an external communications subsystem be attached, with a host adapter card. The host adapter will aggregate the attached serial lines into one or more high-speed data channels, which the computer can then demultiplex as necessary. The advantage of this is that the external processor handles all of the communications details and the server just has to handle the data processing.

Network communications will be discussed in Section 6.0.

4.1.4 Processor Type and Speed

The choice of a processor is dictated by several considerations, such as:

- Type of Operating System Desired
- Type of Languages to be Used for Programming
- Speeds Available and
- Cost of System.

In general, the faster the processor the better, but in some cases funding is better used by purchasing more RAM than a faster processor. All of the considerations must be taken into account however, before a decision can be made.

Most processors fall into two categories, Reduced Instruction Set Computing (RISC) or Complex Instruction Set Computing (CISC). A RISC processor, such as a Sun Sparc, is optimized for performing a small set of tasks very quickly. A CISC processor, such as a Pentium, is optimized to perform more complex tasks, but at the price of speed. In reality, the lines between these types have become blurred, as modern processors exhibit characteristics of both. The processor type to be used should be based on the factors listed above, rather than its internal architecture.

4.2 WORKSTATION HARDWARE

The choice of what type of system to use as a workstation is based on similar factors as the server, but the type of display used is more critical, as it is the primary operator interface. The system used must support the selected system software (discussed in section 5.0), and be comfortable for an operator to used during an entire work shift. Attention must be given to ergonomic factors, such as screen size and resolution, keyboard type and point device, such as a mouse.

In general, workstation hardware will have smaller disks (if any) than a server and do not have the requirements for large amounts of RAM or extremely fast processors. Speed considerations are generally related to screen updates, as a system operator will not wish to wait while a map or other graphic is "painted" onto a screen.

The user interface is interrelated with the operating system and in recent times, is usually a windowing environment. Examples of this are:

- Microsoft Windows
- IBM OS/2 Presentation Manager and
- X-Windows.

The first two are closely tied to a particular operating system, while X-Windows is an open standard available for almost any platform. X-Windows can also be used on a terminal with no local processing capability; all of the computing is done at the system servers. The advantage of this is that a lower cost terminal can be used as an operator workstation and any system software changes made are immediately available; the software does not have to be updated at each workstation. Some loss in speed in the user interface may result, however, as all processing is then done in the server.

<<This Page is Intentionally BLANK>>

5.0 SOFTWARE

This section will discuss the options for the software that could be included in the design of the Gateway Traveler Information System (TIS). In addition to application software, which is typically custom-designed for the particular need, there are two other classes of software to consider. These are Operating System software, and User Interface software. As discussed in Section 4.0, client-server computing is the current standard. The discussion of operating systems in this section will therefore be limited to those that are appropriate for this environment.

5.1 OPERATING SYSTEMS

The basic software used for controlling a computer is called the Operating System. There have been many operating systems over the years, but currently only three are in widespread use for servers and workstations. These are UNIX, various versions of Windows (Windows NT and Windows 95) and to a lesser extent, OS/2. In addition, several propriety operating systems exist. They offer advantages in some situations, therefore one such system is included in this discussion.

5.1.1 UNIX

UNIX was developed at Bell Labs and the University of Berkeley in the early 70's and has grown much since then. It is, at its core, a very minimal operating system, with much of its power residing in standard add-ins and control programs. The large server and workstation vendors such as Sun Microsystems and Hewlett-Packard have standardized on UNIX as their operating system and have developed many custom add-ins to enhance the system. UNIX is a multi-tasking, multi-user operating system and is very adept at handling many operations at the same time. It supports both a text based user interface and the X-Windows system.

5.1.2 Windows

Microsoft developed Windows in the mid 80's for use on desktop computers. A commercial failure at its outset, it has since become the most popular operating system in use today. It has two current variations, Windows 95 and Windows NT. At their core, they are quite different.

Windows 95 is intended to be a single user system for desktop or laptop computers. It does support limited multi-tasking, but can easily be bogged down and even crash when subjected to too many concurrent processes. It can be used for operator workstations, either using it's native windowing interface, or by running an X-terminal emulator program.

Windows NT has a completely different internal structure than Windows 95. It is much more adept at handling multiple users and tasks and can be used as a server.

5.1.3 OS/2

OS/2 is an IBM product, developed in the late 80's. It is more like UNIX and Windows NT than Windows 95 and supports multi-tasking and multi-user environments quite well. It has proven to be quite reliable for use as a network server and supports a wide variety of networking options and protocols.

Unfortunately, OS/2 has not been a widespread commercial success and it has historically been much more difficult to obtain compatible hardware and software for the operating system, compared to Windows or UNIX. In general, while OS/2 is capable of being an effective server, the system designer must possess some other compelling reason to use it in preference to the other popular operating systems.

5.1.4 Proprietary

There are also proprietary operating systems in use. One of these, Digital Equipment Corporation's (DEC) Virtual Memory System (VMS) has been fairly widely used for traffic control projects. VMS is much like UNIX, but optimized for DEC's line of servers. VMS is very stable, fast and powerful.

5.1.5 Hybrid

Although there is not possible for a single computer to have a "hybrid" operating system, it is possible that the Gateway System may include computers with more that one of the operating systems listed herein. From a network standpoint the computers with the different operating systems can all work together as a unit.

5.2 DATABASES

An important aspect of the Gateway TIS is its ability to store and retrieve information from a database. Access to the data by operators and other users will be provided by a database management system (DBMS).

A DBMS gives the user access to their data and helps them transform the data into information. Such database management systems include dBase, Paradox, Oracle, Versant and Ontos. These systems allow users to create, update and extract information from their databases.

A database is a structured collection of data. Data refers to the characteristics of people, things, events, etc. There are two different approaches to managing data through a DBMS. These are through a relational database or a object-oriented database. Each approach is discussed in the following sections.

5.2.1 Relational Databases

Database management systems have evolved from hierarchical to more complex relational models. Today the most widely accepted database model is the relational model. The relational model has three major aspects:

- Structures - Structures are well-defined areas that store the data of the database. Structures and the data contained within them can be manipulated by operations.

- Operations - Operations are clearly defined actions that allow users to manipulate the data and structures of a database. The operations on a database must adhere to a pre-defined set of integrity rules.

- Integrity Rules - Integrity rules are the laws that govern which operations are allowed on the data and structures of a database. Integrity rules protect the data and the structures of a database.

Relational databases are structured in the form of a table or series of interrelated tables. For example, all records for detectors would be stored in one table, the detector table. A table is easily visualized as a tabular

arrangement of data, similar to a spreadsheet, consisting of vertical columns and horizontal rows. A table consists of a number of records, where the field names (column heading) for each record in the table are the same. Every detector may have a type field, identifier field, location field, volume field and occupancy field. Each record occupies one row in the table and each field occupies one column.

Relational databases also have the ability to link together the data in multiple tables. If there was another table for each DOT that listed the equipment that it maintained by the same identifier field, then by knowing the identifier, one would have access to data from multiple tables since there is a common field among the tables. What makes a database relational is that a common field can exist in more than one table.

The use of relational databases is widespread throughout the computing community and it is the most mature of all database types. Oracle, Sybase, dBase, Informix and Structured Query Language (SQL) Server are some of the most popular relational databases. Relational databases are proven products which allow flexibility in building a system.

5.2.2 Object-Oriented Databases

A new type of database management is "object-oriented." Object orientation promises to:

- facilitate the development and maintenance of applications that incorporate large amounts of small heterogeneous data types
- to enhance productivity in the long run by permitting programming pieces or modules that can be very flexibly coupled and re-used and
- to empower the development of software that requires a high level of integration and connectivity.

From a developer's perspective, this implies software that is easier to create, simpler to use, far more reliable and less costly to maintain or evolve in increments. The object-oriented approach is emerging in an increasing fashion in the form of object-oriented databases. An object-oriented database system is a DBMS which is object-oriented (OODBMS), in the meaning of the current crop of object-oriented programming language. That implies:

- The OODBMS must be able to support the encapsulation of data and code (sometimes called methods) together. The main idea with encapsulation is to abstract the user (who may be a programmer) from having to work with the data manually. They should be using a method to access the data. This way, if something changed in how the data was to be retrieved, only the code in the method needs to be changed, not all programs that use the method.

- The OODBMS must be able to support the concept of extensibility; that is the ability to create new objects from existing objects. This is important when writing new programs. Extensibility means that you can draw on previously written code (debugged code) and change what you need to be different by over-riding old methods with new methods.

- Inheritance is another important aspect of OODBMS. Inheritance allows the user or programmer to build on work that has already been done.

Primary differences between relational and object-oriented databases are that relational databases store their information in tables, similar to spreadsheets where an object-oriented database is capable of storing

information that has dynamically varying data structures. An OODBMS combines the data with programming code into something called an object. In a relational DBMS, the data and the access to the data are separate entities. Relational databases are more mature in their life-cycle and therefore have standards developed regarding queries to the database. In an object-oriented database, the concept of a table does not exist. Each object is defined through properties, attributes and models. In the case of the relational database, each table consists of records of fields, where each field contains one piece of data. In the object-oriented database, each object can contain a variable number of items. As new data is received in the relational world, it is stored in a new record. In the object world, it is attached to that object. Since objects vary in size, they can minimize disk space and speed up searches, making them ideal for real-time applications.

Overall, object oriented data bases take longer to set up than relational databases. One shortfall is that object-oriented databases are still struggling with standards development.

5.2.3 Comparison of Relational Database Management Systems (RDBMS) and Object-Oriented Database Management Systems (OODBMS)

Selection of a DBMS requires a careful analysis of the requirements of the desired system and then the selection of a DBMS. The following table summarizes a number of topics that must be addressed and an assessment of how the top RDBMS (Oracle, Informix, Sybase) products compare with existing OODBMS (Versant, ObjectStore) products.

CHARACTERISTIC	RDBMS	OODBMS
MATURITY	High	Medium
STANDARDS	SQL92 (ANSI & ISO), ODBC, JDBC	None
REPORT WRITERS	Excellent. Many. Report writers are available from the vendors and third party sources. The report writers available support user defined reports, batch reporting and programmer generated reports.	Poor. Proprietary with limited functionality. Writing reports against an OODBMS is tricky at best.
DEVELOPMENT TOOLS	Excellent. Wide range of support. Tools available include design tools that will generate the database directly from the design, reverse database design tools, code generators. Multiple language support (C++, C, JAVA, FORTRAN, COBOL, PASCAL) allow easy integration of legacy code with new software development.	Poor. Proprietary. Support from compiler suppliers is sporadic.

CHARACTERISTIC	RDBMS	OODBMS
MANAGEMENT TOOLS	Excellent. Wide range of support. Tools include static database analyzers, performance analyzers and network analyzers that automatically decode the database protocols. Management tools are available from many sources for the major database suppliers (Oracle, Sybase, Informix).	Poor. Proprietary with limited functionality. Many management functions available at the command line for an RDBMS require the user to write and compile a program.
PLATFORM SUPPORT	Excellent. All major platforms are supported (UNIX, Windows NT, Windows, DOS, OpenVMS, etc.).	Good. Most UNIX systems, OpenVMS (frequently), Windows NT and Windows.
ABILITY TO SUPPORT REAL TIME DATA	Very Poor. Databases (both RDBMS and OODBMS) are designed to store data in a useful form for later retrieval and analysis. Storage of high rate dynamic data (such as detector data) is incompatible with this design.	Very Poor. Databases (both RDBMS and OODBMS) are designed to store data in a useful form for later retrieval and analysis. Storage of high rate dynamic data (such as detector data) is incompatible with this design.
SCALABILITY	Excellent	Good
INTEGRATION WITH O-O LANGUAGES	Very Good. Object support within the database is improving rapidly. Several O-O "wrapper" products exist to emulate an O-O.	Very Good

Based on the analysis performed to generate the above table an RDBMS is the most cost effective method. The current generation of OODBMS products show the same problems and limitations (lack of third party support, limited platforms, limited tools) as RDBMS products did 10 years ago. Another significant advantage for RDBMS products is the availability of support personnel within the general labor market. This will be further studied as the Gateway design evolves.

5.2.4 Multiple Databases

Both relational and object-oriented databases are typically used on a network in a "client-server" model. In this model, the database is kept on one central server and all the workstations, or clients, access the data across the network. This works well on small office Local Area Networks (LANs), but tends to run into performance problems when used on a "WAN" (Wide-Area Network) which includes slower links.

In a distributed database architecture, there are multiple servers in different locations on the network, arranged so that each client workstation can get to a server through a fast connection. The servers talk to each other and exchange data between themselves so that they all maintain a current copy of the database. This type of database works best in situations where the data is not changing frequently, or when the data is mostly coming from one source and is being distributed to many widespread clients. Problems can arise when there are many clients trying to update the same data, since it is very difficult to perform true record-locking.

The best example of a commercial distributed database is Lotus Notes. Notes Servers maintain copies of documents and the relationships between them. The servers operate in a loosely coupled fashion, where they periodically talk to each other and exchange copies of documents which have been updated. Depending on the architecture of the network and the number of servers, it can take minutes or hours for a change to propagate throughout the system. This works well in a document-centric collaboration environment, but is not really applicable to a high-volume, data-centric application.

Most commercial RDBMSs now offer the option of "replication," which is the ability of servers to maintain copies of a database at multiple sites. Normally, this is set up as a master/slave relationship, where there is one master server which contains the "real" database and multiple "slaves" which receive copies of the data when it changes. Data can be replicated at the "record" level, where each record with a change is transmitted, or at the "field" level, where only the individual data fields that changed are transmitted. Usually, data can only be updated at the master site, not at the slave sites. Recently, some database vendors have begun offering "symmetric replication," where the replication can be done in both directions. Of course, the issue of multiple remote updates to the same data must still be dealt with and the database servers have very complex algorithms to handle these situations. This is still a new technology and requires a lot of effort in tuning the systems to run efficiently.

Some RDBMS servers offer another form of distributed database management, the "remote query." The data is not distributed, but is kept in different servers in different locations on the network. When a client wants to perform a query that requires data from multiple sites, it can issue a single query to its local server. The local database server then issues distributed queries to the other servers on the network which contain the desired data, collects the results and then returns the result set to the client. This can still have problems with the frequent transmission of large amounts of data over the network, but in can greatly simplify client software architecture.

Object oriented databases show the most promise in distributed applications, but this potential has not yet been fully realized. Since OODBMSs keep data together with the code that knows how to manage the data together, objects in a database could be very smart about how to move data around in a network environment. Each client would have its own "local" copy of the database objects and code within the objects would manage the distribution of data in the most efficient way for the particular application. However, this is not a mature technology and is not readily available at this time.

The Milwaukee MONITOR system uses a hybrid database scheme. All workstations connect to an OODBMS central database for static configuration data and device status information. Real-time detector data is supplied to the map on the workstations using a TransCore (formerly JHK) developed memory resident database called DDD. DDD is required due to the inability of the OODBMS to support the real-time data requirements. The sign system uses a local relational database for its control information but transmits status information to the OODBMS and DDD for display at the workstations.

5.2.5 Single Database

As opposed to a distributed database, all data can reside in one place on one computer. The GCM Corridor Transportation Information Center (C-TIC), the prototype of the Gateway, is an example of this. Although it is an object oriented database, it is easier to visualize it as a single database with all items stored in one database on one hard drive on one server with multiple processors. The database used is Versant. Items stored include the NavTech maps containing road segment identifications, latitude/longitudes, etc. Other data stored includes loop detector number and the associated roadway link , etc. as well as information input by the operator on construction/maintenance activities, etc. Each element can be thought of as an object, with a separate record for each. When one element in a database is changed, it is relatively simple to make the change as the database is all in one place.

To improve the speed of the operator interface, as much of the database as possible is loaded into RAM. Due to the size of the executables, the entire database cannot be loaded into RAM at one time and reads are made to the hard drive as required.

With respect to backups on the database, while it is possible to do backups of only items that have changed, it has been found advisable to backup the entire database on a regular basis. This requires a significant amount of time as it is done online which can affect the speed of processing other requests (e.g. data inputs).

5.3 USER INTERFACE

The user interface is interrelated with the operating system and in recent times, is usually a windowing environment. Examples of this are:

- Microsoft Windows
- IBM OS/2 Presentation Manager and
- X-Windows.

The first two are closely tied to a particular operating system, while X-Windows is an open standard available for almost any platform. X-Windows can also be used on a terminal with no local processing capability; all of the computing is done at the system servers. The advantage of this is that a lower cost terminal can be used as an operator workstation and any system software changes made are immediately available; the software does not have to be updated at each workstation. Some loss in speed in the user interface may result, however, as all processing is then done in the server.

<<This Page is Intentionally BLANK>>

6.0 NETWORKING

The types of networks that are suitable to be used for the Gateway can be grouped into two broad categories: Local Area Networks (LAN) and Wide Area Networks (WAN).

6.1 LOCAL AREA NETWORKS

LANs are used to interconnect groups of computers at a given site. There are several methods which can be used for the connection, both at the physical (media) and logical (network protocol) layers. These are briefly discussed below.

6.1.1 Physical Layer

Modern LANs are connected by either fiber optic cable, coaxial cable, or unshielded twisted pair (UTP), with UTP being the most prevalent. With fiber optic or UTP, the connection to each computer is run to a central hub, where all data is routed to other devices connected to the hub. The central hub can be smart or dumb, the difference being whether or not the hub sends all data to every device, or only to the ones on a particular segment or port of the hub. Smart hubs are more expensive, but can greatly reduce network congestion in a busy system. The disadvantage of a hub based system is that failure of the hub results in complete network failure for all computers on that hub.

In a system connected by coaxial cable, a "T" connection is installed at each computer and the cable is run in a linear arrangement from machine to machine. The advantage of this type of system is that less cable is needed; in many cases one segment can serve an entire room of computers. The obvious disadvantage is that all network data travels to all devices and congestion can occur. Typically this occurs only when the network contains several network intensive devices which can overload this type of network.

It is not uncommon to see a mixture of these technologies within a system.

6.1.2 Logical Layers

The logical layers are the protocols that the devices connected to the network "speak," in order to communicate with each other. Modern LANs almost always use one of two protocols: Ethernet or Token-Ring. Ethernet uses a technique known as CSMA, or Carrier Sense Multiple Access. In this system, when a computer wishes to transmit data, it first listens to the channel and if it does not sense a carrier from another computer, it begins to transmit. If two or more computers transmit at the same exact time, it is likely that the length of the transmissions will be different. If this is the case, then the other computer will hear the carrier when it is finished, thus sensing a "collision." It will then wait a random amount of time and retransmit. The overall speed of an Ethernet LAN is 10 Megabits per second (Mbps) for 10Base-T (CAT-3 twisted-shielded cable), 10Base-5 (thick coaxial cable) and 10Base-2 (thin coaxial cable) networks. There is also a 100Base-T that has a speed of 100 Mbps, but its applications are limited by distance. With proper hardware, the two speed can be used together in one system.

Token-Ring was developed by IBM and is most often used when an IBM mainframe is part of the network. Speeds of Token-Ring networks can be 4 Mbps or 16 Mbps. A Token-Ring operates by passing a "token" around a logical ring and when each computer receives the token, it is allowed to transmit data at that time. The token is then passed to the next computer in the ring.

High-level protocols, such as TCP/IP, NetBios and Internetwork Packet Exchange (IPX), are used to ensure that transmissions are acknowledged when sent and are responsible for retransmission when necessary.

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is actually two protocols generally used as one. IP is the protocol that was developed for the Internet and handles the low-level data transmission of data packets between two places. TCP is a higher level protocol which is responsible for error detection and retransmission of failed packets. IP is routable, which means that it can be sent from network to network using specific addresses; in a non-routable protocol, all devices see all packets on the network.

NetBios (and its cousin NetBuei) is a lower-level, non-routable protocol. Because of its relatively high overhead, it is generally used on small LANS. Microsoft's Network is an example of a NetBuei application.

IPX is Novell's version of IP. It is optimized for the NetWare operating system and works with computers operating NetWare and Windows NT.

6.2 WIDE AREA NETWORKS

Wide Area Networks are used to connect distant LANs. A WAN also has the same two considerations, the Physical Layers and the Logical Layers.

6.2.1 Physical Layers

In most cases, the physical cables used for a WAN are much different from that of a LAN. The longer distances involved, the high speed data traffic usually required and the fact that much of the cable is outdoors all play a factor in the WAN design. The basic options are:

- Leased Telephone Company Circuits and
- Agency-Owned Fiber Optic Networks.

6.2.1.1 Leased Circuits

The telephone companies have many millions of dollars invested in their network infrastructure; it is redundant, reliable but can be expensive to use in the long term. the use of leased circuits vs an agency owned network must be carefully evaluated to determine the actual costs over time.

The telephone companies lease bandwidth on their network in blocks of 64 kilobits per second, known as a DS-0 or channel unit. A DS-1 unit is a multiplexed serial stream of 24 DS-0s. Higher order multiplexed serial streams are: DS-2, comprised of 4 DS-1s; and DS-3, comprised of 28 DS-1s as shown in the table below:

LEASED LINE TYPES	BANDWIDTH
DS-0	64 kbps
DS-1 (T1)	1.544 Mbps (equivalent of 24 DS-0)
DS-2 (T2)	6.3 Mbps (equivalent of 4 DS-1)
DS-3 (T3)	45 Mbps (equivalent of 28 DS-1)

These are the basic leased lines that are available, although several specialized services are also available. Integrated Services Digital Network (ISDN), Frame Relay and Asynchronous Transfer Mode (ATM) are

examples of specialized services. All of these services have potential applications for a WAN, but must be evaluated on a case-by-case basis depending on the particular need.

6.2.1.2 Agency Owned Fiber Optic Network

While other media have been used for long distance communications, a new system today will almost certainly use fiber optic cable. Its superior radio frequency (RF) and lightning immunity, along with low maintenance costs, makes it the logical choice in many applications.

A fiber optic network can be installed as several point-to-point links, or as several "stars" connected to point-to-point trunks, which aggregate the data. Fiber optic cable can be run as either underground or aerial.

6.2.2 Logical Layers

As was the case for the LAN, the WAN uses various protocols to ensure that high speed data transport is accurate and timely. In some cases, the same protocols used for LANs are also used for WANs, but because the amount of data and speeds are different, additional protocol types were developed.

For leased circuits, the telephone companies have several services available. At the most basic level, direct point-to-point links can be established using the DS-0 to DS-3 hierarchy described above. For more complicated networks, other services are available, such as Frame Relay and ATM.

Frame relay is primarily a data-only service where point-to-point connections are established to the phone company switching center and the connections between locations are handled there. For instance, if several control centers needed to be connected together, it would not be necessary to establish physical point-to-point links between all of them, rather, one link from each would be brought into the switching center. The switch would then handle the distribution of data between the control centers as necessary. This can significantly reduce costs since the cost of a connection is based on the distance of the link and this technique would reduce the link distances.

For combining voice, data and video, ATM is beginning to be deployed. ATM is a "cell" based technology, where information that cannot tolerate delay (such as voice or video) is assigned cells which are sent at regular intervals and other data is interleaved between these cells as needed.

ATM is still fairly new and issues of LAN and manufacturer compatibility still exist. In addition, it is quite expensive, but costs have been dropping and it may find widespread use in the near future.

ISDN is another service that is becoming widely available. Basic-rate ISDN provides two 64 kbps data channels and a 16 kbps control channel. In practice, only the two 64 kbps channels are available for users, but they can be easily combined into one 128 kbps channel. ISDN circuits are useful for medium-speed data transfer and highly compressed video signals. ISDN is inherently point-to-point, so a separate line must be installed for each circuit.

All of the above protocols can also be implemented in an agency-owned system as well. In addition, a protocol used in many fiber optic systems is SONET, for Synchronous Optical NETwork. SONET operates at various speeds from, 51 MBPS to 622 MBPS and greater. SONET systems are usually deployed in what is known as a "self-healing ring," which provides very high fault tolerance. A SONET architecture would typically be

deployed as a "backbone" or trunk and user data transmission would take place using the other protocols described above, on top of the SONET protocol.

7.0 INTERFACES

7.1 NATIONAL STANDARDS

In the development of the Gateway System, every attempt will be made to utilize existing national or regional standards. In this manner the Gateway System will be better able to interface, not only with both exiting and emerging transportation systems within the corridor, but also with other regional systems throughout the country and with mobile devices (pagers, in-vehicle devices) which can roam throughout the US.

The principal national standard in regard to the Intelligent Transportation Systems is the National Transportation Communications for ITS Protocol (NTCIP). The primary objective of the NTCIP is to provide a communications standard that ensures the interoperability and interchangeability of traffic control and Intelligent Transportation Systems (ITS) devices. The NTCIP is the first protocol for the transportation industry that provides a communications interface between disparate hardware and software products. The goal of the NTCIP effort is to not only maximize the existing infrastructure, but to also allow for flexible expansion in the future, without reliance on specific equipment vendors or customized software. The NTCIP effort is being supported by the American Association of State Highway Transportation Officials (AASHTO), National Electrical Manufacturer's Association (NEMA), Institute of Transportation Engineers (ITE), Institute of Electrical and Electronics Engineers (IEEE), Federal Highway Administration (FHWA) and the Society of Automotive Engineers (SAE).

The NTCIP is actually a family of standard communications protocols used for data transmission within and between Intelligent Transportation Systems, (ITS). The standard covers both the "how" and "what" of data communications, that is, both the transmission rules and the format and meaning of standardized messages transmitted using those rules. Where possible, the NTCIP is based on existing standards in the telecommunications and computer industries.

The NTCIP aims to do for transportation systems what the Internet has done for communications between general-purpose computers: it will help enable interoperability and interchangeability between devices and between systems from different manufacturers. It can provide more choice, more flexibility and the ability to coordinate the operation of adjacent devices and systems.

The NTCIP family of protocols is continually expanding to address additional needs. The initial standards provide protocols for real-time communications between a master or computer and such field devices as traffic signal controllers, environmental sensor stations, dynamic message signs, highway advisory radio, closed - circuit television cameras and freeway ramp meters. Work is under way on additional protocols for applications such as computer-to-computer or center-to-center data exchange, communications within transit management systems and communications with and between moving vehicles. The NTCIP and related standards are intended to eventually provide a comprehensive family of communications protocols covering all ITS applications.

The NTCIP Joint Steering Committee has identified center-to-center (C2C) communications as a priority for further protocol development. This new protocol will address real-time peer-to-peer data exchange (including some remote control/commands capability) between transportation management centers and systems such as traffic operations centers, transit operations centers, emergency management centers, traffic signal systems, freeway management systems and traveler information systems. The first meeting to shape the framework for developing a standard was held in July of 1996 at which time various developers and system owners came

together to consider the needs and directions of a C2C communications standard. Based upon that initial meeting, papers were developed to explore some of the options that might be considered for standards development in this particular arena. The second meeting was held in January of 1997 that reviewed these papers for alternatives for the C2C communications standards. As a result of that meeting, it was agreed that the approaches presented in three papers would be reviewed further. These three approaches included:

1) The use of remote procedure calls
2) The use of Common Object Request Broker Architecture (CORBA) as an object interchange standard
3) The use of TCP/IP sockets and STMF based upon previous NTCIP work.

The results of these papers were presented at a meeting held in March (at NEMA headquarters) at which time input from the architecture group, the model deployment program, user input and developer input eliminated the first option, "the use of remote procedure calls." They decided instead that the next stage would be to develop a draft framework for standards utilizing a dual approach which focused on "the use of CORBA as an object interchange standard" for object exchange between TMCs combined with "the use of TCP/IP sockets and STMF" for the structured communications protocol (TCP/IP) between control centers. This dual approach is consistent with current NTCIP work developing the objects utilizing ASN.1[2] notation for defining the contents of the message sets or objects that would be transferred between traffic management centers.

The results of the preliminary designs for the dual protocol will be discussed at the next meeting (May 1997) and a specific direction would be selected. The Common Object Request Broker Architecture, (CORBA) allows a variety of applications to communicate with one another. CORBA 1.1 was introduced in 1991 and defined the Interface Definition Language (IDL) and the Application Programming Interfaces (API) that enable client/server object interaction within a specific implementation of an Object Request Broker (ORB). CORBA, adopted in December of 1994, defines interoperability by specifying how ORBs from different vendors can interoperate.

The ORB is the middleware that establishes the client-server relationships between objects. Using an ORB, a client can transparently invoke a method on a server object, which can be on the same machine or across a network. The ORB intercepts the call and is responsible for finding an object that can implement the request, pass it the parameters, invoke its method, and return the results. The client does not have to be aware of where the object is located, its programming language, its operating system, or any other system aspects that are not part of an object's interface. In so doing, the ORB provides interoperability between applications on different machines in heterogeneous distributed environments and interconnects multiple object systems.

Typically for client/server applications, developers use their own design or a recognized standard to define the protocol to be used between devices. Protocol definition depends on the implementation language, network transport and other factors. With an ORB, the protocol is defined through the application interfaces via a single implementation language-independent specification, the IDL. The use of ORBs can let programmers choose the most appropriate operating system, execution environment and programming language to use for each component of a system under construction. In an ORB-based solution, developers can model the legacy

[2] ASN.1 is a high level protocol that began as an ISO standard in 1988 with initial applications in the defense industry. ASN.1 fosters an open systems approach for information transfer.

components using the same IDL they use for creating new objects, then write what is termed a "wrapper" code that translates between the standardized bus and the legacy interfaces.

There is currently some concern that the performance, machine requirements and some of the services that are necessary for a CORBA based standard may pose some problems. Further, the CORBA aspect will be based upon leading edge software technology which is difficult for the agencies to fully understand and for which the rate of change is very rapid. Countering these misgivings, the objects are easy to understand and the concept of message packets and ASN.1 defined objects are also easy to understand.

Other systems currently being deployed use remote procedure calls, TCP/IP sockets and basic serial data streams or message packets between centers. It will take several months for a clear path to be mapped out and the center-to-center (C2C) communications standard to progress rapidly. It is anticipated that draft standards will be available by the third quarter of 1997.

In conjunction with this work, the International Organization for Standardization (ISO) Working Group 9 recently held meetings in Noosa (Australia) and is working on developing the naming conventions for the message sets between traffic management centers. The ISO group has published a committee draft (N173REV) which has been generally accepted within the international community as setting the stage for the naming conventions as it describes the data and the attributes to be transferred between TMCs. This work is now progressing at a more rapid pace and an ISO standard for the naming conventions, attributes and data definition is likely to be available for ballot at the October, 1997 international meeting in Berlin.

7.2 DATA COLLECTION METHODS

Options for data collection methodologies are described below. System security should be considered with C2C communications. As with data distribution, dedicated and dial-up lines will only require minimal security and data traversing the public Internet will use the same security methods described in Section 7.3.1.

7.2.1 Dedicated

A dedicated system would install a specific point-to-point link between two control centers, using either digital or analog circuits. If analog circuits are used, then a bank of modems would be required at the control center. Digital circuits allow more flexibility, as either a point-to-point circuit could be used (i.e., 56 kbps or ISDN) or a switched type (frame relay). The advantages of frame relay are that no large infrastructure is required at the control center. Once the necessary equipment is installed (a router), more users can be added onto the system at any time by the phone company. Only small reconfigurations are required at the control center. If point-to-point links are used, there must be a one-to-one correspondence between users and hardware, thus increasing the cost and complexity of the system.

Frame relay can only be used over digital lines. The difference between frame relay and analog multipoint connections is that with an analog connection, all data is sent to all sites. With frame relay, the phone company system routes the data to only those sites at which it is needed.

If control centers wish to share video images a higher bandwidth line is required along with signal compression/decompression equipment at each end.

7.2.2 Dial-In

A dial-in system would be set-up very similarly to the dedicated system described in Section 7.2.1 above. There would be a bank of modems to handle dial-in information from the remote control centers. Unlike the data distribution, however, it is likely that there would be a one-for-one distribution of modems to remote centers. Dial-in lines would not support transmission of video images, with the exception of low resolution slow-scan TV (1 frame every 1 to 20 seconds).

7.2.3 Internet

It is possible that the Internet could also be used to pass data between control centers. This method is not usually used unless there is a wide geographical distribution between the centers, which would make it more cost efficient than dedicated or dial-up lines. Video images could be transferred over the Internet, but only as a low quality image with slow frame update speeds. If the control centers only need to share a minimal amount of data, then the public Internet Methods described under data distribution might also suffice for data collection to an offsite center.

7.3 DATA DISTRIBUTION METHODS

7.3.1 Internet

The Internet, which is a global system of interconnected computers, has become very popular in today's society. The Internet originally began as a small, specialized network connecting scientists to distant computers and to each other, around the country and around the world. The concept proved so successful that the network steadily grew beyond the scientific community to include researchers and educators from all fields of study and from all kinds of organizations. This foundation in the academic community produced an open and uncensored environment that still exists today.

At its core, is a network of high-speed backbone links between major providers such as AT&T, Sprint, MCI and others. Branching off of the backbone are many thousands of smaller providers. Protocols are standardized so that any one computer can communicate with another, no matter where it is in the world.

Use of the Internet is very attractive as a public data distribution mechanism, as many people already have access (or can obtain it for a low cost) and are familiar with the systems and software needed to receive the data. The most popular element of the Internet is the World Wide Web, which converts tagged text strings and other elements into a graphical representation on a users "browser." The screens can be rich in visual and active content and are ideal for both map or text based information delivery.

The negative side is that most people have a relatively slow connection to the Internet (33.6 kbps) and viewing high-content information can take some time. Future modem and telephone system enhancements should help alleviate this problem.

7.3.2 Proprietary Connections

One type of connection that could be used for secure control center to control center communications is a leased line or a dedicated line. This would essentially be an extension of the network as described and could use any of the media and protocols discussed earlier. In addition, the system could be configured as an "Intranet,"

where only certain users are allowed to receive the data, but it could still be formatted for the web browsers with which many people are familiar. Alternately, special software could also be used to format and display the data.

7.3.3 Remote Access

For controlled remote access to system data, a system of dial-up modems could be used. This would allow news media and others with the correct passwords to obtain information. As stated in Section 7.3.2, the system could be set up as an Intranet, or use special display software.

7.3.3.1 Security

Any computer system that stores or maintains sensitive data should have some type of security measures to reduce the threat of intruders into the system. A common method of security is in the form of password protection. Each user is assigned a user name and password. Some systems allow the user to pick the password and others are computer generated. The timeframe for mandatory password changes may be from every login to once a month or beyond. Proper user name and password must be entered before access is allowed.

Even within the system, users could be assigned a user level which would restrict their level of access to certain parts of the system or its data. These features could be used for local, as well as, remote access to the Gateway.

When controlled access is desired, several measures can be put into place. First, in a dial-up system, a username and password should be required. As the physical connection between the client and the server does not traverse a publicly "viewable" network (as in the Internet), there is little danger (although not impossible) of someone capturing these passwords. Only if someone obtained both the username/password pair and the phone number, could security be breached.

For an Internet or Intranet system, more secure methods must be used. The concerns are that someone could see an unsecured password on the public network and then duplicate it later to get into the system. In addition, it is likely that other computer systems at the control center could be compromised. Fortunately, there are several ways to solve the problems. First, the majority of systems at the control center should be behind a "firewall," which is a computer dedicated to security. Firewall systems allow users inside to get out, but do not allow outside users to get in. In addition, the data server which contains the information should use what is known as secure-sockets layer (SSL). This is a method of encryption which is nearly impossible to break and is more than sufficient for the needs of such a system. One more method involves the use of a "Virtual Private Network," where secure data between two points is "tunneled" through the public Internet. Tunneling involves the use of secure, encrypted data, which is passed though the Internet as though it were a private network.

Any or all of these methods can be used to ensure system security.

7.3.3.2 Dedicated

A dedicated system would install a specific point-to-point link between two points, using either digital or analog circuits. If analog circuits are used, then a bank of modems would be required at the control center. Digital

circuits allow more flexibility, as either a point to point circuit could be used (i.e., 56 kbps or ISDN) or a switched type (frame relay). The advantages of frame relay are that no large infrastructure is required at the control center. Once the necessary equipment is installed (a router), more users can be added onto the system at any time by the phone company. Only small reconfigurations are required at the control center. If point-to-point links are used, there must be a one-to-one correspondence between users and hardware, thus increasing the cost and complexity of the system.

Frame relay can only be used over digital lines. The difference between frame relay and analog multipoint connections is that with an analog connection, all data is sent to all sites. With frame relay, the phone company system routes the data to only those sites at which it is needed.

7.3.3.3 Dial-in

A dial-in system would be set up very similarly to the dedicated system described above. There would be a bank of modems to handle dial-in users, but not necessarily a one-to-one relationship between users and modems. If a high percentage of the ratio is not maintained however, some users will get busy signals when attempting to obtain data.

7.3.3.4 Internet

On-line services to access the Internet represent a means to disseminate pre-trip traveler information. A wide variety of organizations have developed, or are currently developing, pages on the World Wide Web which provide highway and transit related transportation services and information for major metropolitan areas around the country. These pages provide both static and real time information and can be useful for obtaining information before a trip commences.

Several agencies have developed real-time access to traffic data, including CALTRANS and Georgia DOT, which sponsor two of the largest site with the most information available.

7.3.4 Other Distribution Methods

There are several other information distribution methods available. These are described below

7.3.4.1 Personal Communications Devices

Personal Communication Devices (PCDs), or personal digital assistants as referred to by some, utilize one or two-way wireless communication to small devices which relay information to the user. PCDs operate on limited bandwidth and are not designed for high-speed transfer of large data blocks. Examples of a PCD include alphanumerical pagers, cellular telephones and portable computers which are equipped with alphanumeric paging cards.

In several areas of the country, traffic and other data is formatted and sent to these devices over both wireless networks. This can be a useful distribution method.

7.3.4.2 FM Subcarrier

Another radio-based method for transmitting traveler information is to broadcast digital information over a privately operated, FM subcarrier allocation network. Commercial FM radio has "space" between the frequencies. This spare space, which serves as a buffer between stations, can be used to transmit a limited amount of digital information. Radio stations often lease the service as a way of partially offsetting operating costs.

FM subcarrier offers opportunities for providing information to travelers who have access to an FM receiver. Digitally encoded data are transmitted over the FM airwaves, received and decoded/interpreted by an intelligent device added to the FM receiver. The information may be presented in the form of a text and graphic displays or synthesized voice.

7.3.4.3 Radio Data Systems

FM Sideband was invented by the British Broadcasting Corporation. It is also known as Radio Data System (RDS) in Europe and Radio Data Broadcast System (RDBS) in the United States. It involves the use of existing FM radio broadcasts as a bearer for additional data. The information sent takes the form of coded data messages which are presented to drivers via specially designed FM entertainment radios. It provides a silent, digital channel which can be added to any FM radio station. RDBS was recently adopted as a North American standard by the National Association of Broadcasters. An earlier European system known as radio data system (RDS) has implemented some of the features provided by RDBS.

The primary motivation behind RDBS is to allow commercial radio broadcasters to be identified on the front panel of the radio and to allow special self-tuning radios to select the strongest signal carrying a designated entertainment program or to scan among radio stations offering a specific type of programming. However, a secondary function provided by RDBS is the conveyance of traveler information. This function would be provided in two ways. In the first case, codes are defined within the RDBS protocol to indicate to a radio receiver that a particular FM station periodically carries traffic reports and that this station is currently broadcasting such a report (traffic announcement code). The receiver could then use this information to automatically interrupt the current entertainment program to present the voice announcement to the driver. RDBS is at this point not widely deployed in the U.S., but may become a viable alternative for motorist information in the future.

<<This Page is Intentionally BLANK>>

8.0 SUMMARY

This working paper presented an overview of various hardware and software options for the Gateway. While certain of the options relate to software that is in the public domain, such as the NTCIP family of protocols, others are either fully or partially proprietary, such as the operating systems.

It should also be noted that while there appears to be a large number of options, these options will be reduced as the functionality of the Gateway is defined. In addition, once a particular course of action is determined, the number of options available will be reduced.

<<This Page is Intentionally BLANK>>