FINAL

Multi-Modal Traveler Information System

GCM Corridor Architecture Interface Control Requirements Document #17300.02

Prepared by:
De Leuw, Cather & Company
in association with:
JHK & Associates and
HNTB Corporation

Issue Date: October 31, 1997

GARY-CHICAGO-MILWAUKEE CORRIDOR
MULTI-MODAL TRAVELER INFORMATION SYSTEM
GCM CORRIDOR ARCHITECTURE
INTERFACE CONTROL REQUIREMENTS

TABLE OF CONTENTS

LIST OF FIGURES

GARY-CHICAGO-MILWAUKEE CORRIDOR
MULTI-MODAL TRAVELER INFORMATION SYSTEM
GCM CORRIDOR ARCHITECTURE
INTERFACE CONTROL REQUIREMENTS

1. INTRODUCTION

1.1 PROJECT OVERVIEW

The Multi-Modal Traveler Information System (MMTIS) project involves a large number of Intelligent Transportation System (ITS) related tasks. It involves research of all ITS initiatives in the Gary-Chicago-Milwaukee (GCM) Corridor which are currently deployed as well as proposed ITS identified in regional strategic plans and early deployment studies. This information will be used to recommend a MMTIS Corridor Architecture that best suits the characteristics of the diverse needs and resources within the Corridor.

The deployment of the MMTIS will provide a comprehensive, integrated, and multi-modal transportation system that serves the needs of travelers and operators within the GCM Corridor. This system will focus on the collection and distribution of transportation related information and the management of regional multi-modal transportation systems for the benefit of the Corridor. It will also provide the communications mechanism for the implementation of cooperative control procedures for cross agency control of ITS devices.

There will be a minimum of a two phased implementation for the GCM Corridor Gateway TIS. "Initial" and full build-out or "Ultimate." The primary difference between the initial and ultimate phases of the Gateway TIS will be the type of data connections to the data source systems.

The Gateway serves as the central collection and distribution hub for traveler information within the GCM Corridor.

1.2 PURPOSE

The purpose of this document is to identify and define the overall requirements for interfacing between the components of the Corridor Architecture (specifically regional hubs and ITS subsystems) in support of the Multi-Modal Traveler Information System.

These requirements are identified in order to support the design of the Gateway TIS. They provide details regarding interfaces within the Gateway TIS defined in Document #17150 (*Gateway System Definition Document*). This document, in combination with Document #17200 (*Corridor Architecture Functional Requirements*) is intended to be used to gain a more complete understanding of the system. These requirements are intended as testable statements of system design and operation.

1.3 GOALS

This document has the following goals:

- Provide a set of requirements to serve as a baseline for the Gateway TIS design, system integration, validation, and verification.

- Reduce the cost of the design and development effort for the Gateway TIS by minimizing omissions, misunderstandings, and inconsistencies early in the design cycle.
- Provide a basis of understanding among the system designers, participants, and users.
- Provide input to the design and update of ITS within the Corridor, in order to facilitate communications and connection to the Gateway and Gateway TIS.

These requirements will be changing, evolving, and expanding over time. This document will be revised to reflect the changing requirements of the Corridor Architecture. The scope and behavior of a number of ITS projects within the GCM Corridor have not been completely identified or determined at the initial writing of this document.

The Gateway development is targeted in two phases, the initial and the ultimate. These requirements are directed towards both phases. The goal is for complete implementation of these requirements for the ultimate phase.

Note that this document does not describe interface controls in a traditional sense of operating an embedded system or electronic device. Rather this document discusses the movement of information between agencies, specifically the electronic communications between computing equipment involving the passing of agency data and cooperative control requests through this communication line.

1.4 INTENDED AUDIENCE

This document is intended for:

- The GCM Architecture, Communication, and Information Work Group and the Deployment Committee.
- Members of various design groups that have development responsibility for the Gateway, the Gateway TIS, and for other ITS projects within the Corridor.
- ITS agencies who wish to communicate with the Gateway.
- Other parties who may be contemplating the design of a similar ITS communication infrastructure.

1.5 DOCUMENT ORGANIZATION

This document is organized into different sections. **Within each section, specific requirements will be distinguished by being formatted to the fifth heading level (i.e., 9.2.1.3.1)**. Section 2 provides the overall Corridor Architecture requirements in terms of the various members and the basic information flow. Section 3 discusses data compatibility issues and location referencing issues. Section 4 discusses communication interface options and general interface control issues. Section 5 deals with specifics of using the Gateway TIS for cooperative control of resources within the Corridor. Section 6 details the interfaces between the regional hubs and the Gateway. Section 7 discusses interfaces within the various regional areas.

1.6 TERMINOLOGY

In the text of this document, the term “shall” means the statement calls out a necessary requirement which must be included in the design of the Gateway.

The term “may” means the statement indicates a potential capability which need not be initially implemented in the Gateway, but that the Gateway design must allow for that capability to be implemented in the future.

1.7 DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Document #17100-1 (*MMTIS Project Glossary*) contains all definitions, acronyms, and abbreviations associated with this project along with pertinent TIS, communications, computer technology, and other standards in general.

Base GCM LRMS	The location referencing message specification that will be used throughout the GCM Corridor. The profile that will be used initially will be the Geographic Coordinate Profile (latitude, longitude, altitude and street name) with the possibility of supporting more profiles in the ultimate phase.
Borman ATMS	The Indiana regional hub responsible for collecting and disseminating traveler data and information to/from the various ITS subsystems within Northwestern Indiana and providing that information to the Gateway. It will also serve as the interface between these subsystems and the Gateway.
CDSI	Communication and Data System Infrastructure - The Wisconsin Regional Hub responsible for collecting and disseminating traveler data and information to/from the various ITS subsystems within Southeastern Wisconsin and providing that information to the Gateway. It will also serve as the interface between these subsystems and the Gateway.
Corridor Architecture	The standards and practices associated with the design of the MMTIS which provide a recommended design for ITS subsystems, data sharing, and cooperative control within the Corridor.
Data Pipe	The communication network interconnecting the Gateway, regional hubs and ITS subsystems within the GCM Corridor.
Gateway	The physical hardware and software, resident in a central facility, that is responsible for collecting, routing and disseminating all the traveler information collected by the regional hubs.
Gateway TIS	The logical collection of regional hubs and ITS subsystems connected within the GCM Corridor to the Gateway, excluding field devices.
GCOM	GCM Corridor Object Model - The Corridor wide object models which describe ITS objects in the Corridor as well as additional control and coordination objects needed to support the Gateway and other systems within the Corridor.
Illinois Regional Hub	The facility responsible for collecting and disseminating traveler data and information to/from the various ITS subsystems within Northeastern Illinois and providing that information to the Gateway. It will also act as the interface between these subsystems and the Gateway.
ITS Subsystem	A facility within the GCM Corridor which is capable of providing and/or receiving traveler information to/from the Gateway TIS.

MMTIS	Multi-Modal Traveler Information System - The combination of all traveler modes and forms of transportation systems operated through various ITS subsystems within the project limits of the GCM Corridor.

1.8 RELATED DOCUMENTS AND WORKING PAPERS

This document is a 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 #17001 - *Project Operating Plan*
- Document #17100-1 - *Project Glossary*
- Document #17150 - *Gateway Traveler Information System (TIS) System Definition Document*
- Document #17200 - *GCM Corridor Architecture Functional Requirements*
- Document #17250 - *Gateway Functional Requirements*
- Document #17350 - *Gateway Interface Control Requirements*
- Working Paper #18250 - *Cellular 911 - State of the Practice*
- Working Paper #18380 - *Corridor User Needs and Data Exchange Elements*
- Working Paper #18400 - *Current and Proposed ITS Initiatives*
- Working Paper #18500 - *GCM MMTIS Strategic Plan*
- Working Paper #18520 - *Performance Criteria for Evaluating GCM Corridor Strategies and Technologies*
- Working Paper #18550 - *Alternative GCM Corridor Technologies and 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 Phased Implementation Plan*
- Working Paper #19210 - *Lessons Learned*
- Working Paper #19220 - *Gateway Design Options*
- Working Paper #19840 - *Variable Message Signs (VMS)/Highway Advisory Radio (HAR) State of the Practice*
- Working Paper #19845 - *Variable Message Signs (VMS)/Highway Advisory Radio (HAR) Suggested Guidelines*

2. OVERALL CORRIDOR ARCHITECTURE

The Gary-Chicago-Milwaukee (GCM) Corridor Architecture is intended to facilitate data sharing and cooperative control among ITS subsystems within the corridor. This document presents the requirements for interfacing between subsystems to form the Gateway Traveler Information System (TIS).

2.1.1.1.1 The Corridor Architecture shall be a hybrid distributed network where outlying participants are organized into regional hubs that communicate with the main Corridor server known as the Gateway.

2.1.1.1.2 ITS subsystems shall electronically communicate with their associated regional hub all relevant traveler data.

2.1.1.1.3 Field devices shall attach to the Corridor Architecture at the ITS subsystem level only.

2.1.1.1.4 The Gateway and the regional hubs shall provide center to center communications (for data sharing and cooperative control) and shall collect and distribute traveler information within the Corridor (to/from agencies and to information service providers [ISPs] and the general public).

This organization has a number of important benefits:

- It reduces the load on the Gateway (the central hub) by moving some of that load to the regional hub machines. These machines can perform some of the data analysis and organization and then pass the data to the Gateway in a more compact form.
- It reduces communication costs. Locating the hubs in geographically disperse locations (e.g., one in Wisconsin, one in Illinois, one in Indiana) allows local Gateway TIS users to connect at a lower cost to the hub. Communications between the hub and the Gateway can also be streamlined and purchased at lower cost.
- It allows for scaleability. Additional hubs can be connected as the Gateway TIS expands. Each additional hub can support a large number of additional users. If all users had to connect directly to the Gateway, resources there would be quickly overloaded.
- It allows local developments at regional hubs which do not have to be part of the entire Gateway TIS.

2.1.1.1.5 Currently planned regional hubs shall be located in each state.

2.1.1.1.6 As a result of existing infrastructure, the regional hub for the Illinois region may be collocated with the Gateway.

The following figure illustrates the hub layout:

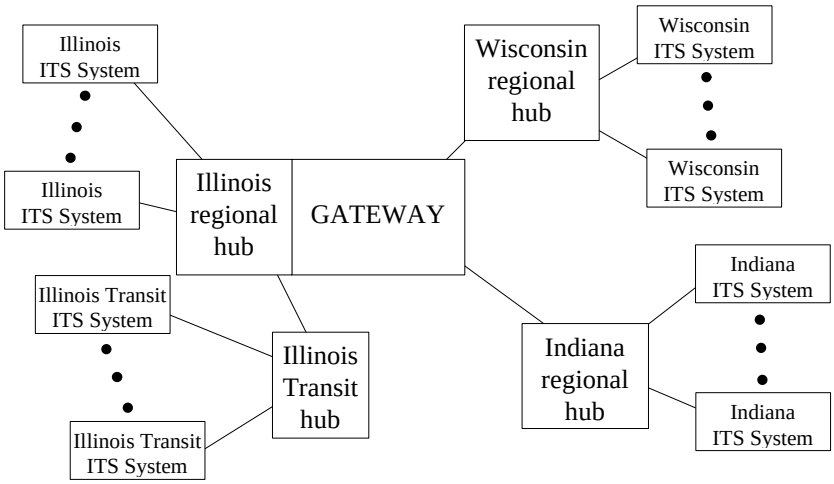

Figure 2-1 - Overall Corridor Connections

2.1.1.1.7 Interfaces between the regional hubs and the Gateway shall be designed and implemented according to the requirements found here and in Documents #17200, #17250, and #17350.

2.1.1.1.8 Interfaces between ITS subsystems and their regional hub shall also follow the requirements indicated in the documents referenced above.

2.1.1.1.9 This document provides requirements for the interfaces between ITS subsystems and their regional hub in the Corridor Architecture. It is likely to be the case that some interfaces between ITS subsystems and the Corridor Architecture will have special characteristics which will require unique designs. The advantage of the hub architecture is that these differences will be hidden from the Gateway and will be handled by the regional hubs.

2.1.1.1.10 The Gateway TIS shall interface with, and integrate data from, as many ITS subsystems within the GCM Corridor area as possible.

2.1.1.1.11 The Gateway TIS shall be easily adaptable for adding new interfaces.

2.1.1.1.12 The Gateway TIS shall be flexible and scaleable to handle new technologies and interface designs.

2.2 CORRIDOR ARCHITECTURE LEVELS

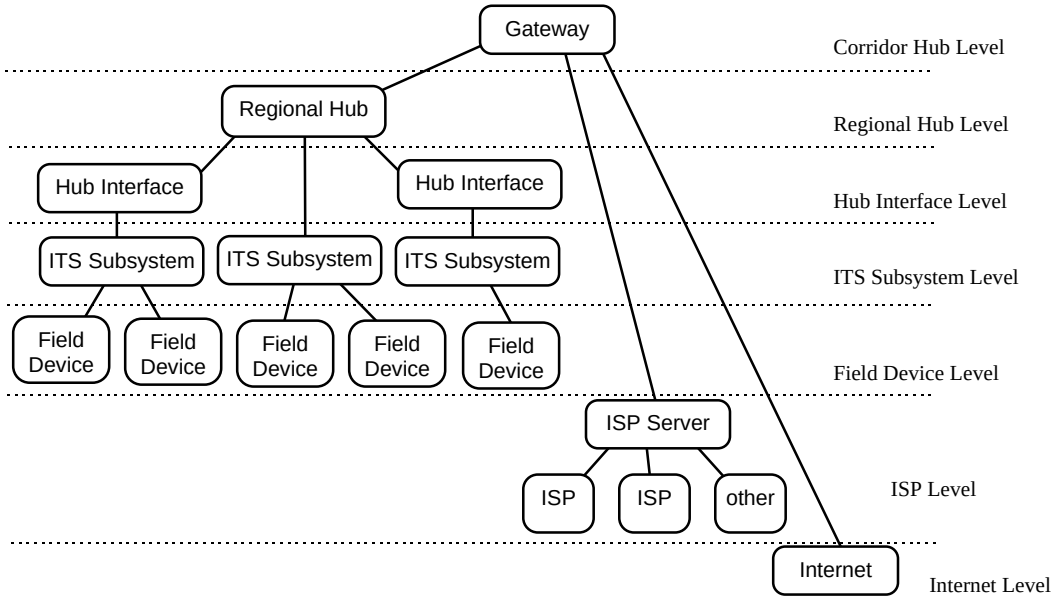

Figure 2-2 - Corridor Connections Hierarchy (Generic View)

Systems within the Corridor Architecture can be organized into levels of connection type and responsibility for data sharing and network routing. The following sections detail these various levels in the Corridor Architecture as shown in Figure 2-2.

2.2.1 Corridor Hub Level

The Corridor Hub for the GCM Corridor Gateway TIS will be the Gateway. The Corridor Hub is the central data collection and distribution point for all traveler information within the Corridor. The Corridor Hub connects to the various regional hubs and provides routing between the various state ITS subsystems within the GCM Corridor.

2.2.2 Regional Hubs Level

There will be three regional hubs within the GCM Corridor Architecture. These are regional hubs for Illinois, Indiana, and Wisconsin. An additional Illinois Transit Hub will also be used to coordinate data from Illinois based transit providers before passing that data on to the Illinois regional hub. The ITS data sources and data users within each state in the GCM Corridor will connect to the appropriate state hub to provide or receive data.

2.2.3 Hub Interface Level

In order to support legacy ITS subsystems within the Corridor, a number of hub interfaces will be fielded within the Corridor. The responsibility of these systems is to convert from legacy protocols and data formats into the Corridor standard protocols and data formats. The hub interface may be collocated with a legacy ITS subsystem and will provide the connection between the ITS subsystem and its regional hub. In cases where ITS subsystems are compliant with the Corridor Architecture and can interface directly through the GCM Data Pipe to their regional hub, the use of hub interfaces will not be needed.

2.2.4 ITS Subsystem Level

This level describes all ITS subsystems that are part of the Gateway TIS. These systems will connect through the GCM Data Pipe to their appropriate regional hub (either directly or through a hub interface). The systems provide ITS data to the Gateway from their field devices. They may also receive ITS data from their regional hub or from other ITS subsystems through the Gateway.

2.2.5 Field Device Level

This level describes field devices. Field devices are associated with a particular ITS subsystem and a particular agency. They are not considered directly part of the Gateway TIS. They are connected to their respective agency (ITS subsystem). The ITS subsystem (in cooperation with a hub interface, if needed) will convert the raw data from field devices into Corridor standard formats. All control of field devices will stay with the ITS subsystem. Cooperative control of field devices will be accomplished through software programs at the ITS subsystem (or hub interface) level.

2.2.6 ISP Level

This level describes information based agencies within the Corridor who need ITS data for dissemination or analysis purposes. It also includes dissemination devices such as kiosks, personal data devices, in-vehicle devices, etc. It also includes broadcast media as well as research organizations. These organizations would mainly be users of ITS information rather than providers. They will not connect directly to the Gateway, but would access data through a separate server, secured from the Data Pipe by a firewall.

2.2.7 Internet Level

The Corridor Architecture will also include connections to the Internet to provide data for use by the general public. The Internet connection may also provide more detailed data to Corridor ITS organizations and ISPs through the use of multiple secured, password protected, pages.

2.3 REGIONAL HUB ARCHITECTURE TOPOLOGY

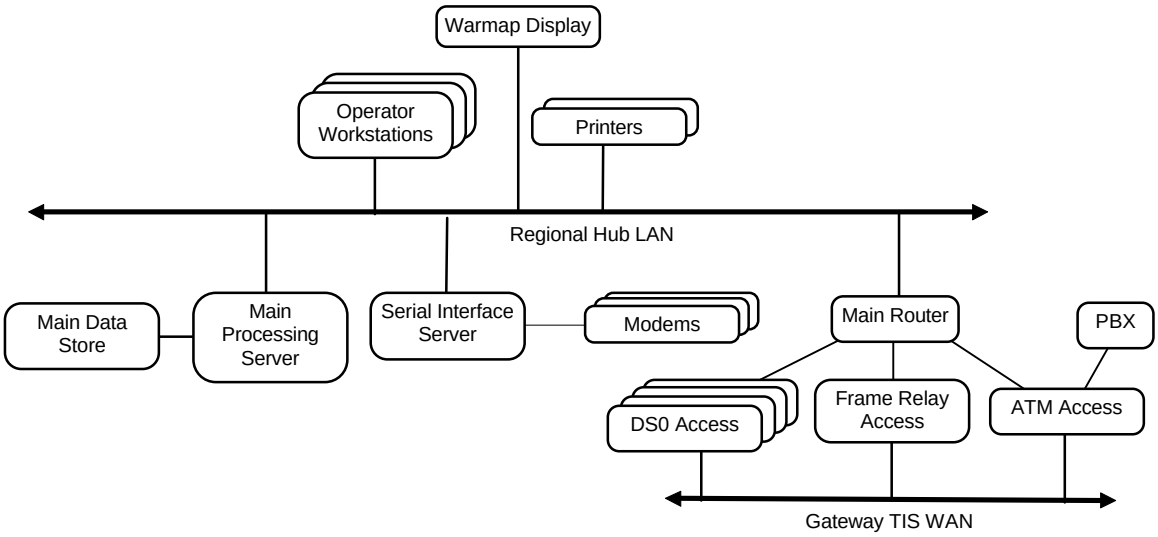

Figure 2-3 - Regional Hub LAN

2.3.1.1.1 A regional hub system shall consist of a range of communication and networking devices (switches, routers, modems, etc.) for communicating with the local ITS data sources; a number of server machines for data processing and storage; a number of operator workstations and system consoles for system control and monitoring; and, additional peripherals such as printers, faxes, pagers, etc.

2.3.1.1.2 A regional hub system shall be configured into a Local Area Network (LAN). A typical regional hub LAN environment is depicted in Figure 2-3.

2.3.1.1.3 A more detailed depiction of the regional hub LAN, including security zones, is contained in Appendix A of this document. A depiction of a typical ITS subsystem connection, with a hub interface system, is also shown. The regional hub LANs and ITS subsystem connections are recommended to conform to these diagrams.

3. DATA CONTENT AND INTERFACING REQUIREMENTS

This section first reviews general types of data to be interfaced. Next it discusses requirements for the transfer of information from one site to another (both within the hub and between the hubs and the Gateway). The requirements for data transfer involve the format of the data, the integrity of the data, and other coordination factors. These requirements are described in the sections below.

It is important to understand that the interfacing of data must be carefully controlled to avoid confusion, accidental misuse of data, and accidental misrepresentation of the facts.

There are two main ways of examining the data interchange to insure there is a common understanding. The first way involves how the providers and users of the data understand what they are exchanging to achieve data integrity. This means that the people involved in exchanging the data agree to the meaning of the data and to the fact that the data is useful.

The second way involves how designers of computer programs will view the data. Data can be used mistakenly if it is not tagged with supplementary information (e.g., the data is uncertain, or it is sensitive). Problems also arise from different impressions about how the data is aggregated or what the internal hierarchy and relational attributes of the data elements are. Here the use of good data representations and object oriented techniques can assist in making sure the systems within the Corridor can exchange data without being corrupted or losing information.

3.1 DATA CONTENT REQUIREMENTS

The system will collect and distribute information of the following contents.

3.1.1 General Requirements

3.1.1.1.1 For each type of data, appropriate standard object designs (i.e., an object data dictionary) shall be made which shall be used in all data sharing within the Corridor.

3.1.1.1.2 This object data dictionary shall be referred to as the GCM Corridor Object Model (GCOM).

3.1.2 Detector Data

3.1.2.1.1 Data from traffic detectors shall be made available to the Gateway TIS to allow for the calculation of congestion information for the national highway system routes/strategic regional arterials and other major arterials.

3.1.2.1.2 This data should be made available at standard periodic intervals. For example, IDOT's Traffic Systems Center provides the current C-TIC with data values every minute.

3.1.2.1.3 Systems which provide detector data shall use a permanent, reliable, electronic connection to the appropriate regional hub.

3.1.3 Travel Time Data

3.1.3.1.1 Travel time data (from whatever source) shall be made available to the Gateway TIS system to allow for the calculation of congestion information for the national highway system routes/strategic regional arterials and other major arterials.

3.1.3.1.2 This data should be made available at standard periodic intervals. For example, WisDOT's MONITOR system provides the current C-TIC with travel time values every five (5) minutes.

3.1.3.1.3 Systems which provide travel time data shall use a permanent, reliable, electronic connection to the appropriate regional hub.

3.1.4 Incident Data

3.1.4.1.1 Data from traffic impacting incidents shall be made available to the Gateway TIS where the incident affects the national highway/strategic regional arterials or other major arterial systems.

3.1.4.1.2 This data shall be made available in an event driven manner (i.e., the data shall be sent as soon as possible after the incident is known to the reporting agency).

3.1.4.1.3 Depending upon the frequency of incident information sent, systems which provide incident information may use a dial-up procedure to connect to the Gateway TIS if a higher bandwidth electronic connection is not installed.

3.1.4.1.4 Agencies which have a high rate of incident reports (more than one per hour) shall use a permanent electronic connection to the appropriate regional hub.

3.1.5 Construction and Maintenance Data

3.1.5.1.1 Data regarding scheduled closings of national highway/strategic regional arterials or other major arterial systems due to construction, maintenance, or special events shall be made available to the Gateway TIS daily or as soon as details are available.

3.1.5.1.2 Event data shall include start and stop times, possible lane closures or other traffic effects.

3.1.5.1.3 Event information shall be sent to the appropriate regional hub either through dial-up means or through a permanent electronic connection.

3.1.6 Transit Schedule Data

3.1.6.1.1 Data regarding scheduled transit times for public transportation shall be made available to the Gateway TIS. Additional data on schedule adherence should also be provided where it is available.

3.1.6.1.2 This data could also be made available through publishing on the Internet and providing the link address through the Gateway web pages.

3.1.7 Video Data

3.1.7.1.1 This type of data will consist of video images from cameras viewing the national highway or major arterial systems. Video data shall be made available throughout the Gateway TIS if such information is needed by other agencies within the Corridor and to the Internet.

3.1.7.1.2 Video data feeds create requirements for high speed communication capabilities and shall not be propagated through the Gateway TIS network unless necessary.

3.1.7.1.3 Agencies which provide or obtain video feed from the Gateway TIS shall be connected to the Gateway TIS through a high speed, permanent, electronic connection.

3.1.7.1.4 A standard, digital, video format shall be selected for video sharing in the Corridor. Similarly, a standard set of encoding schemes (for full motion and for slow scan and still pictures) shall be selected for the Corridor (either Motion-JPEG or MPEG-2).

3.1.8 VMS Data

3.1.8.1.1 The content and status of Variable Message Signs (VMS) shall be made available to the Gateway TIS by those agencies which have this data.

3.1.9 Weather Data

3.1.9.1.1 Information regarding road surface conditions and weather within the Corridor shall also be made available to the Gateway TIS.

3.1.9.2 Airport Data

3.1.9.2.1 Traveler information (possibly including schedules, schedule adherence information, parking data, and local traffic congestion information) for airports within the Corridor shall be made available to the Gateway TIS. Airports are anticipated to provide their own web pages, if this is the case, the Gateway shall include a link to the airport web pages.

3.1.9.3 Hazmat Data

3.1.9.3.1 For incident management purposes, data regarding the type of hazmat being transported in the Corridor, the schedule and route being taken, and if available, the current location of hazmat transport for the national highway system routes/strategic regional arterials and other major arterial roads shall be made available to the Gateway TIS by agencies who maintain such information.

3.2 DATA FORMAT REQUIREMENTS

Each system within the Corridor may have its own internal representation of data elements. When interfacing these systems, differences in data representation become very important and require unique programs to be developed for each different representation.

3.2.1.1.1 The Gateway and hubs shall make use of a common data representation.

3.2.1.1.2 This representation shall be object-oriented and based on the CORBA communication interfaces which the processes on the Gateway and hub machines shall use to communicate with each other.

3.2.1.1.3 The format of data sent to the Gateway TIS from the various ITS subsystems within the corridor shall also follow a set of standard formats and use CORBA calls.

3.2.1.1.4 The design phase of the Gateway shall provide the details for the formats which shall be used within the Corridor Architecture to exchange data. A limited set of formats will be designed for global use within the Corridor (corresponding, where appropriate, to NTCIP). These formats shall be part of the GCOM.

3.2.1.1.5 Interfaces between the Gateway and the hubs shall utilize the CORBA system and incorporate the common internal data representation.

3.2.1.1.6 It shall be the duty of the hub interfaces to convert the existing data format from each of its client ITS subsystems into the internal common data representation if not done at the source.

3.2.1.1.7 The conversion shall depend upon clear descriptions of the data representations on the client ITS machines and of the interface between the hub and the client system. In many cases, these conversions will be complicated programming tasks and thus must be carefully designed and implemented.

3.2.1.1.8 Specifically, the design shall provide at least the following:

- A set of CORBA IDL wrappers specifying object level communications interfaces.
- A set of serial data formats for systems which are not using the CORBA interface.
- A restricted set of video compression and format techniques to allow agencies to share video information and for video to be displayed on the WWW.

3.3 DATA INTEGRITY

This section discusses requirements for the data being exchanged regardless of the technique used to exchange it. Many of these issues revolve around the need for the Gateway or for the regional hub to know precisely what it is receiving. When data is analyzed by electronic means, even small misunderstandings or discrepancies between the data being received and what the system developers thought would be received can cause serious problems. For this reason, the integrity and control of the data content between interfacing systems cannot be trivialized or ignored.

Additionally, it is important for the end consumers of this data to know as much as possible about how the data was obtained and its reliability. Users should not expect the data to have characteristics that they do not have.

In the Gateway TIS, the primary concerns for data integrity involve the following factors. Each is discussed in detail in the sections that follow.

- Problems reconciling location information provided in different location referencing schemes.
- Differences in abbreviations and terminology.
- Multiple (possibly conflicting or corrective) reports for the same event or value.
- Data quality.
- Accidental distribution of sensitive or private information.

3.3.1 Location Referencing

Different ITS subsystems within the Corridor use different schemes for indicating the location of some object (e.g., an incident, a detector, etc.). For example, many 911 agencies use the street address to indicate an incident location; many highway systems use link information or latitude/longitude coordinates. The Gateway TIS needs to be able to fix a precise point (within a given tolerance) for data coming from each of these sources (and others).

The National ITS Architecture Project (organized by the US Department of Transportation and the Federal Highway Administration) is developing a set of architecture recommendations including a standard location referencing format referred to as LRMS (National Location Referencing Message Specification). The GCM will build off the national specification and develop a base GCM LRMS.

3.3.1.1.1 The Gateway TIS shall utilize the base GCM LRMS standard. All communication between the Gateway and the hubs shall conform to this base GCM LRMS.

3.3.1.1.2 LRMS describes a number of location referencing "profiles" or techniques which are supported within the LRMS umbrella. The Gateway and regional hubs shall initially use the Geographical Coordinate Profile as its base LRMS profile.

3.3.1.1.3 This profile describes locations by latitude, longitude, altitude, and cross street and shall be based on predefined GCM datum points throughout the Corridor.

3.3.1.1.4 Conversion programs between the base profile and other profiles shall be created as needed based on the same GCM datum points.

3.3.1.1.5 The results of the conversion programs which convert between agency specific location referencing and LRMS and between various LRMS profiles shall be verified and the programs modified until values are within the necessary tolerance.

3.3.1.1.6 Communication between Gateway TIS clients and their local hub are recommended to conform to the base GCM LRMS.

3.3.1.1.7 Support of the base GCM LRMS by other ITS subsystems within the Corridor will allow for better interoperability and increased assurance that locations indicated by one agency can be interpreted by another agency (possibly for a joint cooperative response). As there may be existing systems which cannot be altered to support the base GCM LRMS, hub interfaces shall be responsible for converting information to the base GCM LRMS where necessary.

3.3.1.1.8 Programs which convert between existing location referencing techniques and the base GCM LRMS shall be developed for use by hub interfaces for any non-compliant information from ITS client systems. Conversion should be done at the source wherever possible.

3.3.1.1.9 Output information provided by the Gateway to its clients shall be base GCM LRMS compliant.

3.3.2 Standard Abbreviations and Terms

The orientation of computing systems is towards exact matching. Fuzzy matching of patterns is difficult to program. As a result, a computer program can often fail to recognize that 123 Main Street and 123 Main St. are the same location.

3.3.2.1.1 A standard set of abbreviations and terms shall be constructed for the Corridor.

3.3.2.1.2 The hub interfaces shall include software which shall translate abbreviations used in messages and locations into the standard terms.

3.3.2.1.3 Where possible, the ITS subsystems within the Corridor shall use the standard set of abbreviations and terms in constructing data values to be provided to the Gateway TIS.

3.3.3 Data Duplication and Fusion

Considerable data integrity problems can arise from duplicate information being fed into a central data system like the Gateway TIS. This can involve duplication of incidents and other events (if they are reported by multiple data sources or if the same data source reports them multiple times). In this case, for example, calculated travel times can be off by a considerable amount. Some of the reasons for duplicate data are:

- Multiple sources reporting the same event.
- A source sends the same event multiple times by accident.
- A source sends a correction or update to the event, but the system does not connect the update with the original event.
- Information about the event is supposed to be sent by the source multiple times (e.g., for as long as the event is current), but the system does not understand this.

To handle this integrity problem it needs to be clear how a source will handle updates and corrections to previously reported information and how the Gateway TIS should respond.

3.3.3.1.1 The Gateway and regional hubs shall include a capability for recognizing duplicate reports and fusing them together.

3.3.3.1.2 This technique shall attempt to eliminate duplication of data values already reported (such as incident information or detector values).

3.3.3.1.3 These fusion techniques shall be able to recognize updated information and update related internal values appropriately.

3.3.3.1.4 This technique shall only be considered the last resort and should not be relied on to obviate the problem of duplication entirely.

3.3.3.1.5 Procedures shall be established in the Gateway TIS design for the interaction between the ITS subsystems in the Corridor and their hubs to document how data duplication and fusion issues will be handled.

3.3.3.1.6 In some cases (such as reports from *999) duplicate reports will be used to verify possibly erroneous initial reports.

3.3.4 Data Quality

The quality of the incoming data is very important to correct calculations and reporting. In some cases, agencies cannot verify the data instantly (e.g., a 911 call may be incorrect, or may reference the wrong location). The need to control the quality of the data provides a strong requirement on ITS subsystems.

3.3.4.1.1 Techniques shall be established to seamlessly and easily handle issues of data errors, updates and unknown information.

3.3.4.1.2 Techniques for canceling or updating erroneous incident reports and other data values shall be built into the Gateway TIS.

3.3.5 Private information

3.3.5.1.1 The Gateway TIS shall not receive private or sensitive information (e.g., license plate numbers, graphic accident descriptions) from the ITS subsystems.

3.3.5.1.2 This information shall be removed at the source before data is sent into the Gateway TIS.

3.3.5.1.3 Where this is not the case, the hub interfaces shall remove this information before sending data to the appropriate regional hub.

3.3.5.1.4 Some sensitive information may be needed by the Gateway. To insure information is not accidentally made public, it shall be identified as sensitive and tagged as such as it moves through the system.

3.4 DATA COORDINATION

A number of steps will be taken to coordinate and manage data within the Corridor Architecture. These steps will include appropriate source identification, sensitivity indication, and coordinated time values.

3.4.1 Source Identification

3.4.1.1.1 The regional hubs shall tag information from their client ITS subsystems to indicate the source of the information.

3.4.1.1.2 Information passed into the Gateway shall be traceable back to the ITS subsystem which created it.

3.4.2 Sensitivity Identification

3.4.2.1.1 The ITS subsystems or the regional hubs shall tag data with sensitive information which will indicate which data users can use that information.

3.4.2.1.2 It shall be the duty of the ITS subsystem or the regional hub to decide the level of sensitivity of a piece of information.

3.4.2.1.3 This sensitivity tag will be used when differentiating between data for general public consumption and data which will be password protected.

3.4.3 Time Coordination

3.4.3.1.1 The Gateway TIS shall provide a means for coordination of times among the systems within the corridor.

3.4.3.1.2 The Gateway shall have the authoritative time.

3.4.3.1.3 This time shall be passed to the regional hubs and from the hubs to their ITS clients.

3.4.3.1.4 The Gateway system shall use a reliable mechanism to obtain the current time, such as the current GPS system used by the C-TIC.

4. COMMUNICATIONS INTERFACE REQUIREMENTS

A considerable number of different physical techniques and hardware will be supported by the GCM Corridor architecture. The exact nature of the interface between an ITS subsystem and its regional hub will be selected based on data type, frequency, quantity, and criticality, plus available resources within the client ITS subsystem and the region from among the acceptable and supported techniques discussed in this section.

4.1 NTCIP

One of the goals for the Corridor Architecture is conformance with the National ITS Architecture standards and protocols for communication. Most of these standards and protocols are embodied in the National Transportation Communications for ITS Protocols (NTCIP).

The overall goal of the NTCIP is to provide “seamless” communications amongst ITS devices and systems using non-proprietary, open architecture techniques.

The NTCIP is currently being developed. While it is the intention that the interfaces within the Corridor Architecture conform to the standard, in some cases it is not clear what the standard will be and what solutions it will recommend or disallow.

4.1.1.1.1 The Corridor Architecture interfaces shall conform to the NTCIP standards.

4.1.1.1.2 The Corridor Architecture shall be able to incorporate new NTCIP standards as they arrive.

The focus of the NTCIP is primarily on communications between, from, and to field devices, control devices, embedded systems, operations centers, and independent service providers. The overall corridor systems described in this document usually correspond to operations-center-to-operations-center communications, or NTCIP Class E protocols.

Currently the NTCIP Class E protocols indicate the use of TCP/IP for the low level networking. Use of TCP/IP allows a wide range of alternatives for the physical network medium. NTCIP also allows the use of CORBA at the application layer for communications between centers.

4.2 COMMUNICATIONS

In order to support interoperability among the ITS subsystems within the Corridor, this document provides a required set of communication techniques for systems within the Corridor. Conformance to these requirements shall allow an ITS subsystem the best range of interoperability and communication with the other systems in the Corridor. Therefore, ITS subsystems should follow these requirements.

4.2.1.1.1 In the case that other influences prevent conformance, a range of other communications techniques shall also be supported. These techniques are discussed in the sections below.

4.2.2 Recommended Networking

4.2.2.1.1 The main Corridor Architecture shall be a Wide Area Network (WAN) to which the Gateway, the regional hubs, and a subset of the ITS subsystems in the Corridor shall belong.

4.2.2.1.2 The WAN shall be constructed using Asynchronous Transfer Mode (ATM) technology.

4.2.2.1.3 The connections between the regional hubs and the Gateway shall provide a bandwidth of at least 45Mbps.

4.2.2.1.4 Connections between the ITS subsystems and their regional hubs shall provide a bandwidth calibrated to the amount of data being sent and received. The minimum dedicated connection shall be 56kbps, the minimum dialup connection shall be 28.8kbps.

4.2.2.1.5 Internal networks at the Gateway, the regional hubs, and the connected ITS subsystems can either be ATM networks or can operate other protocols as long as converter equipment is available.

4.2.2.1.6 Internal networks (LANs) at the Gateway and the regional hubs shall support a transfer rate greater than 45Mbps.

4.2.2.1.7 The physical carrier for a particular WAN connection can be whatever medium is most appropriate to that connection (i.e., T1, T3, fiber, microwave, satellite, etc.).

4.2.2.1.8 Network traffic shall be routed appropriately within the WAN so that any two machines on the WAN can communicate with each other (through the Gateway) as long as appropriate permissions are set and approved.

4.2.2.1.9 Routers will also prevent unnecessary network traffic from being transmitted over segments of the WAN where they are not needed.

4.2.3 Recommended Data Exchange

4.2.3.1.1 Data communications between programs within the Corridor shall be through the Common Object Request Broker Architecture (CORBA).

4.2.3.1.2 A standard object design and hierarchy shall be constructed and CORBA IDL wrappers shall be constructed which support this communication.

4.2.3.1.3 Raw data feeds, such as audio or video, shall follow the formats provided by the design phase of the Gateway.

4.3 OTHER SUPPORTED COMMUNICATIONS

4.3.1.1.1 The Gateway TIS shall support additional Corridor standard communications techniques for communications between the regional hubs and ITS subsystems.

4.3.1.1.2 The Gateway TIS shall be designed to handle this range of communications techniques and be flexible enough to accommodate new techniques as they become available and are chosen as Corridor standards.

4.3.2 Electronic Based Communications

4.3.2.1.1 A range of additional electronic communications techniques may be at use within the Corridor (both wireline and wireless). They may use different protocols, different media, and different communications techniques. The regional hubs shall accommodate a subset of these systems.

4.3.2.1.2 Again, the regional hub will hide the details of unique interfaces and present a standard interface to the Gateway.

4.3.2.1.3 While there are many non-standard and proprietary solutions available, the interoperability and extensibility of the Corridor would benefit from the selection of open, non-proprietary, standards in communication protocol and hardware. As a result, the Corridor Architecture shall only include additional communications protocols and hardware based on open standards in concert with the NTCIP philosophy.

4.3.2.1.4 Priority will be given in allocating support for the various communications techniques to existing infrastructure and the recommendations of this document.

The communication techniques which shall also be supported include the following:

- Networked Dial-up

  A low speed, analog connection through standard phone lines using commonly available modems. The hubs may provide a set of modems for ITS clients to dial in on. Communications shall be based on using PPP to establish a temporary network link. CORBA or other advanced techniques shall then be used to communicate. This procedure should only be used for low volume, low frequency data.

- Networked Dedicated

  A digital connection, available at a range of speeds. Common speeds are 56Kbps connections and 1.544Mbps (T1) connections. Appropriate signal units at the client and at the hub maintain the connection. Communications shall be based on network protocols. Regional Hubs shall convert into ATM. This procedure shall be used for higher volume or higher frequency data.

4.3.2.1.5 The GCM Corridor currently makes use of a number of wireless communications services including microwave, spread spectrum, packet data radio, trunk radio, cellular, and satellite technologies. It is anticipated that these communications systems will be installed in specific circumstances within the Corridor and will continue to exist. The Corridor Architecture shall accommodate these wireless systems.

4.3.3 Non-Electronic Communications

4.3.3.1.1 A number of non-electronic communications techniques (listed below) shall be supported by the overall Corridor Architecture.

- Fax (to an operator at the regional hub)
- Traditional Phone Call
- Pager (to an operator at the regional hub)
- E-Mail (to an operator at the regional hub)
- Fax (to a computer at the regional hub)
- Pager (to a computer at the regional hub)
- E-Mail (to a computer at the regional hub)
- Traditional mail

- Internet access (including WWW browsing, FTP, direct TCP/IP routing, etc.)

4.3.3.1.2 Regional hubs shall construct a communications infrastructure to support a reasonable subset of these techniques.

Use of these techniques will be considered a temporary or interim technique until supported electronic communications can be established.

4.3.4 Data Exchange Techniques

4.3.4.1.1 The following additional techniques for exchanging data through electronic communications shall be supported by the Corridor Architecture:

1. E-mail

   This will require using any of a number of e-mail packages to send text formatted data for analysis. This technique is prone to errors (it is difficult to analyze the text). This technique also does not follow standard protocols.

2. FTP

   This technique utilizes FTP (File Transfer Protocol) to ship files between computers. Processes on the receiving computer notice the new file and begin processing it.

3. Telnet

   This technique uses connections through telnet to execute various shell commands on the receiving computer which simulate a user entering commands.

4. Sockets

   This technique connects to a running program on the receiving computer and basically sends a stream of data to that program and receives a stream of data back. This is the basic underlying mechanism for more advanced communication techniques.

5. Serial feed

   This technique utilizes a connection through a modem which does not perform any networking (e.g., not using PPP). The computer reading the serial information from the modem must run a specific program to send and receive raw data from the supplier. These connections shall be avoided wherever possible.

Use of these techniques will be considered a temporary or interim technique until supported CORBA based communication can be established.

4.4 SECURITY

4.4.1.1.1 Security is a concern when moving across a non-agency owned system. However, dedicated lines and WANs are often considered reliable. For these connections, simple user ids and passwords shall be required.

4.4.1.1.2 For dial-up connections, user ids and passwords shall be used to verify the identity of the caller.

4.4.1.1.3 For public networks (i.e., the Internet), data shall be encrypted before being transferred.

4.5 RELIABILITY

4.5.1.1.1 All data transfer methods shall incorporate error checking (e.g., checksums, CRC checks) and shall have procedures in place to deal with indications that errors are detected.

4.6 PERFORMANCE

4.6.1.1.1 The Corridor Architecture shall be designed with appropriate performance levels so that minimal data is lost or unprocessable when being transferred over the Corridor WANs and that any data transferred is received in a timely manner.

4.6.1.1.2 One exception to this requirement is the allowable dropping of video frames if they cannot be delivered on time.

4.6.1.1.3 However, video appearance shall not be allowed to seriously degrade.

5. COOPERATIVE CONTROL REQUIREMENTS

One of the objectives of the Corridor Architecture is to allow cooperative system control. This involves:

- A single agency implementing real-time measures across multiple jurisdictions and systems to ensure uniform and coordinated actions.
- One agency providing a function needed by multiple agencies to avoid the need for duplication of systems or to act as a backup or part-time service provider.
- A single agency integrating the operation of multiple local systems all within its jurisdiction.

5.1.1.1.1 The Corridor Architecture shall support cooperative control of:

- Variable Message Signs
- CCTV camera positioning and viewing
- camera data feed selection
- traffic signal control

5.1.1.1.2 Appropriate security shall be in place to insure that unauthorized users do not gain access to these cooperative control features.

5.1.1.1.3 Coordinated time of day information shall be propagated within the Gateway TIS to synchronize the times on cooperative control requests.

5.1.1.1.4 Cooperative control requests and responses shall be recorded by the Gateway or regional hubs and archived at the source.

5.1.1.1.5 Performance of the Architecture shall allow for the necessary throughput for these operations.

5.1.1.1.6 In particular, control of camera positioning shall have minimal delay to allow for ease of use.

5.1.1.1.7 The Architecture shall also support the following information sharing techniques:

- Corridor wide e-mail
- Video Teleconferencing
- Establishment of an Intranet
- Voice calls

5.1.1.1.8 The architecture shall also support the sharing of detector data in real time where it is appropriate for ITS subsystems to use in their travel time and incident detection algorithms.

6. INTERFACE CONTROLS (GATEWAY TO REGIONAL HUBS)

The following figure shows the Corridor WAN connections from regional hubs to the Gateway:

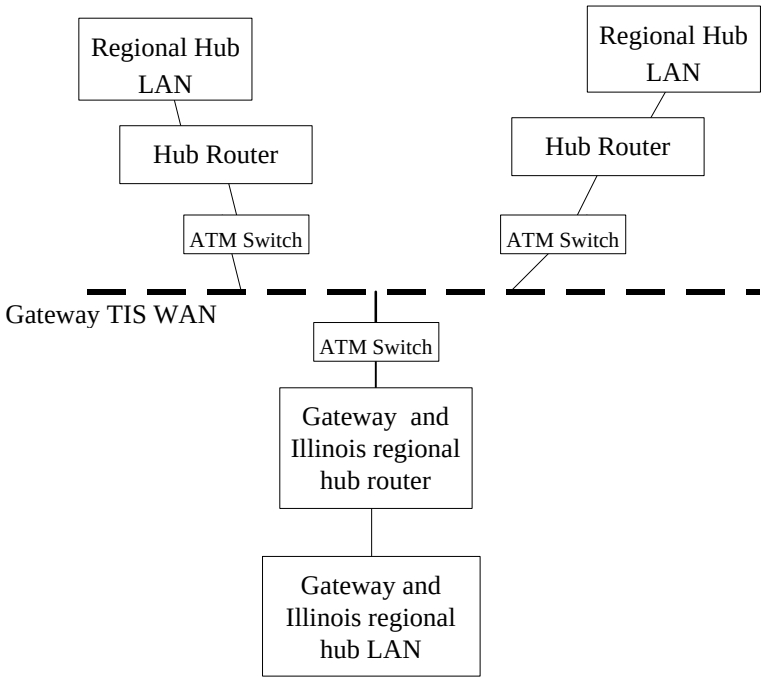

Figure 6-1 - Corridor WAN (Regional Hub to Gateway)

This section discusses the interface between the Gateway and the various regional hubs. This topic is discussed in detail in Document #17350 (*Gateway Interface Control Requirements*). Note that the Illinois regional hub and the Gateway will be collocated. As a result, the Gateway LAN will also include a range of equipment and servers which will be similar to those in other regional hubs.

6.1.1.1.1 The regional hubs and the Gateway will be connected through a Wide Area Network (WAN).

6.1.1.1.2 The WAN shall be composed of high speed permanent connections.

6.1.1.1.3 The WAN shall be operational 24 hours a day, 7 days a week.

6.1.1.1.4 The connections shall, at a minimum, support a reliable, high speed, continuous connection.

6.1.1.1.5 Bandwidth shall be sufficient to allow a number of video feeds (possibly 4) to be processed through the WAN without degrading the required speed of data and control information.

6.1.1.1.6 Full motion video can consume as much as 15Mbps of bandwidth. Compression techniques and frame dropping can reduce the requirement to approximately 10% of that value. Bandwidth shall be greater than the maximum amount required by the quantity and type of video feeds expected to cross a particular WAN connection.

6.1.1.1.7 Communication between the regional hubs and the Gateway shall be accomplished with the TCP/IP protocol as per the NTCIP.

6.1.1.1.8 The high level information protocol shall be the Common Object Request Broker Architecture (CORBA).

6.1.1.1.9 Data shall be sent to and from the Gateway through CORBA objects.

6.1.1.1.10 Processes dedicated to receiving data from the various regional hubs shall be constantly running on the Gateway and shall activate when data is arriving and shall escort it through the system and into the Gateway database.

6.1.1.1.11 If additional processing is immediately called for, it shall be initiated at this time (e.g., for a pass through command).

6.1.1.1.12 Outgoing raw or specially processed data which is to be routed through the regional hubs shall be sent over the WAN.

6.1.1.1.13 Primary output information shall also be sent over a high speed line to a Web Server which is connected to the Internet.

6.1.1.1.14 Data and control information shall have priority on the WAN over video feeds.

6.1.1.1.15 The Web server shall either be collocated within the Gateway or shall be reached by a high speed line.

6.1.1.1.16 The Gateway shall update its web pages based on its periodic feed of data.

6.1.1.1.17 The Gateway system shall also include other external distribution servers to broadcast to the media and other ISPs in the form of a stand alone ISP Server(s).

Additional details for the Gateway and its interfaces can be found in Documents #17250 and #17350.

7. INTERFACE CONTROLS (WITHIN REGIONS)

The following figure shows a typical regional hub with various connections to regional ITS subsystems and connection to the Gateway:

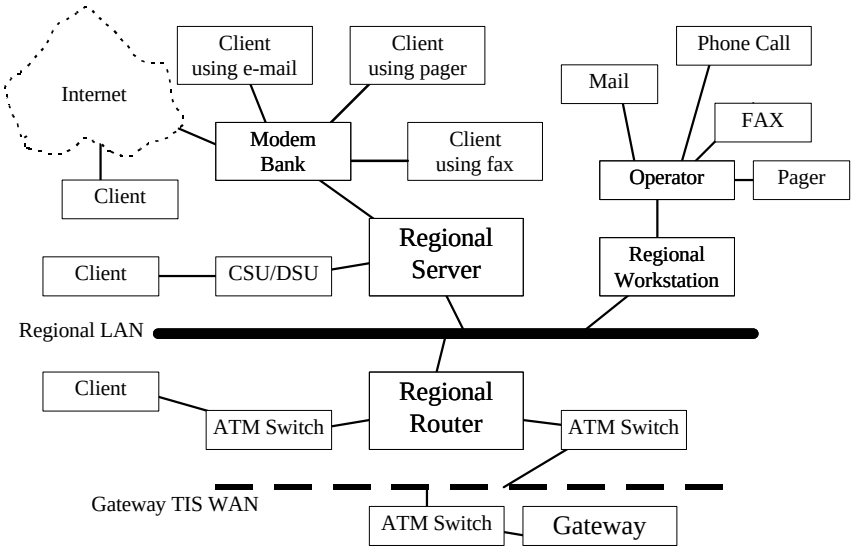

Figure 7-1 - Regional Hub Logical Architecture

In the sections below, each currently identified source and direct user of ITS data likely to connect to the Gateway TIS is identified. Additional sources and direct users will be added as the system evolves; one of the major goals of the Gateway TIS it to allow for this growth.

The sections below indicate the type of information available from the ITS subsystem, any data required by the ITS subsystem which will not be made available from the Gateway Internet pages, and any architecture requirements unique to the system.

7.1.1.1.1 The Corridor Architecture shall support connections to the ITS entities described in the following section.

7.1.1.1.2 The Architecture shall be designed to allow for a large number (100-300) of additional ITS clients to be connected as the need arises.

Additional detailed information regarding these and other potential ITS subsystems can be found in Working Paper #18600 (*Systems Interface and Data Exchange*) and in Working Paper #18400 *(Current and Proposed ITS Initiatives*).

7.2 ILLINOIS CONNECTIONS

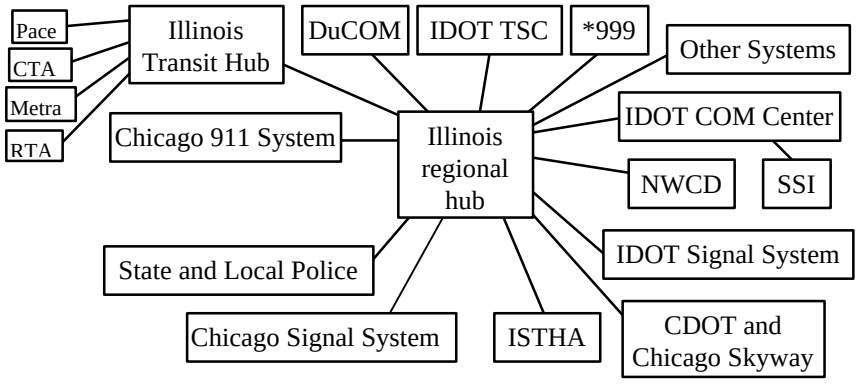

Figure 7-2 - Illinois Hub

7.2.1 General Requirements

7.2.1.1.1 The Illinois regional hub will communicate with the various ITS subsystems within the Illinois area of the GCM Corridor.

7.2.2 IDOT Traffic Systems Center

The TSC is responsible for managing congestion on the 150-mile IDOT District 1 expressway system. This system includes vehicle detection, ramp metering, Close Circuit Television (CCTV), Variable Message Signs (VMS), and CB radio monitoring sites.

7.2.2.1 Data Provided

7.2.2.1.1 The TSC receives real time data from over 2200 loop detectors along the regional expressway system and Lake Shore Drive. This data shall be volume, occupancy and/or speed information and provided to the Illinois regional hub.

7.2.2.1.2 Transmission of data for every loop detector shall be performed in a block of at least one minute intervals to the Illinois regional hub.

7.2.2.1.3 Additional transmission of loop detector information from the TSC may be needed by other ITS subsystems in the Corridor at faster rates than one minute. The TSC (through the hub interface) shall provide this data also.

7.2.2.1.4 The TSC operates algorithms which can detect the possibility of traffic incidents based on changes in loop detector data. Where incident likelihood is determined from detector data, the possible location of the incident shall be provided to the Illinois regional hub during the next available block data transfer.

7.2.2.1.5 The TSC shall provide VMS data (text message and sign status) every 5 minutes in the block data transfer to the Illinois regional hub.

7.2.2.1.6 The TSC currently has 3 CCTV cameras located along the Kennedy Expressway. These cameras have pan-tilt-zoom (PTZ) capabilities. Additional cameras are being installed in

strategic locations along the expressway system. The TSC shall provide digital video feeds from these cameras to the Corridor.

7.2.2.1.7 The TSC operates and manages the ramp metering devices for the Illinois District One highway system. The TSC shall provide the Illinois regional hub with ramp meter information such as: location, status (on/off) and possibly ramp meter rates.

7.2.2.1.8 Transmission of data for every ramp meter shall be performed in a block of at least one minute intervals to the Illinois regional hub.

7.2.2.1.9 Additional transmission of ramp meter information from the TSC may be needed by other ITS subsystems in the Corridor at faster rates than one minute. The TSC (through the hub interface) shall provide this data also.

7.2.2.2 Data Requested

7.2.2.2.1 The TSC shall field a computer for the purposes of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway (through the Illinois regional hub).

7.2.2.2.2 The TSC may obtain additional detector data (at more frequent intervals than used by the Gateway) from other ITS subsystems within the Corridor through the Corridor WAN.

7.2.2.2.3 The TSC may view video feeds from other ITS subsystems within the Corridor.

7.2.2.3 Cooperative Control

7.2.2.3.1 The TSC shall field a program that will allow other ITS subsystems within the Corridor to set messages on the TSC VMS (subject to TSC approval).

7.2.2.3.2 The TSC may need to set the VMS text of other ITS subsystems within the Corridor (subject to the operating agency's approval).

7.2.2.3.3 The TSC shall field a program that will allow the Gateway and other ITS subsystems to operate the PTZ capabilities of its CCTV cameras (subject to TSC approval).

7.2.2.3.4 The TSC shall field a program that will allow the Gateway and other ITS subsystems to select which of the TSC cameras it wishes to receive a video feed from.

7.2.2.4 Summary

7.2.2.4.1 The TSC shall need a high speed connection to the Illinois regional hub through a DS3 or higher bandwidth connection.

7.2.3 IDOT Communications Center

The Communications Center (COM Center) acts as the 24 hour incident management center for IDOT's District 1 and has control over the Highway Advisory Radio (HAR) system and the Kennedy Expressway reversible lane control (RevLac) system. During off hours, the COM Center operates the TSC's VMSs

Initially, IDOT District 1 agencies (ETP, construction/maintenance, traffic, etc.) shall provide data to the COM Center which shall in turn provide that data to the Illinois regional hub. In the

future, direct connections from various IDOT District 1 agencies to the Illinois regional hub may be established.

7.2.3.1 Data Provided

7.2.3.1.1 Data regarding special events which affect traffic shall be sent to the Illinois regional hub as information is available to the COM Center.

7.2.3.1.2 The COM Center shall provide the Illinois regional hub with information on the direction of the reversible lanes on the Kennedy expressway. When the reversible lanes are changed, the COM Center shall inform the Illinois regional hub.

7.2.3.1.3 The COM Center currently has a range of cameras to view the status of the reversible lanes of the Kennedy Expressway. Additional cameras are being installed in strategic locations along the expressway system. The COM Center shall provide digital video feeds from these cameras to the Corridor.

7.2.3.2 Data Requested

7.2.3.2.1 The COM Center shall field a computer for the purpose of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway (through the Illinois regional hub).

7.2.3.2.2 The COM Center may need to view video feeds from other ITS systems within the Corridor.

7.2.3.3 Cooperative Control

7.2.3.3.1 The COM Center may need to set the VMS text of other ITS systems within the Corridor (subject to the operating agency's approval).

7.2.3.3.2 The COM Center shall field a program that will allow other ITS systems to select which of the COM Center cameras it wishes to receive a video feed from.

7.2.3.4 Summary

7.2.3.4.1 To support its video feeds, the COM Center must be connected to the Illinois regional hub using a DS3 or greater connection.

7.2.4 IDOT ETP

IDOT provides an Emergency Traffic Patrol capability know as the IDOT Minutemen. These ETP vehicles provide road service for disabled motorists and assists in traffic incidents.

Initially the ETP shall provide data to the COM Center which shall in turn supply that data to the Illinois regional hub. In the future, a direct connection between the Minutemen and the Illinois regional hub may be established.

7.2.4.1 Data Provided

7.2.4.1.1 The ETP shall provide data on incidents to the Illinois regional hub (possibly through the COM Center) as they occur. This does not exclude direct paging from the Minutemen.

7.2.4.2 Data Requested

7.2.4.2.1 TBD.

7.2.4.3 Cooperative Control

7.2.4.3.1 TBD.

7.2.4.4 Summary

7.2.4.4.1 Initially, no connection is required. In the future, a DS0 level connection may be established to the Illinois regional hub or a single high speed connection from IDOT District 1 to the Illinois regional hub may be established which can be used by the ETP.

7.2.5 IDOT Traffic

IDOT Traffic coordinates construction and maintenance activities on IDOT roadways.

Initially IDOT Traffic shall provide data to the COM Center which shall in turn supply that data to the Illinois regional hub. In the future, a direct connection between IDOT Traffic and the Illinois regional hub may be established.

7.2.5.1 Data Provided

7.2.5.1.1 IDOT Traffic shall provide data on planned and active construction and maintenance to the Illinois regional hub (possibly through the COM Center) as they occur or on a scheduled basis.

7.2.5.2 Data Requested

7.2.5.2.1 TBD.

7.2.5.3 Cooperative Control

7.2.5.3.1 TBD.

7.2.5.4 Summary

Initially, no connection is required. In the future, a DS0 level connection may be established to the Illinois regional hub or a single high speed connection from IDOT District 1 to the Illinois regional hub may be established which can be used by IDOT Traffic.

7.2.6 IDOT SSI Connection

The Scan System is composed of electronic equipment located at several remote field locations and at one central monitoring location. The equipment consists of surface and environmental sensors. The surface sensors, embedded in the pavement, provide surface condition information. The environmental sensors provide information such as air temperature, relative humidity, dew point and level of precipitation. There are currently between 60 and 70 sites with 250 pavement sensors in the three state area.

7.2.6.1 Data Provided

7.2.6.1.1 SSI pavements and environmental sensors are distributed throughout the GCM Corridor. The sensors provide information about the pavement surface condition (icy, wet, snow

covered, etc.) and the local air temperature, humidity, dew point, precipitation, wind speed and direction. SSI provides this data to IDOT's COM Center. The COM Center shall make this data available at their District 1 Headquarters and shall provide the data to the Illinois regional hub through an electronic connection on a 5 minute periodic basis.

7.2.6.2 Data Requested

7.2.6.2.1 None.

7.2.6.3 Cooperative Control

7.2.6.3.1 None.

7.2.6.4 Summary

7.2.6.4.1 To support the data transfer, the IDOT District 1 SCAN computer which has the SSI data needs to connect to the Illinois regional hub with at least a 56kbps type connection. In the future, a single high speed connection from IDOT District 1 to the Illinois regional hub may be established which can be used by the SCAN computer system.

7.2.7 IDOT Traffic Signal Systems

Throughout IDOT District 1 there are in excess of 180 traffic signals operated in Closed Loop Signal Systems (CLSS) on IDOT maintained roadways. These systems are comprised of on-street master controllers with actuated intersection controllers and a dial-up modem connection to a central location. The purpose of a CLSS is to allow real-time traffic monitoring and modifications from a remote centralized location, to allow automatic traffic response control based on actual vehicle traffic, and to provide a simple real-time notification and tracking of signal malfunctions.

7.2.7.1 Data Provided

7.2.7.1.1 IDOT's traffic signal system shall alert the Illinois regional hub when a signal malfunction is detected. It shall then alert the Illinois regional hub when the signal is operational.

7.2.7.1.2 In the future, detector information for travel time and other calculations shall also be provided to the Illinois regional hub from various traffic signal systems on the national highway/strategic regional arterials or other major arterials system within the Corridor.

7.2.7.2 Data Requested

7.2.7.2.1 None.

7.2.7.3 Cooperative Control

7.2.7.3.1 TBD.

7.2.7.4 Summary

7.2.7.4.1 Alerts from IDOT's signal systems shall be accomplished through dialup procedures to the Illinois regional hub. In the future a single high speed connection from IDOT District 1 to the Illinois regional hub may be established which can be used by IDOT Traffic Signal Systems.

7.2.7.4.2 Data from IDOT's signal systems should be coordinated in a central machine or machines located at IDOT which should then contact the Illinois regional hub when malfunction data is available.

7.2.8 ISTHA

The Illinois State Toll Highway Authority includes the North-South Tollway (I-355), the Tri-State Tollway (I-94 + I-294 + I-80/I-294), the Northwest Tollway (I-90) and the East-West Tollway (I-88). ISTHA is currently installing electronic toll collection equipment at all toll lanes in the system. In addition to collecting and processing toll payments automatically, plans include a process to determine vehicle travel times from the toll tag transactions. ISTHA also maintains VMSs and has an emergency dispatch capability (Highway Emergency Lane Patrol, or HELP). Future plans may include the addition of CCTV cameras along the tollway system.

7.2.8.1 Data Provided

7.2.8.1.1 ISTHA will be able to calculate travel times over the tollway system through electronic toll collection devices (located in vehicles) and roadside detectors and toll plaza based detectors. This data shall be provided to the Illinois regional hub.

7.2.8.1.2 Transmission of data for every road segment shall be performed in a block at five minute intervals to the Illinois regional hub.

7.2.8.1.3 ISTHA operates several VMS. Every 5 minutes, ISTHA shall include the VMS data (sign status and message text) in the block data transfer to the Illinois regional hub.

7.2.8.1.4 ISTHA shall provide the Illinois regional hub with construction and maintenance schedules on a daily basis.

7.2.8.1.5 Additional data regarding special events which affect traffic shall be sent to the Illinois regional hub as information is available to ISTHA.

7.2.8.1.6 ISTHA shall provide data on incidents known to HELP to the Illinois regional hub as they occur.

7.2.8.1.7 ISTHA may implement a number of cameras located along the tollway system. In the future, ISTHA may provide digital video feeds (at least 4) from these cameras to the Corridor.

7.2.8.2 Data Requested

7.2.8.2.1 ISTHA shall field a computer for the purposes of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway (through the Illinois regional hub).

7.2.8.2.2 ISTHA may need to view video feeds from other ITS systems within the Corridor.

7.2.8.3 Cooperative Control

7.2.8.3.1 ISTHA may field a program that will allow other ITS systems within the Corridor to set messages on ISTHA VMS (subject to ISTHA approval).

7.2.8.3.2 ISTHA may need to set the VMS text of other ITS systems within the Corridor (subject to the operating agency's approval).

7.2.8.3.3 ISTHA shall field a program that will allow other ITS systems to operate the PTZ capabilities of its cameras (subject to ISTHA approval).

7.2.8.3.4 ISTHA shall field a program that will allow other ITS systems to select which of the ISTHA cameras it wishes to receive a video feed from.

7.2.8.4 Summary

7.2.8.4.1 As a result of its video feed capability, a DS3 or greater line should be installed between ISTHA and the Illinois regional hub.

7.2.9 Chicago Department of Transportation (CDOT)

CDOT operates and maintains a range of transportation infrastructure within the City of Chicago. They coordinate construction and maintenance efforts. CDOT also operates a number of monitored signalized intersections in the downtown area and plans to expand its centralized monitoring capability to include all of the City's 2700 signalized intersections. In the future, CDOT may install CCTV cameras at strategic points within the Chicago transportation infrastructure. As well, CDOT may install VMS on major arterials in the Corridor.

7.2.9.1 Data Provided

7.2.9.1.1 CDOT shall provide the Illinois regional hub with construction and maintenance schedules on a daily basis.

7.2.9.1.2 In the future, CDOT shall provide VMS data to the Illinois regional hub.

7.2.9.1.3 In the future, CDOT shall provide CCTV video feeds to the Illinois regional hub.

7.2.9.1.4 CDOT's traffic signal system shall alert the Illinois regional hub when a signal malfunction is detected. It shall then alert the Illinois regional hub when the signal is operational.

7.2.9.1.5 In the future, detector information shall also be provided to the Illinois regional hub from various traffic signal systems on the national highway/strategic regional arterials or other major arterials system within the Corridor.

7.2.9.2 Data Requested

7.2.9.2.1 CDOT shall field a computer for the purposes of displaying the CGM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway (through the Illinois regional hub).

7.2.9.2.2 CDOT may need to view video feeds from other ITS systems within the Corridor.

7.2.9.3 Cooperative Control

7.2.9.3.1 CDOT shall field a program that will allow other ITS systems to operate the PTZ capabilities of its cameras (subject to CDOT approval).

7.2.9.3.2 CDOT shall field a program that will allow other ITS systems to select which of the CDOT cameras it wishes to receive a video feed from.

7.2.9.3.3 CDOT may field a program that will allow other ITS systems within the Corridor to set messages on CDOT VMS (subject to CDOT approval).

7.2.9.3.4 CDOT may need to set the VMS text of other ITS systems within the Corridor (subject to operating agency's approval).

7.2.9.4 Summary

7.2.9.4.1 To support receiving video feeds from CDOT, a DS3 or greater connection is needed.

7.2.9.4.2 Data from CDOT's signal systems shall be coordinated in a central machine or machines which should then contact the Illinois regional hub when malfunction data is available.

7.2.10 Chicago Skyway

The Chicago Skyway operates one toll plaza. Plans exist to upgrade that plaza to include electronic toll collection. If additional detectors are also included, the Chicago Skyway can provide travel time information to the Illinois regional hub. Construction and maintenance data on the Skyway shall be provided by CDOT to the Illinois regional hub.

7.2.10.1 Data Provided

7.2.10.1.1 TBD.

7.2.10.2 Data Requested

7.2.10.2.1 TBD.

7.2.10.3 Cooperative Control

7.2.10.3.1 TBD.

7.2.10.4 Summary

7.2.10.4.1 Connection to the Skyway should be supported through the main connection between CDOT and the Illinois regional hub.

7.2.11 Northwest Central Dispatch

Northwest Central Dispatch (NWCD) serves as the Police and Fire dispatch agency for seven cities in the Northwest suburbs of Chicago. NWCD handles traffic and non-traffic related emergency incidents. Traffic related incidents are filtered at NWCD and are currently provided to the C-TIC.

7.2.11.1 Data Provided

7.2.11.1.1 NWCD will provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.11.2 Data Requested

7.2.11.2.1 TBD.

7.2.11.3 Cooperative Control

7.2.11.3.1 TBD.

7.2.11.4 Summary

7.2.11.4.1 Connection to NWCD shall be through a DS0 Frame Relay circuit. In the future, a higher bandwidth, more interactive, connection may be established to provide the GCM warmap, video feeds and other data from the Gateway (if a Corridor Architecture compliant system is implemented).

7.2.12 *999

The Chicago metropolitan area currently uses a public sponsored, dedicated number, cellular emergency system, *999, to cover the City of Chicago and the surrounding six counties. There is a single command center for this operation which is staffed 24 hours a day. The operators receive in excess of 300,000 calls per year dealing with a variety of roadway based emergencies. The operators receive each call, note the incident information from the motorist, and relay the calls to the appropriate service providers.

7.2.12.1 Data Provided

7.2.12.1.1 *999 will provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.12.2 Data Requested

7.2.12.2.1 TBD.

7.2.12.3 Cooperative Control

7.2.12.3.1 TBD.

7.2.12.4 Summary

7.2.12.4.1 Connection to *999 shall be through a DS0 Frame Relay circuit.

7.2.13 Illinois State Police (District 15)

The Illinois State Police (District 15) provides policing services on the Illinois Tollroads.

7.2.13.1 Data Provided

7.2.13.1.1 The Illinois State Police (District 15) will provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.13.2 Data Requested

7.2.13.2.1 TBD.

7.2.13.3 Cooperative Control

7.2.13.3.1 TBD.

7.2.13.4 Summary

7.2.13.4.1 It is anticipated that the District 15 State Police shall share the main ISTHA to Illinois regional hub link. As such, they may access the CGM warmap.

7.2.14 Illinois State Police (District Chicago)

The Illinois State Police (District Chicago) provides policing services on the expressways and tollways in the Chicago area.

7.2.14.1 Data Provided

7.2.14.1.1 The Illinois State Police (District Chicago) will provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.14.2 Data Requested

7.2.14.2.1 TBD.

7.2.14.3 Cooperative Control

7.2.14.3.1 TBD.

7.2.14.4 Summary

7.2.14.4.1 Connection to Illinois State Police (District Chicago) shall be through a DS0 Frame Relay circuit. Alternatively a higher bandwidth, more interactive, connection may be established (if a Corridor Architecture compliant system is implemented in the future) which can provide the GCM warmap, video feeds and other data from the Gateway.

7.2.15 DuCom

DuCom provides centralized emergency dispatch service for 28 police and fire departments in the DuPage County area. DuCom is in the process of installing a new CAD (computer aided dispatch) system which will fully automate their operations. Connection to DuCom would be similar to that of NWCD and *999. Alternatively a higher bandwidth, more interactive, connection may be established which can provide the GCM warmap, video feeds, and other data from the Gateway (if a Corridor Architecture compliant system is implemented in the future).

7.2.15.1 Data Provided

7.2.15.1.1 DuCom may provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.15.2 Data Requested

7.2.15.2.1 TBD.

7.2.15.3 Cooperative Control

7.2.15.3.1 TBD.

7.2.15.4 Summary

7.2.15.4.1 Connection to DuCom shall be through a DS0 Frame Relay circuit (or higher bandwidth connection).

7.2.16 Police Departments

Various police departments in the Illinois section of the GCM Corridor have jurisdiction over parts of the national highway system/strategic regional arterials and other major arterials. Connections shall be made to as many local police dispatch systems as available. Connections to local police departments would be similar to that of NWCD and *999. Alternatively a higher bandwidth, more interactive, connection may be established which can provide the GCM warmap, video feeds, and other data from the Gateway (if a Corridor Architecture compliant system is implemented in the future).

7.2.16.1 Data Provided

7.2.16.1.1 Local police departments may provide data on traffic related incidents to the Illinois regional hub as they occur.

7.2.16.2 Data Requested

7.2.16.2.1 TBD.

7.2.16.3 Cooperative Control

7.2.16.3.1 TBD.

7.2.16.4 Summary

7.2.16.4.1 Connections to local police departments shall be through DS0 Frame Relay circuits (or higher bandwidth connection).

7.2.17 ILLINOIS TRANSIT HUB

The Illinois Transit Hub shall coordinate transit information from the following sources:

- The Chicago Transit Authority (CTA)
- Pace
- Metra
- The Regional transit Authority (RTA)
- Amtrak

It is envisioned that this hub will make transit schedules, schedule adherence, fare rates and other pertinent information from the above sources available to the public via the Internet and to other GCM participants through the Corridor WAN by way of a connection to the Illinois regional hub. Note that the Transit hub will not be available until sometime during the ultimate phase of the Gateway implementation. In the interim, direct, dedicated electronic connections from the above sources to the Illinois regional hub is recommended.

7.2.17.1 Data Provided

7.2.17.1.1 The CTA shall be capable of providing information on current bus and train schedules (i.e., delays, schedule adherence, fare rates, etc.).

7.2.17.1.2 The CTA shall be capable of providing bus locations (probe information), utilizing their AVL system, which can then be calculated into travel time information for NHS/SRA roadways.

7.2.17.1.3 The CTA shall be capable of providing traffic related incidents on NHS/SRA roadways as they occur.

7.2.17.1.4 Pace shall be capable of providing information on current bus schedules (i.e., delays, schedule adherence, fare rates, etc.).

7.2.17.1.5 Pace shall be capable of providing bus locations (probe information), utilizing their AVL system, which can then be calculated into travel time information for NHS/SRA roadways.

7.2.17.1.6 Pace shall be capable of providing traffic related incidents on NHS/SRA roadways as they occur.

7.2.17.1.7 Metra and Amtrak shall be capable of providing information on current train schedules (i.e., delays, schedule adherence, fare rates, etc.).

7.2.17.2 Data Requested

7.2.17.2.1 The CTA may field a computer for the purposes of displaying the GCM warmap.

7.2.17.2.2 The CTA may need to view video feeds from other ITS systems within the Corridor, specifically in the Chicago land area.

7.2.17.2.3 The CTA, Pace, Amtrak and Metra shall be capable of receiving Corridor data through a direct connection during the Initial phase and through the Transit hub after its implementation.

7.2.17.3 Cooperative Control

7.2.17.3.1 TBD.

7.2.17.4 Summary

7.2.17.4.1 Connections from the various transit systems to the Illinois Transit Hub shall conform to the bandwidth requirements that are outlined within this document and will be determined during the design phase..

7.2.18 Other

Any additional ITS subsystems within the Illinois area are candidates for connection to the Gateway TIS. The nature of connections between these systems and the Corridor Architecture will be determined when the need arises.

7.2.18.1 Data Provided

7.2.18.1.1 TBD

7.2.18.2 Data Requested

7.2.18.2.1 TBD

7.2.18.3 Cooperative Control

7.2.18.3.1 TBD

7.2.18.4 Summary

7.2.18.4.1 TBD

7.3 INDIANA CONNECTIONS

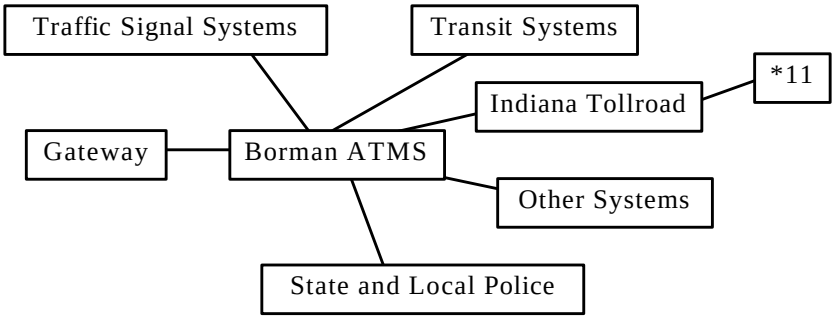

Figure 7-3 - Indiana Regional Hub Connections

7.3.1 General Requirements

7.3.1.1.1 The Indiana regional hub shall coordinate information from Indiana ITS subsystems within the GCM Corridor and provide that information to the Gateway.

7.3.1.1.2 The Borman ATMS Center shall provide the services of the Indiana regional hub.

7.3.2 Borman ATMS Center

The Borman ATMS will consist of complete deployment along the 16 miles of the Borman expressway beginning at the Illinois state line and continuing eastward. The Borman ATMS will consist of mainline vehicle detection, video surveillance, variable messages signs, highway advisory radio, the Hoosier Helpers freeway patrol, and a control center.

7.3.2.1 Data Provided

7.3.2.1.1 The Borman ATMS operates traffic detectors along the Borman Expressway. Traffic time data shall be provided to the Gateway through the Borman ATMS Indiana regional hub facilities.

7.3.2.1.2 Transmission of data for every detector shall be performed in a block of at least one minute intervals to the Gateway.

7.3.2.1.3 Additional transmission of detector information from the Borman ATMS may be needed by other ITS subsystems in the Corridor at faster rates one minute. The Borman ATMS shall provide this data also.

7.3.2.1.4 The Borman ATMS operates multiple variable message signs (VMS). Every 5 minutes, the Borman ATMS shall include the VMS data (text message and sign status) in the block data transfer to the Gateway.

7.3.2.1.5 The Borman ATMS shall include multiple CCTV cameras located along the Borman Expressway. The Borman ATMS shall provide digital video feeds from these cameras to the Corridor.

7.3.2.1.6 The Borman ATMS shall provide information on scheduled construction and maintenance, as well as any special events to the Gateway on a daily basis.

7.3.2.2 Data Requested

7.3.2.2.1 The Borman ATMS shall field a computer for the purposes of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway.

7.3.2.2.2 The Borman ATMS may obtain additional detector data (at more frequent intervals than used by the Gateway) from other ITS subsystems within the Corridor through the Corridor WAN.

7.3.2.2.3 The Borman ATMS may view video feeds from other ITS subsystems within the Corridor.

7.3.2.3 Cooperative Control

7.3.2.3.1 The Borman ATMS shall field a program that will allow other ITS subsystems within the Corridor to set messages on the Borman ATMS VMS (subject to Borman ATMS approval).

7.3.2.3.2 The Borman ATMS may need to set the VMS text of other ITS subsystems within the Corridor (subject to the operating agency's approval).

7.3.2.3.3 The Borman ATMS shall field a program that will allow the Gateway and other ITS subsystems to operate the PTZ capabilities of its CCTV cameras (subject to Borman ATMS approval).

7.3.2.3.4 The Borman ATMS shall field a program that will allow the Gateway and other ITS subsystems to select which of the Borman ATMS cameras it wishes to receive a video feed from.

7.3.2.4 Summary

7.3.2.4.1 As a regional hub, the Borman ATMS shall need a high speed connection to Gateway through a DS3 or higher bandwidth connection.

7.3.3 Indiana Tollroad Traffic Management Center

The Indiana Tollroad Traffic Management Center (TMC) operates the Indiana Tollroad (I90 and I80/90) in Indiana. The Indiana Tollway system is in the process of designing for electronic toll collection. When the system is complete it may include VMS and CCTV as well as travel time detection for the Tollroad.

7.3.3.1 Data Provided

7.3.3.1.1 The Indiana Tollroad TMC shall provide traffic time data as available to the Indiana regional hub.

7.3.3.1.2 Transmission of travel time data shall be performed in a block of at least one minute intervals to the Indiana regional hub.

7.3.3.1.3 Additional transmission of detector information from the Indiana Tollroad TMC may be needed by other ITS subsystems in the Corridor at faster rates than one minute. The Indiana Tollroad TMC shall provide this data also.

7.3.3.1.4 The Indiana Tollroad TMC may include multiple variable message signs (VMS). Every 5 minutes, the Indiana Tollroad TMC shall include the VMS data (text message and sign status) in the block data transfer to the Indiana regional hub.

7.3.3.1.5 The Indiana Tollroad TMC may include multiple CCTV cameras located along the Tollroad. The Indiana Tollroad TMC shall provide digital video feeds from these cameras to the Corridor.

7.3.3.1.6 The Indiana Tollroad TMC shall provide information on scheduled construction and maintenance, as well as any other special events to the Indiana regional hub on a daily basis.

7.3.3.2 Data Requested

7.3.3.2.1 The Indiana Tollroad TMC shall field a computer for the purposes of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Indiana regional hub.

7.3.3.2.2 The Indiana Tollroad TMC may obtain additional detector data (at more frequent intervals than used by the Gateway) from other ITS subsystems within the Corridor through the Corridor WAN.

7.3.3.2.3 The Indiana Tollroad TMC may view video feeds from other ITS subsystems within the Corridor.

7.3.3.3 Cooperative Control

7.3.3.3.1 The Indiana Tollroad TMC shall field a program that will allow other ITS subsystems within the Corridor to set messages on the Indiana Tollroad TMC VMS (subject to Indiana Tollroad TMC approval).

7.3.3.3.2 The Indiana Tollroad TMC may need to set the VMS text of other ITS subsystems within the Corridor (subject to the operating agency's approval).

7.3.3.3.3 The Indiana Tollroad TMC shall field a program that will allow the Gateway and other ITS subsystems to operate the PTZ capabilities of its CCTV cameras (subject to Indiana Tollroad TMC approval).

7.3.3.3.4 The Indiana Tollroad TMC shall field a program that will allow the Gateway and other ITS subsystems to select which of the Indiana Tollroad TMC cameras it wishes to receive a video feed from.

7.3.3.4 Summary

7.3.3.4.1 In order to provide video connections, the Indiana Tollroad TMC shall need a high speed connection to Indiana regional hub through a DS3 or higher bandwidth connection. In the event that video is not available or needed, the Indiana Tollroad TMC shall connect to the Indiana regional hub through a DS0 or higher bandwidth connection.

7.3.4 *11

The Indiana Department of Transportation Tollroad Division is currently using a cellular phone call in service to report emergency calls. This service is very similar in operation to the *999 emergency service in the Chicago land area.

7.3.4.1 Data Provided

7.3.4.1.1 *11 may provide data on traffic related incidents to the Indiana regional hub as they occur.

7.3.4.2 Data Requested

7.3.4.2.1 TBD.

7.3.4.3 Cooperative Control

7.3.4.3.1 TBD.

7.3.4.4 Summary

7.3.4.4.1 It is anticipated that *11 will share the main Indiana Tollroad TMC connection. If this is not the case, connection to *11 shall be through a DS0 Frame Relay circuit (or higher bandwidth connection) to the Indiana regional hub.

7.3.5 Police Departments

Various police departments in the Indiana section of the GCM Corridor have jurisdiction over parts of the national highway system/strategic regional arterials and other major arterials. Connections shall be made to as many local police dispatch systems as available. Connections to local police departments would be similar to that of NWCD and *999. Alternatively a higher bandwidth, more interactive, connection may be established which can provide the GCM warmap, video feeds, and other data from the Gateway (if a Corridor Architecture compliant system is implemented in the future).

7.3.5.1 Data Provided

7.3.5.1.1 Local police departments may provide data on traffic related incidents to the Indiana regional hub as they occur.

7.3.5.2 Data Requested

7.3.5.2.1 TBD.

7.3.5.3 Cooperative Control

7.3.5.3.1 TBD.

7.3.5.4 Summary

7.3.5.4.1 Connections to local police departments shall be through DS0 Frame Relay circuits (or higher bandwidth connection).

7.3.6 Other

Any additional ITS subsystems within the Indiana area are candidates for connection to the Gateway TIS. The nature of connections between these systems and the Corridor Architecture has not yet been determined.

Additional ITS subsystems within the Indiana hub area include (but are not limited to):

- Traffic Signal Systems and Closed Loop Signal Systems
- Transit Systems

7.3.6.1 Data Provided

7.3.6.1.1 TBD

7.3.6.2 Data Requested

7.3.6.2.1 TBD

7.3.6.3 Cooperative Control

7.3.6.3.1 TBD

7.3.6.4 Summary

7.3.6.5 TBD

7.4 WISCONSIN CONNECTIONS

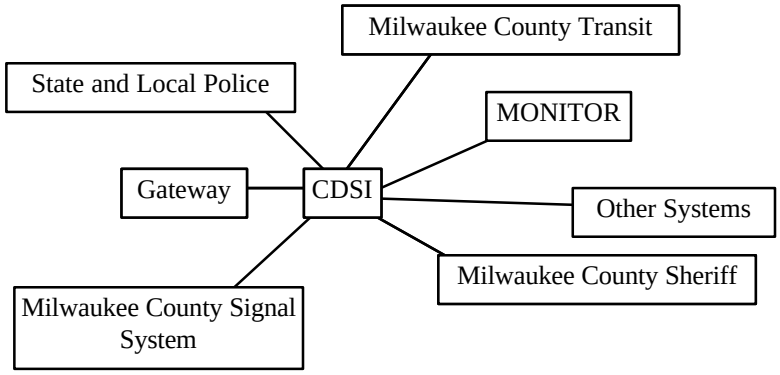

Figure 7-4 - Wisconsin Regional Hub Connections

7.4.1 General Requirements

7.4.1.1.1 The Wisconsin regional hub shall coordinate information from Wisconsin ITS subsystems within the GCM Corridor and provide that information the Gateway TIS.

7.4.1.1.2 Wisconsin is currently developing a project called Communication and Data System Infrastructure (CDSI). When this project is implemented it will serve as the regional hub for the Wisconsin area.

7.4.2 MONITOR

The MONITOR freeway traffic management program was initiated along the Interstate and primary highway network within the Milwaukee area to mitigate the increasing impacts of traffic incidents and recurring congestion by managing the existing freeway traffic. The MONITOR system consists of freeway mainline traffic detectors, Closed-Circuit Television (CCTV) cameras, ramp metering with exclusive High Occupancy Vehicle lanes, variable message signs, and related infrastructure.

7.4.3 Data Provided

7.4.3.1.1 MONITOR receives real time data from various detectors along their expressway system. This travel time information shall be provided to the Wisconsin regional hub.

7.4.3.1.2 Transmission of data for every travel time detector shall be performed in a block of at least one minute intervals to the Wisconsin regional hub.

7.4.3.1.3 Additional transmission of travel time detector information from MONITOR may be needed by other ITS subsystems in the Corridor at faster rates than one minute. MONITOR shall provide this data also.

7.4.3.1.4 MONITOR operates multiple variable message signs (VMS). Every 5 minutes, MONITOR shall include the VMS data (text message and sign status) in the block data transfer to the Wisconsin regional hub.

7.4.3.1.5 MONITOR currently has several CCTV cameras located along their NHS/SRA routes. These cameras have pan-tilt-zoom (PTZ) capabilities. MONITOR shall provide digital video feeds from these cameras to the Corridor.

7.4.3.1.6 MONITOR shall provide construction and maintenance, as well as any other special event information to the Wisconsin regional hub on a daily basis.

7.4.3.1.7 MONITOR shall provide the Wisconsin regional hub with ramp meter information such as: location, status (on/off) and possibly ramp meter rates.

7.4.3.1.8 Transmission of data for every ramp meter shall be performed in a block of at least one minute intervals to the Wisconsin regional hub.

7.4.3.1.9 Additional transmission of ramp meter information from MONITOR may be needed by other ITS subsystems in the Corridor at faster rates than one minute. MONITOR shall be capable of providing this data also.

7.4.4 Data Requested

7.4.4.1.1 MONITOR shall field a computer for the purposes of displaying the GCM warmap. The warmap shall be obtained by standard HTTP/Java transactions from the Gateway (through the Wisconsin regional hub).

7.4.4.1.2 MONITOR may obtain additional detector data (at more frequent intervals than used by the Gateway) from other ITS subsystems within the Corridor through the Corridor WAN.

7.4.4.1.3 MONITOR may view video feeds from other ITS subsystems within the Corridor.

7.4.5 Cooperative Control

7.4.5.1.1 MONITOR shall field a program that will allow other ITS subsystems within the Corridor to set messages on MONITOR VMS (subject to MONITOR approval).

7.4.5.1.2 MONITOR may need to set the VMS text of other ITS subsystems within the Corridor (subject to the operating agency's approval).

7.4.5.1.3 MONITOR shall field a program that will allow the Gateway and other ITS subsystems to operate the PTZ capabilities of its CCTV cameras (subject to MONITOR approval).

7.4.5.1.4 MONITOR shall field a program that will allow the Gateway and other ITS subsystems to select which of MONITOR cameras it wishes to receive a video feed from.

7.4.6 Summary

7.4.6.1.1 MONITOR shall need a high speed connection to the Wisconsin regional hub through a DS3 or higher bandwidth connection.

7.4.7 Milwaukee County Transit

The Milwaukee County Transit Systems (MCTS) SmarTrack Vehicle Management System included the replacement of each transit bus radio with a computer aided dispatched 800 MHz trunked radio system. The system includes schedule adherence, silent alarm, and Automated Vehicle Location (AVL) features. Additional features to be added to the system include automated passenger counting, automated real-time transmission of mechanical failure alarms, on-board video surveillance, real-time passenger information, fare collection, expanded transit traveler information services, and transit signal priority expansion.

7.4.7.1 Data Provided

7.4.7.1.1 The MCTS shall be capable of providing information on current bus schedules (i.e., delays, schedule adherence, fare rates, etc.).

7.4.7.1.2 The MCTS shall be capable of providing bus locations (probe information), utilizing their AVL system, which can then be used to calculate travel time information for NHS routes.

7.4.7.1.3 The MCTS shall be capable of providing traffic related incidents on NHS routes as they occur.

7.4.7.2 Data Requested

7.4.7.2.1 TBD

7.4.7.3 Cooperative Control

7.4.7.3.1 TBD

7.4.7.4 Summary

7.4.7.4.1 The connection from MCTS to CDSI shall conform to the bandwidth requirements that are outlined within this document and will be determined during the design phase

7.4.8 Milwaukee County Signal System

When Milwaukee's signal system is implemented, it shall provide information on travel times, signal malfunctions, and other pertinent traffic data to the Wisconsin regional hub which will share with the Gateway TIS.

7.4.8.1 Data Provided

7.4.8.1.1 Milwaukee County Signal System (MCSS) shall alert CDSI when a signal malfunction is detected. It shall then alert CDSI when the signal is operational.

7.4.8.1.2 Future provisions shall allow for travel time and other pertinent detector data to be provided to CDSI.

7.4.8.2 Data Requested

7.4.8.2.1 None.

7.4.8.3 Cooperative Control

7.4.8.3.1 None.

7.4.8.4 Summary

7.4.8.4.1 Alerts from MCSS shall be accomplished through dialup procedures to CDSI.

7.4.8.4.2 Data from MCSS should be coordinated in a central machine or machines which should then contact CDSI when malfunction data is available.

7.4.9 Milwaukee County Sheriff Dispatch

The Milwaukee County Sheriff's Department (MCSD) is currently in the process of implementing a Computer Aided Dispatch system to be incorporated into their new communications dispatch center to provide emergency dispatch services for the Sheriff's Department. The services that the new system will provide include: collection and reporting of calls for service; location and duration of incidents; statistical analysis of data; expansion of the existing 911 service; and provide a connection to MONITOR.

As this system is in early development, connection parameters are yet to be determined.

7.4.9.1 Data Provided

7.4.9.1.1 TBD.

7.4.9.2 Data Requested

7.4.9.2.1 TBD.

7.4.9.3 Cooperative Control

7.4.9.3.1 TBD.

7.4.9.4 Summary

7.4.9.4.1 The connection from The Milwaukee County Sheriff Department to CDSI shall conform to the bandwidth requirements that are outlined within this document and will be determined during the design phase

7.4.10 Police Departments

Various police departments in the Wisconsin section of the GCM Corridor have jurisdiction over parts of the national highway system/strategic regional arterials and other major arterials. Connections shall be made to as many local police dispatch systems as available. Connections to local police departments would be similar to that of NWCD and *999. Alternatively a higher bandwidth, more interactive, connection may be established which can provide the GCM warmap, video feeds, and other data from the Gateway (if a Corridor Architecture compliant system is implemented in the future).

7.4.10.1 Data Provided

7.4.10.1.1 Local police departments may provide data on traffic related incidents to the Indiana regional hub as they occur.

7.4.10.2 Data Requested

7.4.10.2.1 TBD.

7.4.10.3 Cooperative Control

7.4.10.3.1 TBD.

7.4.10.4 Summary

7.4.10.4.1 Connections to local police departments shall be through DS0 Frame Relay circuits (or higher bandwidth connection).

7.4.11 Other

Any additional ITS subsystems within the Wisconsin area are candidates for connection to the Gateway TIS. The nature of connections between these systems and the Corridor Architecture has not yet been determined.

7.4.11.1 Data Provided

7.4.11.1.1 TBD

7.4.11.2 Data Requested

7.4.11.2.1 TBD

7.4.11.3 Cooperative Control

7.4.11.3.1 TBD

7.4.11.4 Summary

7.4.11.4.1 TBD