FINAL

Multi-Modal Traveler Information System

Gateway
Functional Requirements
Document #17250.02

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

Issue Date: November 17, 1997

GARY-CHICAGO-MILWAUKEE CORRIDOR
MULTI-MODAL TRAVELER INFORMATION SYSTEM
GATEWAY FUNCTIONAL REQUIREMENTS

TABLE OF CONTENTS

LIST OF FIGURES

GARY-CHICAGO-MILWAUKEE CORRIDOR
MULTI-MODAL TRAVELER INFORMATION SYSTEM
GATEWAY FUNCTIONAL 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 projects identified in regional strategic plans and early deployment studies. This information will be used to recommend an MMTIS Corridor Architecture that best suits the characteristics of the diverse needs and resources within the Corridor.

The deployment of the Gateway Traveler Information System (TIS) 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 coordination 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. Together with the regional hubs and connections to ITS subsystems within the Corridor it composes the Gateway TIS.

1.2 PURPOSE

The purpose of this document is to identify and define the functional requirements for the Gateway and the Illinois regional hub components of the Corridor Architecture in support of the Multi-Modal Traveler Information System (MMTIS).

These requirements are identified in order to support the design of the Gateway. They provide statements of needed functionality and associated design requirements for the Gateway defined in Document #17150 (*Gateway TIS System Definition Document*) and the remainder of the Corridor Architecture. This document, in combination with Document #17350 (*Gateway Interface Control 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.

As the Gateway is part of the overall GCM Corridor Architecture, the system will also conform to requirements presented in Documents #17200 (*Corridor Architecture Functional Requirements*) and #17300 (*Corridor Architecture Interface Control Requirements*).

1.3 GOALS

This document has the following goals:

- Provide a set of functional requirements to serve as a baseline for Gateway design, system integration, validation, and verification.
- Reduce the cost of the design and development effort for the Gateway 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 subsystems within the Corridor, in order to facilitate communications and connection to the Gateway and Gateway TIS.

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. 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 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.

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 and Gateway TIS and for other ITS projects within the Corridor.
- ITS agencies who wish to communicate with the Gateway and through the Gateway TIS.
- 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 presents an overview of the Gateway system and its position and purpose within the Corridor Architecture and its association with the National ITS Architecture and standards. Section 3 discusses subsystem functional requirements for the Gateway and Illinois Hub. Section 4 discusses general requirements for Gateway design. Section 5 reviews the hardware based requirements for the Gateway and Illinois Hub. Section 6 reviews the requirements associated with commercial software within the Gateway and Illinois Hub. Section 7 discusses Gateway produced software and general Gateway and Illinois Hub testing strategy. Section 8 provides requirements for the Gateway web pages. Section 9 presents communications related requirements including bandwidth, wide and local area networking, and necessary hardware. Section 10 discusses unique requirements associated with the Illinois hub and Section 11 discusses requirements associated with the ISP server.

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 easily 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 ITS, communications, computer technology, and other standards in general.

The following terms, acronyms or abbreviations are used within this document:

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 #17300 - *GCM Corridor Architecture Interface Control 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. GATEWAY OVERVIEW

2.1 INTRODUCTION

This section will provide a system-level overview of the GCM Gateway's tasks, as well as the functional requirements to be achieved within the project. Additional details and requirements are contained in later sections of this document. This overview of the Gateway concept is given to establish a framework for the development of the necessary modules, data streams, operational procedures, and control flows, both during the initial (2-3 years) and ultimate phases (3 years and beyond).

The Gateway is a central part of the Gateway TIS, which unites ITS subsystems along with regional hubs into a computer network for the sharing of traveler information and for the facilitation of cooperative controls between ITS agencies. The Corridor Architecture defined in Document #17200 (*GCM Corridor Architecture Functional Requirements*) and #17300 (*GCM Corridor Architecture Interface Control Requirements*) supports the creation of the Gateway TIS.

This document is not intended to provide design specifications for any of the Gateway identified activities. However, in addition to the detailed functional requirements, important design or implementation statements will be made where appropriate. Another important note is that this project will be evolving over time, and thus, as new, not yet defined, ITS subsystems emerge throughout the Corridor, connections will need to be established to the Gateway TIS and/or the GCM Data Pipe. Therefore, this document will need to be modified and updated accordingly.

2.2 OBJECTIVES

The Gateway will be designed to serve several purposes in the GCM Priority Corridor as the Corridor Hub (uniting all regional hubs) for the Gateway TIS.

The primary responsibility of the Gateway and the Gateway TIS is to collect, organize, and redistribute all transportation related data including travel time, construction and maintenance, incident, and weather information on the National Highway System and Strategic Regional Arterials within the Corridor. In addition, the Gateway TIS will be multimodal, collecting and distributing transportation related data from a variety of transportation modes.

The other main objective of the Gateway and Gateway TIS will be to serve as a pass through for control and monitoring commands of various field devices among connected agencies where cooperative control agreements have been arranged.

In order to collect information from sources throughout the Corridor, the Gateway will be connected by a Corridor wide electronic network together with regional hubs within the three states and with all appropriate ITS data sources.

The Gateway will redistribute the information it collects from these sources.

Congestion, construction, and incident information will be provided to the public through numerous maps on the Internet. However, as newer technologies develop in the future, different ways to distribute the data will be explored.

Along with providing the regional hubs with real-time traveler information on a periodic basis, selective major data sources will also receive a Corridor wide "war" map. This map will supply more detailed information than that which is provided to the public and will be automatically refreshed at a minimum of every five minutes.

The Gateway will also have a special stand alone server for providing the different Information Service Providers (ISPs) in the Illinois area with traveler information for their own packaging and dissemination.

The Illinois regional hub shall be designed to interface with ITS subsystems within the Illinois area. It shall serve as a provider to the Gateway of data obtained from Illinois and will serve as a distributor for the Gateway for data requested by Illinois ITS subsystems.

Similar regional hubs, compliant with the Corridor Architecture, shall be located in Wisconsin and Indiana.

2.3 NATIONAL ITS ARCHITECTURE

The National ITS Architecture defines the interfaces and communications requirements for the information flows between physical subsystems. In so doing, it provides the framework with which to design an Intelligent Transportation System. The Architecture was specifically developed to allow multiple design approaches which can be tailored for specific environments and individual needs of the user by defining only required interfaces and their communications. This National ITS Architecture is the key to providing a base for the standards needed to support national and regional interoperability.

Each interface must supply the components with the required data for each required functionality. In other words, the interface must be standard. The ITS Architecture supports open communications standards and requires that the interface is able to network with other communications media by utilizing open standards. The Architecture also requires that the communications media provide the necessary coverage for each component. That is, if a National ITS System is deployed, seamless communications must be available nationwide.

Conformance with the National ITS Architecture is required throughout the entire GCM Corridor where appropriate and necessary. In regards to the development and design of the Gateway, the Gateway will act as the main Center Subsystem or focal point for the collection and distribution of traveler and transportation related data throughout the GCM Corridor and will be required to be compliant to the National Architecture.

2.4 NTCIP

The National Transportation Communication for ITS Protocol (NTCIP) is an evolving communications protocol that allows for interfacing between traffic control devices and centers, and center-to-center communications. Currently the NTCIP consists of a series of protocols for communications to/from and between field devices (actuated traffic signal controllers, message signs, etc.). Communications protocols between these types of components are referred to as Class B protocols. Class B protocols that are either already defined by the NTCIP Committee (or in the process of being defined) include those for actuated signal controllers, dynamic message signs, environmental sensor stations, highway advisory radio, freeway ramp meters, video camera control and traffic sensor stations. The Class B protocol technical specifications for traffic signal controllers have been published by NEMA. As the other Class B protocols are approved, they will also be released.

In the future, the NTCIP will also define the protocol for communications between transportation operations centers. These are referred to as center-to-center communications and are Class E protocols. Both Class B and Class E message structures are important to the GCM Corridor. The Gateway shall comply with the NTCIP standards as they currently exist and are defined in

the future. (Further discussion will be needed to define which options within a given NTCIP specification will be required.)

In setting the message structures for field devices, the NTCIP precisely defines the data to be exchanged for each field element (actuated signal controllers, dynamic message signs, environmental measurement devices, etc.). For center-to-center communications, the NTCIP needs to also define the data which will be exchanged. So far, there are four categories of data streams where definitions are being developed: Traffic Coordination, Event Notification, Data Sharing and Regional Command Distribution. All four of these categories are pertinent to the GCM Corridor. Traffic Coordination messages will allow the traffic management centers in different jurisdictions to coordinate operations. Event Notification messages will allow different jurisdictions to learn about events close to their borders that may impact their operations. Data Sharing messages allow the various agencies to collect and distribute transportation system data. Regional Command Distribution messages make it possible to coordinate the activity of multiple traffic management centers by issuing commands at a regional level.

2.5 LRMS

A common method of referencing transportation links and nodes is essential for many of the ITS services involving cooperative processing between ITS subsystems. A common frame of reference is needed so that these communications between subsystems can be rationally reduced to an unambiguous reference to the same transportation links, ramps, intersections, etc. A standard method for location referencing is being developed and is called the Location Referencing Message Specification (LRMS).

The GCM Architecture is adopting this specification to describe locations. This specification is being developed by Viggen Corporation and Oak Ridge National Laboratory (ORNL) with funding by FHWA. The GCM Corridor is one of the test sites for implementation of this specification. This specification is established so that all agencies within the Corridor will have the same reference points when describing locations. It is the intention that all agencies within the GCM eventually adopt and implement the LRMS format (considered “base” LRMS for GCM Corridor purposes throughout this document) for the ease of sharing and comprehending traveler data. Base GCM LRMS conformance will also aid in the receiving and transmitting of locations to other systems within the Corridor.

Currently the GCM Corridor is reviewing the compatibility between various map databases, with the intent of using different Corridor location data without major modifications. The accuracy of incident locations and construction and maintenance activities may be acceptable and not require a fully compatible system among all map databases.

If this is not the case, it may be necessary that the location referencing profiles be based upon predefined GCM datum points throughout the Corridor. The GCM datum points would serve as a standard network of ground control points that will anchor spatial references between databases of different kinds. If two databases have a common frame of reference (e.g., the GCM datum), then location referencing is a matter of posing references in terms of the common GCM datum regardless of the particular referencing method used. The GCM datum would support location referencing by geographic coordinates, linear referencing and link referencing. Therefore it could potentially support both existing, legacy databases in public agencies and the continuing growth of the vehicle map database industry.

Initially the Gateway will only distribute traveler data in the base GCM LRMS format. It is the responsibility of the receiving entity to conform with the base GCM LRMS. Of the several “profiles” specified by LRMS, for the Initial Phase it is envisioned that only the Geographic

Coordinate Profile will be used for dissemination, although the Ultimate design may require the Gateway to support more or all profiles. The Geographic Coordinate Profile consists of latitude/longitude/altitude and street name based upon the GCM datum discussed earlier.

The Gateway will be responsible for taking the data it receives and storing it using the base GCM LRMS standard. The Gateway will then distribute all traveler information to the regional hubs and ISPs in the base GCM LRMS format. Translations may be required in the inbound stream into the Illinois regional hub from existing Illinois ITS subsystems, before the information can be stored in the Gateway database in the base GCM LRMS format. All incoming data from the regional hubs to the Gateway are required to be in the base GCM LRMS format, and all out going data from the Gateway will be in the base GCM LRMS format.

The Gateway LRMS database will be based upon a non-proprietary software package that can accommodate all types of location information that may be input into the Gateway or used throughout the Corridor and be capable of supporting unique identifications to reduce the probability of ambiguous locations. The map database will also be capable of being modified/updated in situations where street names are changed or added, throughout the Corridor, in a seamless manner.

Where necessary, the Gateway may augment locationing data provided in the base GCM LRMS format with anecdotal information such as if a location is on a ramp, or what lane of a roadway is being referenced.

2.6 CORRIDOR ARCHITECTURE

2.6.1 Phased Approach

The Corridor Architecture will be deployed in two phases. The Initial Phase will consist of systems that will be implemented within the next two to three years and the Ultimate Phase will encompass the ultimate Corridor vision of systems to be developed or implemented after the Initial Phase. Please refer to Document # 18500 (*GCM MMTIS Strategic Plan*) and Document # 17150 (*Gateway TIS System Definition Document*), for a more detailed overview of the two phases.

2.6.2 Corridor Definition

The Gary-Chicago-Milwaukee Corridor is one of the corridors selected by the USDOT to receive priority attention under the ISTEA legislation. The corridor is broadly identified by the 16 urbanized counties in the states of Wisconsin, Illinois, and Indiana. It includes all major highways, airports, transit, and rail systems, ports and intermodal transfer stations. The GCM Corridor extends 130 miles and covers more than 2,500 square miles. It is home to more than ten million people and employs more than four million persons.

The GCM Corridor offers the opportunity to support USDOT ITS operational test and to provide a testbed for long-term research and evaluation of ITS. As part of the effort, a twenty year Corridor Program Plan has been developed. This Plan outlines a vision for ITS applications and the creation of a state-of-the-art testbed.

2.6.3 Regional Hubs

The Corridor Architecture is based on the idea that each region or state within the Corridor will have its own “hub” for collecting traveler data. These regional hubs will be responsible for processing any data they receive from their sources. The regional hubs will then be connected with the Gateway which in turn will do any minor processing of the data necessary and

redistribute the information back to the regional hubs. The Gateway will receive only traffic related data for the National Highway System (NHS) roads, Strategic Regional Arterials (SRA) and major arterials within the Corridor, as well as other transportation related data for transit, rail, ports, airports and other related transportation information within the Corridor. It is foreseen that there will be an added Transit Hub in the Illinois region to specifically handle Northeast Illinois transit data (including: CTA, Pace, Metra, Amtrak and the RTA). The Gateway will function as the overall "Corridor Hub" to connect the regional hubs in the three states to allow sharing of information as well as control and monitoring of field devices. There shall be no planned connections to the Gateway from other sources in Illinois, Indiana, or Wisconsin except through the appropriate regional hub.

2.6.4 Gateway

As stated in the above section, the Gateway will function as an overall "Corridor Hub" uniting information throughout the GCM Corridor. The Gateway will host the Corridor MMTIS server and supporting systems. The Gateway will dispense Corridor wide data to ITS subsystems within the Corridor, to regional ISPs, and to the general public.

The Gateway system will be initially located in Illinois and will be combined with the Illinois regional hub system. Though their responsibilities are logically different, these two systems can be implemented in the same local area network and can share physical servers for their processing.

The Gateway and Illinois regional hub system will consist of a range of communication and networking devices (switches, routers, modems, etc.) for communicating with the other regional hubs, the Illinois ITS subsystem data sources, ISPs, the media, and the Internet; 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.

The Gateway and Illinois regional hub system will be configured into a Local Area Network (LAN). This network will be referred to as the Gateway LAN.

The system will be designed with the ability to separate the Gateway and the Illinois regional hub at some future date by purchasing additional equipment. The Gateway and Illinois Hub computer programs will make no assumptions regarding the collocation of the Gateway and Illinois regional hub systems.

2.6.5 GCM DATA PIPE

Part of the Gateway design is to support the concept of a Corridor wide electronic communication network for sharing data — the GCM Data Pipe. The networking component of the Gateway (linking the Gateway, the regional hubs, and ITS systems within the corridor) is part of the GCM Data Pipe. This data pipe will be a Corridor Wide Area Network (WAN). Systems on the Data Pipe will use common networking protocols (compliant with NTCIP) and common intercomputer (and interprocess) communications.

2.7 DATA PROVIDERS

The following is a list of client ITS system which can provide relevant data to the Gateway TIS. ITS subsystems in the first section are anticipated to participate in the Initial Gateway TIS phase. ITS subsystems in the second list will be incorporated during the Ultimate Gateway TIS phase. Details regarding the interface between the Gateway and regional hubs and each ITS subsystem can be found in Document #17350 (*Gateway Interface Control Requirements*).

Initial phase data providers include:

1. Illinois Department of Transportation Traffic Systems Center (electronic connection)
2. Illinois Department of Transportation Communication Center (fax initially, then electronic connection)
3. Illinois State Toll Highway Authority (ISTHA) - IPASS (electronic connection) and Construction/Maintenance data (fax initially, then electronic connection)
4. Chicago Department of Transportation (CDOT) - Construction/Maintenance data (fax initially, then electronic connection)
5. Illinois State Police - District 15 (electronic connection)
6. Northwest Central Dispatch (NWCD) (electronic connection)
7. *999 (electronic connection)
8. Chicago Transit Authority (electronic connection)
9. Pace (electronic connection)
10. Metra (electronic connection)
11. Indiana Department of Transportation Borman ATMS (including Hoosier Helpers) (fax and pagers initially, then electronic connection)
12. Indiana Tollroad Traffic Management Center (fax initially, then electronically through the Borman ATMS)
13. Wisconsin Department of Transportation MONITOR System (electronic connection)
14. Weather (electronic connection)

Ultimate phase data providers include (Note: these connections are presumed to be electronic) the above plus:

1. CDOT - Traffic signal systems
2. Illinois Department of Transportation Traffic Signal Systems
3. Chicago Skyway
4. Illinois State Police - District Chicago
5. Chicago 911
6. *11
7. Indiana State Police
8. Gary Public Transportation Corporation
9. Indiana Department of Transportation Traffic Signal Systems
10. Milwaukee County Transit
11. Milwaukee County Sheriff Dispatch
12. Wisconsin Department of Transportation Traffic Signal Systems
13. DuCom

Additional ITS subsystems and agencies shall be connected during the ultimate phase as they are identified. These can include:

1. Other State and Local Police Departments
2. Other Corridor Traffic Signal Systems
3. Airports
4. Local Water Ports
5. Other Transit Systems

3. SYSTEM REQUIREMENTS

This section provides the functional decomposition of the Gateway system. Various subsystems within the Gateway are identified and their tasks are detailed. Functional requirements associated with the various subsystems are presented.

While this section presents Gateway subsystems, the Illinois regional hub design will also include the same subsystems.

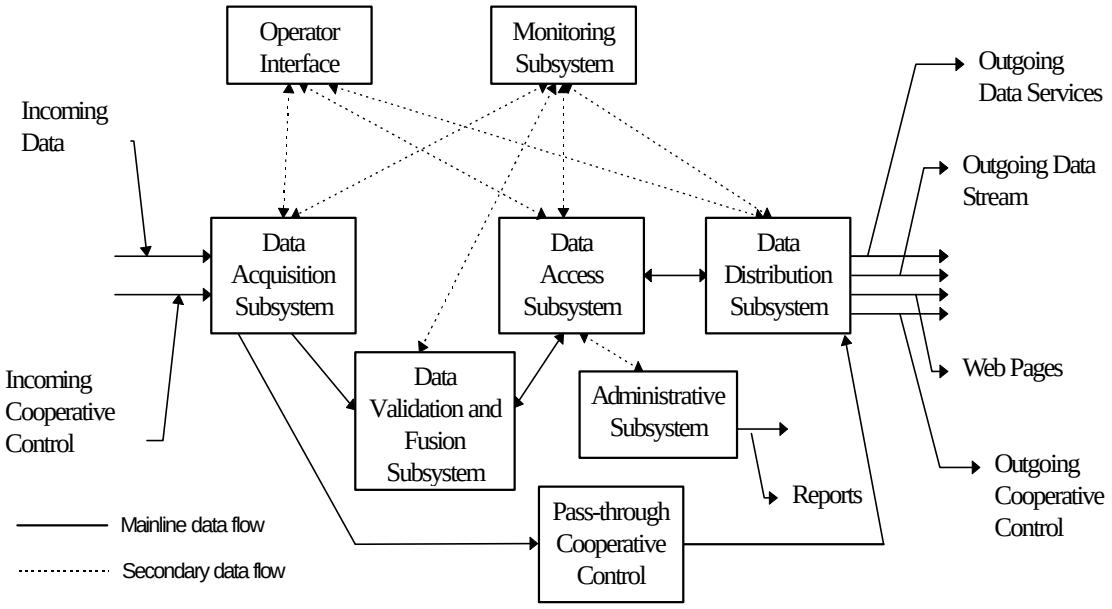

Figure 3-1 - Gateway High Level Module Diagram

3.1 DATA ACQUISITION SUBSYSTEM

3.1.1.1.1 The data acquisition subsystem shall accept data from incoming data streams. For the regional hubs, this data shall come from connected ITS subsystems and from operator input. For the Gateway, this data shall come from the regional hubs and from operator input.

3.1.1.1.2 It shall provide the range of CORBA callable objects which allow regional hubs to send the Gateway at least their one minute periodic updates.

3.1.1.1.3 It shall receive inputs from the operator interface (e.g., an incident report entered by an operator on an GUI form).

3.1.1.1.4 It shall submit data to the validation/fusion subsystem.

3.1.1.1.5 All data coming into the Gateway or regional hub shall pass through this subsystem.

3.1.1.1.6 All data produced by this subsystem shall be in a standard data format (though not necessarily validated data).

3.1.1.1.7 The subsystem shall report all data formatting errors, communication errors, early communications termination, etc. to the monitoring subsystem for logging and report to the operator.

3.2 DATA VALIDATION AND FUSION SUBSYSTEM

3.2.1.1.1 The data validation and fusion subsystem shall perform all data integrity checking.

3.2.1.1.2 It shall receive new data only from the data acquisition subsystem.

3.2.1.1.3 It shall examine individual data values to see if they are the appropriate type and have reasonable values.

3.2.1.1.4 It shall check existing data values in the system (by calling the data access subsystem) to see if existing data corresponds to the new candidate data.

3.2.1.1.5 If there is correspondence with existing data, data fusion shall be performed to merge data values and recognize updates, clarifications, duplicate reports, confirming reports, conflicting reports, or data errors.

3.2.1.1.6 When data is validated, it is submitted to the data access subsystem for storage.

3.2.1.1.7 If data fusion occurred, the updates to existing data shall be communicated to the data access subsystem.

3.2.1.1.8 If data is invalid or cannot be fused, the details will be reported to the monitoring subsystem for logging and report to the operator.

3.2.1.1.9 Primary data validation and fusion shall occur in the regional hubs.

3.2.1.1.10 The fusion and validation system shall be implemented as a set of CORBA calls on the data objects which can be called by the acquisition system (or master scheduling program).

3.3 DATA ACCESS SUBSYSTEM

3.3.1.1.1 The data access subsystem shall interface with the permanent data store (database).

3.3.1.1.2 It shall provide all data storage and update services for the Gateway or regional hub.

3.3.1.1.3 It shall allow other subsystems to view an object oriented view of the data in the database (whether the database is relational or an object oriented database).

3.3.1.1.4 It shall support adding new object instances, updates of object attributes (through method calls), etc.

3.3.1.1.5 The access subsystem shall be implemented as a set of CORBA calls which provide access to the existing data schema and data values within the data store.

3.3.1.1.6 All access to the data in the data store shall be through this subsystem, except for direct data queries and reports performed by Gateway or regional hub operators using the appropriate database management tools associated with the database used to store the Corridor data.

3.4 DATA DISTRIBUTION SUBSYSTEM

3.4.1.1.1 The data distribution subsystem shall compose outgoing data streams, reports and the Gateway web pages.

3.4.1.1.2 The subsystem will be located on several systems: the Internet server, the ISP server, and the main distribution server.

3.4.1.1.3 Values will be exported using CORBA (for ISP and for main distribution) and using web technology (for the Internet).

3.4.1.1.4 Web pages, reports, and the outgoing data stream will be composed by communicating with the data access subsystem.

3.4.1.1.5 The data distribution subsystem shall also support Corridor data services (requests for particular data values). These services shall utilize the data access subsystem to provide values.

3.4.1.1.6 For the regional hubs, the data distribution subsystem shall provide the data stream and the data service components.

3.5 MONITORING SUBSYSTEM

3.5.1.1.1 The monitoring subsystem shall monitor the execution of processes and devices within the Gateway or regional hub and produce logs of their status and error information.

3.5.1.1.2 Any error information shall be provided to the operators as they occur with both an audio and visual alert.

3.5.1.1.3 The monitoring subsystem shall monitor and log the actions of all Gateway or regional hub operators.

3.5.1.1.4 It shall monitor the status of incoming and outgoing connections and report problems with both an audio and visual alert.

3.5.1.1.5 It shall monitor the status of system resources and provide indications in the form of audio and visual alerts when resources are becoming scarce.

3.5.1.1.6 The monitoring subsystem shall alert the operator when intervention is necessary.

3.5.1.1.7 The monitoring subsystem for the regional hubs shall alert the Gateway when system failures are detected.

3.6 ADMINISTRATIVE SUBSYSTEM

3.6.1.1.1 The administrative subsystem shall provide user identification and permissions information for the processes in the Gateway.

3.6.1.1.2 The administrative subsystem shall compose system usage and error reports.

3.6.1.1.3 It shall provide for CORBA service controls and configuration.

3.6.1.1.4 It shall provide for SNMP administration.

3.6.1.1.5 It shall provide for TCP/IP administration and DNS (Domain Name Service) operation.

3.6.1.1.6 It shall provide e-mail services.

3.6.1.1.7 It shall allow systems to be started, stopped, or paused in operation.

3.6.1.1.8 It shall maintain administrative logs.

3.6.1.1.9 All user access permission functions shall be routed through this subsystem. The CORBA security services shall be used to maintain and serve permissions information within the regional hub or Gateway.

3.7 OPERATOR INTERFACE

3.7.1.1.1 The operator interface subsystem shall provide the Graphical User Interface and interface between the user and the other subsystems.

3.7.1.1.2 It shall provide all necessary operator interaction with the data acquisition system (to provide anecdotal and other data provided to the operators), with the data access system (for queries), with the dissemination system (for the web pages and reports), and with the monitoring subsystem and administrative subsystem (for system status information and administrative activity).

3.7.1.1.3 It shall display system status at all times on the operator console.

3.7.1.1.4 The graphical displays shall use color to the maximum extent possible.

3.7.1.1.5 User commands and responses shall be in accepted traffic engineering or other non-specialist terms that can be readily comprehended by a trained operator and shall not be cryptic.

3.7.1.1.6 All user inputs which affect system operation (e.g., changing a parameter, stopping a process, etc.) shall be adequately protected from operator errors.

3.7.1.1.7 The Gateway or regional hub shall provide for multi-user capability, whereby different users can interact with the system by means of the GUI simultaneously from different workstations.

3.7.1.1.8 The workstations shall have full and complete access to the application software and the operating system software dependent only on the access level of the user logged on.

3.7.1.1.9 There are two (2) means by which the user can request actions to be taken by the system:

- Operator request. Operator requests shall take place immediately and shall have priority over activity scheduler. Operator requests include standard reports, map displays, data inputs, and data modification.
- Activity scheduler. Operator generated requests which are scheduled for completion by time of day and day of week. Examples includes: reports, tape backups, file and log maintenance, etc.

3.7.1.1.10 The user interface shall be capable of providing the ability to:

- display data in real time including the ability to display color coded congestion maps and tabular reports,
- manually enter data and to modify anecdotal and incident data received electronically from other sources where needed,
- monitor accuracy and efficiency of all processes on a system including the receipt and transmittal of data,

- list and/or print all system database and system monitoring information,
- maintain a record of actions by the operator in the form of a time sequential log including the details of the input commands and data,
- provide statistical information on system operations and run simple queries,
- provide for user configurable reports,
- allow for reports to be printed at scheduled times,
- be seamless to the operator when accessing various menus, reports and status's,
- display a visual alarm and an audible alarm when a process has failed or has experienced an unusual condition,
- maintain and display process status lights, or other means, which provide a way of identifying the occurrence of a processing error condition or when a process has failed including both the operation of the process and data flows into and out of the process.

3.7.1.1.11 The operator shall be able to display a corridor map showing at least all roadways involved in the GCM Corridor data collection. In general, these roads include all NHS/SRA roads in the GCM Corridor.

3.7.1.1.12 The corridor map shall display icons which represent incidents, road closures, lane closures, CCTV cameras, VMS displays, ramp meters, loop detectors, weather sensors/conditions, which are either manually or automatically entered.

3.7.1.1.13 The corridor map shall be able to display the entire corridor area on one screen and selectively show underlying information with the use of layering.

3.7.1.1.14 The corridor map shall allow for quick zooming and scrolling.

3.7.1.1.15 The entire corridor area map shall be decomposable at least to a regional area; i.e., to a Gary, Chicago, or Milwaukee level. Additional zooming and scrolling capability shall be provided within the regional area map display.

3.7.1.1.16 The corridor map shall be able to display with user settable parameters including road levels, road colors and road names.

3.7.1.1.17 The corridor map shall be able to display state and jurisdictional boundaries.

3.7.1.1.18 The corridor map shall provide a display showing the location of all traveler information and collection devices and distribution sources including: detectors, sensors and field devices and TMC locations, appropriately labeled with their names.

3.7.1.1.19 The corridor map shall provide underlying details for a given icon by clicking on that icon.

3.7.1.1.20 Through the corridor map, the operator shall be able to manually input incident data using the map display and a menu, including the ability, where needed, to modify data received electronically or previously entered.

3.7.1.1.21 The Gateway and regional hubs shall be capable of displaying data in the GUI in real-time as it arrives.

3.7.1.1.22 Monitoring of events and graphical displays shall be updated automatically at the data receipt rate when being viewed by the operator; i.e. the operator should not have to perform a display 'refresh' in order to view the latest data received.

3.7.1.1.23 The operator shall be capable of displaying statistics on all traveler information gathered, by either pre-defined or user settable reports.

3.7.1.1.24 Data entry shall be constructed so that it minimizes the operator's use of keystrokes, mouse clicks, and time by adhering to the following data entry requirements:

- the operator can enter a minimum number of keystrokes in order to access a function,
- the operator shall not be required to memorize any commands,
- on-line help shall be available for all features,
- the primary input device shall be the mouse,
- the secondary input device shall be the keyboard using hot keys.

3.7.1.1.25 The operator interface shall incorporate consistency checks into the data entry process. This would check for interrelationships between entry fields and limit entries based on programmed instructions (limitations) and data type and range checking where appropriate.

3.7.1.1.26 The operator interface shall meet the following performance requirements:

- ability to present desired screen, window or process no later than five (5) seconds after the request is made at least 95% of the time,
- ability to begin printing a desired, predefined report no later than ten (10) seconds after the request is made, assuming an empty print queue,
- ability to scroll the map screen in a smooth manner without the need for excessive screen refresh.
- operator usage shall not affect the ability of other operators to perform their functions.

3.8 COOPERATIVE CONTROL PASS THROUGH

3.8.1.1.1 This subsystem shall pass through the Gateway or regional hub any cooperative control message from one ITS subsystem to another.

3.9 OPERATION

3.9.1.1.1 The Gateway and regional hubs shall be designed to operate in an unattended mode to the extent possible.

3.9.1.1.2 The Gateway and regional hubs shall be designed to continue operation in the event of the failure of any of its subsystems to the maximum extent possible.

3.9.1.1.3 The Gateway and regional hubs shall be staffed during regular business hours, but system design will not rely on operator involvement and regular staffing.

3.9.1.1.4 The Gateway and regional hubs shall provide for controlled shutdown and startup.

3.9.1.1.5 The Gateway and regional hubs shall include self diagnostic routines for determining errors or system parameters which are near tolerance.

3.9.1.1.6 Shutdown of the Gateway or regional hub system shall be performable in 10 minutes or less.

3.9.1.1.7 Startup of the Gateway or regional hub system shall be performable in 10 minutes or less.

3.10 BACKUPS

3.10.1.1.1 The Gateway shall be able to perform backups of database tables and other files onto long term storage media both in a full backup mode and in an incremental backup mode.

3.10.1.1.2 Full backups shall be performable in less than four hours.

3.10.1.1.3 Incremental backups shall be performable in less than one hour.

3.10.1.1.4 Gateway operation shall be able to continue while backups are being performed. Backups shall not seriously affect the responsiveness of the Gateway.

3.10.1.1.5 An automated or operator initiated backup of the system shall be supported.

3.10.1.1.6 For automated backup, the system shall support archiving without operator intervention.

3.10.1.1.7 The system shall be capable of performing a backup of each physical disk to an appropriate media.

3.10.1.1.8 The system shall be capable of performing a database backup independently of a physical disk backup.

3.10.1.1.9 The backup process shall perform a backup media verification process in that the contents of the file on disk will be compared with the contents of the backup media and an operator alert will be generated for manual backups and a log file maintained for automatic backups.

3.11 DATA USERS

3.11.1.1.1 The Gateway and regional hubs shall distribute data back to the above ITS subsystems as needed. The Gateway will also provide data to the general public and to Information Service Providers (ISPs) within the Corridor.

3.11.1.1.2 The Gateway shall distribute data to the general public through the Internet. A series of Web pages shall be created by the Gateway for this purpose.

3.11.1.1.3 The Gateway and regional hubs shall distribute data to ITS subsystems within the Corridor through the Corridor Architecture infrastructure or through the Internet using a set of privileged Web pages.

3.11.1.1.4 The Gateway shall distribute data to ISPs through a dedicated ISP server as well as through the Internet using a (different) set of privileged Web pages.

3.11.1.1.5 It is also anticipated that a set of kiosks may be created throughout the Corridor. These kiosks shall be supported through the ISP server or through connections to the appropriate regional hub.

3.11.1.1.6 The other regional hubs (or ITS subsystems) within the Corridor are not prohibited from distributing data they collect directly as needed.

Additional information regarding the interfaces to users of the ITS data collected by the Gateway can be found in Document #17350 (*Gateway Interface Control Requirements*).

3.12 GCM CORRIDOR OBJECT MODEL

As part of the Gateway design, a Corridor wide object model shall be established which describes the real objects within the Corridor and additional conceptual objects which are manipulated by systems in the Corridor (these are often referred to as business objects).

3.12.1.1.1 The GCM Corridor Object Model (GCOM) shall be designed in cooperation with other ITS subsystems and agencies within the Corridor.

3.12.1.1.2 Data passing to and from the Gateway shall comply with the GCOM.

3.12.1.1.3 The use of the CORBA system shall be used to allow processes modeling GCOM objects to communicate.

3.12.1.1.4 The GCOM shall be designed to be compatible with the NTCIP.

3.13 DATA TYPES SUPPORTED

This section discusses the requirements for data types to be supported by the Gateway and the regional hubs. Additional requirements for the data types is contained in Document *#17350 (Gateway Interface Control Requirements*).

3.13.1 Detector Data

3.13.1.1.1 The Gateway and regional hubs shall be capable of receiving either processed or raw detector data for calculation of congestion information or other travel time data.

3.13.2 Travel Times

3.13.2.1.1 The Gateway and regional hubs shall be capable of receiving and processing calculated travel times for road segments within the Corridor.

3.13.3 Incidents

3.13.3.1.1 The Gateway and regional hubs shall be capable of receiving and processing incident data for traffic impacting incidents within the Corridor.

3.13.4 Construction/Maintenance Events

3.13.4.1.1 The Gateway and regional hubs shall be capable of receiving and processing data regarding scheduled construction or maintenance activities within the Corridor as well as emergency road closures and special events.

3.13.5 VMS

3.13.5.1.1 The Gateway and regional hubs shall be capable of receiving text messages and sign status of VMS within the Corridor.

3.13.6 Weather and Road Condition

3.13.6.1.1 The Gateway and regional hubs shall be capable of receiving data from SSI detectors in the Corridor regarding atmospheric and road surface conditions.

3.13.7 Traffic Signal Data

3.13.7.1.1 The Gateway and regional hubs shall be capable of receiving data regarding malfunctioning traffic signals along the national highway system/strategic regional arterials and other major arterials in the Corridor. Future provision shall be made for receiving other signal data such as: detector (travel time) data, signal timing and phase plans, etc.

3.13.8 Ramp Meters

3.13.8.1.1 The Gateway and regional hubs shall be capable of receiving ramp meter information. This information shall include location, status (on/off), and possibly metering rates of the ramp.

3.13.9 Transit Schedules and Transit Schedule Adherence

3.13.9.1.1 The Gateway and regional hubs shall be capable of providing links to appropriate transit provider information where data on transit schedules and real-time schedule adherence may be displayed.

3.13.10 Voice

3.13.10.1.1 The Gateway and regional hubs shall be capable of receiving and transmitting voice communications among the hubs. Additional requirements for voice formatting are detailed in Section 9 of this document.

3.13.11 Video

3.13.11.1.1 The Gateway and regional hubs shall be capable of receiving and transmitting video data among the hubs and to the Internet. Additional requirements for video formatting are detailed in Section 9 of this document.

3.13.12 Airport Data

3.13.12.1.1 The Gateway and regional hubs shall be capable of receiving information about airport operations such as schedules, schedule adherence, parking congestion, and traffic congestion within and around the airport.

3.13.12.2 Hazmat Data

3.13.12.2.1 The Gateway and regional hubs shall be capable of receiving information regarding the route of hazmat transportation through the Corridor in order to determine if a particular incident may involve hazmat.

3.14 TRANSFER TECHNIQUES SUPPORTED

3.14.1.1.1 The Gateway and Illinois regional hub system shall be capable of supporting these types of incoming data:

- fax reception, followed by operator entry into the system,

- fax received by computer program and automatically entered (or subject to operator verification),
- pager reception, followed by operator entry into the system,
- pager received by computer program and automatically entered (or subject to operator verification),
- e-mail, followed by operator entry into the system,
- e-mail analyzed by computer program and automatically entered (or subject to operator verification),
- other text reception (telephone, mail, pagers, anecdotal information), followed by operator entry into the system,
- serial data interface through standard modems,
- distributed video, and,
- networked connection communication through CORBA.

3.14.1.1.2 The preferred method for providing data to the Gateway and Illinois regional hub is networked electronic communications using CORBA. Other techniques may be supported; however, all connections should include a plan for moving to the preferred method of data sharing.

3.15 LOCATION REFERENCING REQUIREMENTS

3.15.1.1.1 A common method of referencing transportation links and nodes shall be used so that the data exchange between subsystems will be based upon an unambiguous reference to the same transportation links, ramps and intersections. The current application for this will be in the form of the Location Referencing Message Specification (LRMS).

3.15.1.1.2 The Gateway base LRMS will conform to the base GCM Datum once established.

3.15.1.1.3 The Gateway shall initially use the Geographic Coordinate Profile as the base profile. This profile consists of latitude/longitude/altitude and street name. The Gateway shall be able to handle all other location referencing profiles throughout the Corridor and translate into the Geographic Coordinate Profile. Other profiles the Gateway may support in the ultimate phase include:

- Address Profile
- Cross Streets Profile
- Grid Profile
- ISP-Vehicle Profile
- Linear Referencing Profile
- Point/Link ID Interface Profile
- Text Profile

3.15.1.1.4 Translation methods from a specific agency to the Gateway include:

- Hub interface systems at each specific agency, translating their locationing scheme to the base GCM LRMS standard.
- Regional hubs receiving their local information and performing the translation.
- Connected agencies adopting the base GCM LRMS.

3.15.1.1.5 The Gateway shall be able to work with data that is provided in any LRMS format and shall initially export data only in the base GCM LRMS.

3.15.1.1.6 Until all existing sources are modified to utilize the base GCM LRMS, it will be necessary to provide a translation for received data that is not base GCM LRMS compliant.

3.15.1.1.7 Database requirements identified in Section 6.5 apply to the Gateway LRMS database.

3.15.1.1.8 A separate database may be used for the Gateway Location Referencing System.

3.15.1.1.9 Wrapper objects (with CORBA bindings) shall be used to interact with the Gateway LRMS database. These wrapper objects shall export location information in the base GCM LRMS.

4. GENERAL REQUIREMENTS

This section presents general requirements which shall be followed in designing the Gateway hardware, software, and operational elements.

Where appropriate, these requirements also apply to the Illinois regional hub design and should also be followed in designing the various regional hubs.

4.1 NATIONAL STANDARDS COMPLIANCE

4.1.1.1.1 The Gateway system, hardware and software, shall conform to the published and approved National ITS Architecture requirements.

4.1.1.1.2 The Gateway system, hardware and software, shall conform to the published and approved National Transportation Communication ITS Protocol (NTCIP), IEEE and other national standard requirements where applicable.

4.2 OPEN SYSTEMS

The Gateway, including all system level software, hardware and networking, shall have an open systems architecture to ensure interoperability, interconnectivity, portability, and scaleability across various hardware platforms and networks (fostering vendor neutrality).

4.2.1.1.1 The system shall be compliant with established and mature open system characteristics (such as defined by X/Open, an international standards house):

- interconnectivity, or general networking ability to connect and seamlessly exchange information with other systems,
- interoperability, or the seamless access of distributed data across hardware and among software applications,
- vendor neutral, both hardware and software,
- portability, or the ability to move applications from one vendor's computer system (hardware and operating system) to another with minor or no modifications required,
- scaleability, or the ability to run applications without modification on larger or smaller computer systems.

4.2.1.1.2 By basing the Gateway on open system characteristics, the following system attributes shall be exhibited :

- integration of future technologies with existing or legacy systems,
- maintainability,
- modularity.

4.3 TOPOLOGY

4.3.1.1.1 The Gateway shall be capable of interfacing with the regional hubs and the regional hubs with their respective ITS subsystems. The nature of each interface shall be determined as a requirement as each system is identified and is ready for connectivity to the Gateway TIS and

defined in Document #17300 (*GCM Corridor Architecture Interface Control Requirements*) and Document #17350 (*Gateway Interface Control Requirements*).

4.3.1.1.2 A distributed 3-tier client/server architecture shall be used for the Gateway.

4.3.1.1.3 The client processes and the server processes do not need to be on the same physical machine, though it is acceptable if they are.

4.3.1.1.4 The Gateway and Illinois regional hub shall be designed with the ability to either be collocated on the same equipment or physically separated. The design shall allow for the systems to be combined or separated at a later date.

4.4 OBJECT ORIENTATION

4.4.1.1.1 Object oriented technology shall be used for designing, developing, and implementing the application software.

4.4.1.1.2 Object oriented technology shall be used for data modeling.

4.4.1.1.3 Distributed objects implemented through CORBA will be used for application to application interfaces.

4.4.1.1.4 CORBA Interface Definition Language (IDL) shall be used to define the application to application interfaces. IDL facilitates language independent development.

4.5 FLEXIBILITY

4.5.1.1.1 The software shall be flexible and shall allow for future additions. Flexibility is the ability to adapt the software for different environments and domains, while minimizing code changes and recompilation.

4.5.1.1.2 Flexibility is supported through parameterization (obtaining environmental parameters from input files, database, conditional compilation, etc.), data-driven approaches, and the use of object frameworks and proxies.

4.5.1.1.3 To the extent possible, the software shall be designed to be parameter driven and to obtain specific details regarding its operating environment and connections from input parameters, compilation parameters, parameter files, database entries, and from the CORBA trader or naming services. Global variables and shared memory shall be avoided to the extent possible.

4.5.1.1.4 Design shall allow new attributes and methods to be added to objects without requiring existing programs to be rewritten.

4.6 SCALEABILITY

4.6.1.1.1 The Gateway architecture (software and hardware) shall be scaleable; i.e. the architecture shall allow for the inclusion of additional resources (e.g., memory, disk space) and shall be able to take advantage of those resources. The architecture shall also allow for additional usage (e.g., more connections).

4.6.1.1.2 The most common measures of load are data size, transactions per second, and number of active users. The Gateway shall be designed to accommodate increases in these factors (by a factor of 3) by adding new resources.

4.7 ADAPTABILITY

4.7.1.1.1 The Gateway shall maintain its functionality while adapting to new and emerging ITS technologies.

4.7.1.1.2 The Gateway shall maintain its functionality while additional ITS subsystems are connected to the network.

4.8 SECURITY

4.8.1.1.1 The Gateway shall provide at least these two distinct areas of security:

- Access security, which dictates who gets into the system and how much of it they can use once they are in.
- Data security, which determines which data a user can reference and what they can do to it once they have access to it.

4.8.1.1.2 The system shall allow its security features to be maintained by administrative users.

4.8.1.1.3 Gateway communication links connecting the Gateway and regional hubs, as well as individual systems, shall be protected from unauthorized access by using one of the following:

- use of secure private, dedicated lines,
- password access for dial-up lines (modems),
- data encryption for public networks (such as the Internet).

4.8.1.1.4 The Gateway design shall allow for future security features.

4.8.1.1.5 Security for the Gateway shall include moving the implementation into the CORBA ORB itself using an OMG Security Service. The CORBA Security service will verify each object access against the assigned authorization of the user associated with the process making the CORBA requests.

4.8.1.1.6 C2 is a government security standard for operating systems that require users and applications be authenticated before gaining access to any operating system resource. To obtain C2 certification on a network, all clients must provide an authenticated user ID, all resources must be protected by access control lists, audit trails must be provided, and access rights must not be passed to other users that reuse the same items. The Gateway shall provide C2 compliance.

4.8.1.1.7 Some parts of the C2 standard may prove too restrictive. The Gateway and Illinois regional hub design phase shall determine to what extent all C2 requirements shall be implemented.

4.8.1.1.8 Data security within the Gateway shall be provided by the DBMS (Database Management System) and the CORBA security service.

4.8.1.1.9 Optionally, a Kerberos or other centralized user validation scheme may be used (in combination with CORBA security). In this case, the Gateway shall provide the centralized security access information.

4.8.1.1.10 The Gateway and regional hub LANs shall be secured through the use of firewalling. This shall be accomplished with the use of multiple firewall routers which can create various zones of accessibility, and an application (or I/O) server which can intercept and validate any requests coming into the Gateway or regional hub from the Corridor WAN or through other connections.

4.8.1.1.11 A similar scheme may be used by ITS subsystems to secure their own local networks.

4.9 RELIABILITY

4.9.1.1.1 The Gateway system shall provide safe, reliable and efficient control and monitoring operations under a full range of working conditions, continuously 24 hours per day, 7 days a week, 365 days a year including unattended operation for the life of the system, subject to having reasonable regular scheduled maintenance.

4.9.1.1.2 The system shall be designed to operate for 10 or more years.

4.9.1.1.3 Any data transferred to and from the Gateway shall incorporate error-checking methods to make sure that data is delivered correctly. If the data link does not provide error checking, then error checking shall be used to verify the data at the application layer.

4.9.1.1.4 Attended operation with a high level of user interaction will generally occur during normal weekday working hours. The system shall be capable of unattended operation including monitoring of the subsystems and providing event and status logging, at all times.

4.9.1.1.5 The Gateway system shall provide reasonable system operation without a full complement of system equipment (i.e., operate in a degraded mode or be able to perform its functions with the loss of some or several external interfaces to the extent practical).

4.9.1.1.6 In the event of degraded mode operation, the Gateway system shall provide alert and status messages to connected systems where possible.

4.10 FAULT DETECTION AND RECOVERABILITY

4.10.1.1.1 The Gateway and Illinois Hub shall be capable of identifying component or subsystem failure and erratic operation and localize the effect and source of the foregoing conditions.

4.10.1.1.2 Unrecoverable faults, or unusual system or equipment conditions, exhibited by any equipment in the Gateway shall be detected by system equipment and shall be automatically and safely terminated in an orderly manner to the extent possible. Examples of unrecoverable faults can include: CPU failure, unexpected CPU halt, memory failure, disk failure, other peripheral equipment failure and communications failure. Any such fault shall be logged and reported to the local operators and to the Gateway operators.

4.10.1.1.3 Upon return of power, Gateway equipment shall be capable of returning to operation automatically with little or no operator intervention required. This shall include the following: no file system operations (transactions) will be left incomplete and the structure of disk volumes

will remain intact without the need to run a disk repair utility, database operations shall be rolled-back to the time of failure.

4.10.1.1.4 Appropriate logs and operator indicators shall be provided to indicate faults, fault status, fault repair, and possible data loss which occurred during a system fault.

4.10.1.1.5 Under no circumstances shall the loss of any connection impact the remaining operations or efficiency of the Gateway.

4.11 PERFORMANCE

4.11.1.1.1 The Gateway shall be capable of receiving information and exchanging data among its external data interfaces with no frequent, continual, noticeable loss of system performance (such as: transfer speed, reliability, etc.).

4.12 ERROR DETECTION

4.12.1.1.1 The Gateway and regional hubs shall continuously monitor their component equipment and subsystems in order to determine if any errors exist in equipment operation, communication, or data integrity.

4.12.1.1.2 Any detected errors or out of tolerance conditions shall be logged and reported to the operators.

4.13 PRIVACY

4.13.1.1.1 The Gateway and regional hubs shall insure that no private information is made available to unauthorized recipients.

4.13.1.1.2 Data flows shall not provide any information to the Gateway which is not needed by the Gateway or the other Corridor members (i.e., strip private and sensitive information at the source). This can also be accomplished by the hub interface system.

4.13.1.1.3 The Gateway and regional hubs shall tag sensitive information which is needed by some Corridor members or by the Gateway, but should not be distributed to the general public or to any other particular group of users.

4.13.1.1.4 Appropriate encryption technology shall be used for any sensitive information which is passing through the Corridor WAN, the Gateway, the regional hubs, or across the Internet.

4.14 SUPPORT FOR FUTURE TECHNOLOGIES

4.14.1.1.1 The Gateway shall be capable of incorporating future ITS technologies as they are developed and have applicability to the GCM Corridor Architecture.

5. HARDWARE REQUIREMENTS

This section presents requirements for the hardware design and selection for the Gateway. Where appropriate, these requirements also apply to the Illinois regional hub.

The Gateway and the Illinois regional hub may be designed to operate on the same hardware in order to reduce costs and increase the interoperability between the Gateway and the Illinois regional hub. As a result, these requirements specify the extra capability necessary for that dual operation. Design for the other regional hubs may therefore require a slightly reduced set of requirements from those specified here.

5.1 PERFORMANCE

5.1.1.1.1 The Gateway system shall be capable of handling multiple operators (at least 5) simultaneously along with processing of incoming and outgoing information.

5.1.1.1.2 The system throughput shall be sufficient to completely process a set of periodic data before the next receipt of that data, even under peak load conditions.

5.1.1.1.3 The system throughput shall be sufficient to process all incoming sets of periodic data (existing and planned).

5.1.1.1.4 The system throughput shall be sufficient to process an estimated peak load of event-driven data elements without effecting the throughput for periodic activity or interface response time.

5.1.1.1.5 The system shall be able to update and deliver all its output information at least once per minute.

5.1.1.1.6 The system response time shall be sufficient to allow user interface activity to appear responsive (actions complete within 1 second for simple actions, within 5 seconds for complex actions).

5.1.1.1.7 The system shall be able to serve its web pages with response time equivalent to standard Internet practice.

5.1.1.1.8 To support future expansion, the system shall be designed to exceed its estimated peak performance requirements by at least a factor of 3.

5.2 RELIABILITY

5.2.1.1.1 The goal of the system components shall be to provide at least a 99% uptime (excepting scheduled maintenance). No components will be selected which have mean time between failures (MTBF) of less than two years.

5.2.1.1.2 The system shall provide continuous operation, 24 hours a day, 7 days a week.

5.2.1.1.3 The system shall support 99% availability and not require scheduled maintenance more than once per month.

5.2.1.1.4 The system shall be designed not to become unusable if any communications or network connection (or any combination) fails.

5.2.1.1.5 The components of the system shall provide visual indications whether they are in good operation or have had an error (e.g., indicator lights).

5.2.1.1.6 Components shall exhibit sturdy manufacture and be enclosed in protective cases.

5.2.1.1.7 Components shall be easily replaceable. They shall not be items of unique manufacture.

5.3 SAFETY

5.3.1.1.1 The components of the system and its installation and operating environment shall be organized for the safety of the operators, system engineers, and the general public.

5.3.1.1.2 Appropriate insulation shall exist to prevent accidental contact with electricity (even low voltage) and short circuits.

5.3.1.1.3 Appropriate warning labels shall indicate voltage areas and control switches which should not be accidentally contacted or pressed.

5.3.1.1.4 Cables shall be managed so as not to cause either a fire or tripping hazard.

5.3.1.1.5 Access to the system hardware will be controlled.

5.4 TESTING

5.4.1.1.1 The components of the system shall undergo an appropriate IDOT approved testing period of continuous operation wherein they will not exhibit any hardware errors.

5.5 SERVER MACHINES

5.5.1.1.1 The Gateway shall consist of one or more server machines.

5.5.1.1.2 The main server machine shall be a symmetric multiprocessor machine capable of being scaled to four or more processors. Use of a SMP (symmetric multiprocessing) machine allows for direct scaleability for the main processing and database operations.

5.5.1.1.3 The speed rating (SPECint95, SPECfp95) of the main server machine shall be at least SPECint95=8, SPECfp95=20.

5.5.1.1.4 The speed rating of additional servers shall be at least SPECint95=6, SPECfp95=16.

5.5.1.1.5 The main server (or servers) shall operate the database, perform data processing, create reports and web page content.

5.5.1.1.6 Additional server tasks may be off loaded to additional server machines. These tasks include:

- Process incoming communications (data acquisition).
- Provide outgoing communications (data distribution).
- Operating the web server.
- Executing monitoring and administration software.
- Automatic archiving and backups.

- Firewall and related security and network management tasks.

5.5.1.1.7 The web server and ISP server shall be separate machines.

5.5.1.1.8 Where possible, scaleable design shall be used in separating tasks among machines. Factors which are likely to grow linearly (e.g., the number of incoming communications) shall be supported by separate servers, where appropriate, so that additional machines can be brought in to handle increasing demand.

5.5.1.1.9 Additional machines may be single processor machines.

5.5.1.1.10 The server machines shall be common, commercially available systems which have a proven operational track record.

5.5.1.1.11 The server machines shall be easily replaced in the event of hardware failure.

5.5.1.1.12 Systems which are currently depreciated (discontinued or no longer supported) or scheduled for depreciation by their vendors shall not be used.

5.5.1.1.13 The servers shall be scaleable in terms of I/O connections, disk drive connections, peripheral connections, etc.

5.5.1.1.14 The servers shall be capable of operation (possibly in a degraded mode) in the event of component failure.

5.5.1.1.15 The servers shall contain sufficient memory to avoid frequent swapping and to handle peak load periods.

5.5.1.1.16 The server operating the database will have sufficient memory to handle the additional demand of that operation.

5.5.1.1.17 The servers memory capacity will initially provide 4 GB of main memory and be scaleable with the ability to provide 16 GB or more of main memory.

5.5.1.1.18 Access time for the memory will be within the boundaries common to the industry (at most 60ns).

5.5.1.1.19 Each server shall contain disk storage capable of storing their operating system, application software and associated libraries, and appropriate swap space for virtual paging activities. A minimum of 2GB of disk space will be available in each server for this system software in addition to storage designated for Gateway operations.

5.5.1.1.20 Gateway memory shall provide transparent error detection and correction for single bit errors.

5.6 SYSTEM COMPONENTS

5.6.1.1.1 The server shall use common, commercially available hardware components with proven track records.

5.6.1.1.2 Components shall be easily replaced.

5.6.1.1.3 Components which are currently depreciated or scheduled for depreciation by their vendors shall not be used.

5.6.1.1.4 Components shall, where appropriate, be manageable using SNMP (Simple Network Management Protocol).

5.6.1.1.5 The Gateway shall contain components that do not require a special environment such as temperature, humidity, and particulate controls; i.e., a "computer room" controlled environment. All components shall operate in an standard office environment.

5.6.1.1.6 The servers shall provide for SCSI peripherals.

5.6.1.1.7 Separate SCSI buses will be used for the main disk storage and any alternative peripherals such as tape drives, CD recorders, and communication equipment.

5.6.1.1.8 Servers will include consoles to be used for bootup and administrative purposes, and to display running status logs.

5.6.1.1.9 The servers may share the same console and keyboard using a simple cable switch or multiple consoles and keyboards may be used.

5.6.1.1.10 Servers shall include a CDROM drive and a floppy drive.

5.6.1.1.11 At least one server shall include tape backup equipment.

5.7 MAIN STORAGE

5.7.1.1.1 The system shall provide main data storage to hold the following:

- 48 hours of incoming congestion data
- 14 days of construction and maintenance event data
- 14 days of incident data
- The location database
- Administrative data and user databases
- System monitor and logging information

5.7.1.1.2 In addition to the above, the system shall have considerable excess capacity to handle unforeseen events and moderate growth. This excess shall be at least three times the initial needed capacity.

5.7.1.1.3 The data storage shall support a RAID (Redundant Array of Inexpensive Disks) system.

5.7.1.1.4 RAID will be used where appropriate to maintain uninterrupted service.

5.7.1.1.5 The data storage shall, where appropriate, be disk drives mounted in removable, swapable SCSI canisters. An enclosure shall be included which accepts the disk canisters. These hot swapable canisters can be swapped whenever a disk drive experiences an error. The drives and the enclosure shall support RAID operation.

5.7.1.1.6 Access time for the main storage drives shall be within the boundaries common to the industry (no more than 12ms).

5.7.1.1.7 Fast/Wide SCSI II shall be used.

5.7.1.1.8 Disk drives shall be checked for reliability during a testing period. Drives which exhibit any errors will be replaced.

5.7.1.1.9 The Gateway server operating system shall contain a logical volume manager. This allows the system administrator to create logical disks from all or parts of the physical disk domain which can reduce the effect of applications and the RDBMS disk contention as well as potentially reducing disk bottlenecks when writing trace files and report output.

5.7.1.1.10 The logical volume manager shall support disk striping by spreading the blocks of the logical disk across the physical disks in such a way that a random pattern of access to any of the data in the logical volume will generate an equal load on each disk.

5.7.1.1.11 Disk technology used for on-line storage shall support RAID technology. RAID technology is an enhancement of both data integrity and performance.

5.7.1.1.12 RAID controllers shall be capable of implementing disk mirroring, a process in which each write is made to two separate drives. This capability provides a degree of fault tolerant capability for enhancing data integrity.

5.8 OFF-LINE STORAGE

5.8.1.1.1 The system shall have the capacity to archive and backup data to magnetic tape (or comparable medium).

5.8.1.1.2 If a tape system is used, it shall be a high capacity system (e.g., a 20GB 8mm).

5.8.1.1.3 The backup system shall support data compression.

5.8.1.1.4 The system shall have the capacity to perform a backup in unattended mode.

5.8.1.1.5 The backup system capacity shall either be sufficient to hold the backup or the system shall provide an automatic tape loader or multi-tape peripheral or corresponding device.

5.9 LOCAL AREA NETWORK

5.9.1.1.1 The Gateway servers, workstations and printers shall be connected by a Local Area Network.

5.9.1.1.2 The LAN shall operate at speeds of at least 100Mbps or greater.

5.9.1.1.3 The LAN shall be a secure LAN. Firewall technology shall be utilized to prevent unauthorized access to the LAN from the Corridor WAN.

5.9.1.1.4 Design shall determine if a second LAN shall be used to route video data.

5.10 PRINTER

5.10.1.1.1 The Gateway LAN shall include a PostScript capable Laser printer which has its own LAN address.

5.10.1.1.2 The laser printer shall support 600x600 dpi resolution (or better) and provide support for letter paper size.

5.10.1.1.3 The laser printer shall provide at least 16 pages per minute printing speed.

5.10.1.1.4 The printer shall provide a TCP/IP connection.

5.10.1.1.5 The printer shall provide standard serial (RS232) and parallel (Centronix) connections.

5.11 WORKSTATION MACHINES

5.11.1.1.1 The Gateway shall include a number of operator workstation machines. The exact number will depend upon the number of operators staffing the Gateway and Illinois regional hub. There will be at least 2 operator workstations initially with support for 5 workstations and up to 10 operators.

5.11.1.1.2 Workstations shall be common, commercially available, PC based systems.

5.11.1.1.3 X windows emulation software shall be used to provide graphical display of administrative functions if the selected GUI is X windows compliant.

5.11.1.1.4 These machines shall provide high quality graphical displays.

5.11.1.1.5 Monitor sizes shall be at least 17” or greater and shall support 1280x1024 resolution and at least a .27 dot pitch.

5.11.1.1.6 Workstations shall at least be 200Mhz Pentium PC’s.

5.11.1.1.7 Workstations shall contain disk drives for holding operating system and display software and temporary storage. Minimum size shall be at least three times the amount needed for the complete operating system, GUI system, application software, and running swap space. Minimum size shall be at least 4 GB.

5.11.1.1.8 Workstations shall also provide sufficient memory for high performance operation. A minimum of 32MB, expandable to at least 64MB,of memory shall be used in each disk based workstation.

5.11.1.1.9 Should non-disk workstations be used, they should be supported (including their X windows software) from a separate disk based workstation and not from the main server.

5.11.1.1.10 Non-disk X terminals shall include the maximum amount of memory which can be included.

5.12 LARGE SCREEN DISPLAY SYSTEM

5.12.1.1.1 The need for (and requirements for) a large screen display system in the Gateway control room shall be determined during the Gateway design phase.

5.13 OPERATING ENVIRONMENT

5.13.1.1.1 Wherever possible, the components of the system shall be housed in standard equipment racks.

5.13.1.1.2 The equipment racks shall be equipped with rack fans.

5.13.1.1.3 Equipment shall be secured to the equipment rack wherever possible.

5.13.1.1.4 The equipment racks shall be secured to the floor.

5.13.1.1.5 Appropriate cable management practices shall be followed in cabling the components together (e.g., designated cable runs, removal of excess cable slack).

5.13.1.1.6 Unused cables shall not be left attached to the equipment or to the rack.

5.13.1.1.7 Cables shall be labeled and, where possible, color coded. This includes telco connections.

5.13.1.1.8 Cable lengths shall not exceed industry standards.

5.13.1.1.9 The system shall be housed in a standard office area; however, temperature, humidity, and dust will be controlled using appropriate air conditioning equipment.

5.13.1.1.10 Air conditioning shall operate 24 hours a day.

5.13.1.1.11 Filtered, fresh air shall be introduced into the air conditioner for comfort of the system operators.

5.13.1.1.12 Room lighting shall be dimmable and shall be oriented to prevent glare on workstation screens.

5.13.1.1.13 Sufficient lighting to identify room exits and walkways shall be provided as well as sufficient lighting for equipment maintenance and repair.

5.13.1.1.14 Non-static surfaces and carpeting shall be used.

5.13.1.1.15 A non-liquid based fire prevention system shall be used in the operating room.

5.13.1.1.16 Noise-reduction treatments shall be used.

5.13.1.1.17 Access to the operating room shall be limited, possibly through separate keys, access cards, or a combination lock system.

5.14 POWER

5.14.1.1.1 The system shall be powered by standard, commercially available power.

5.14.1.1.2 Wattage requirements of the selected system components shall be followed. Appropriate wiring shall be installed in the Gateway computer center if it is necessary.

5.14.1.1.3 An uninterruptable power supply (UPS) shall be part of the system to provide an orderly system shutdown in the event of commercial power interruption.

5.14.1.1.4 The UPS shall condition the incoming power.

5.14.1.1.5 The UPS shall have sufficient capacity to operate all parts of the system for one hour or more without incoming power.

5.14.1.1.6 The UPS shall support warning the servers or any operators logged on that power is going off to allow the servers to shutdown gracefully or the operator to perform a system shutdown.

5.14.1.1.7 The UPS shall be able to page an attendant in order to alert them that there is no line-power to the system.

5.15 STARTUP/SHUTDOWN

5.15.1.1.1 Power failure at the Gateway shall cause the system to automatically shut down in a recoverable fashion. Equipment will be connected to the UPS and will continue to operate up to the limit of the UPS and thereafter shut down in a recoverable fashion.

5.15.1.1.2 Upon return of power, the system shall automatically restart, perform necessary condition operations including recovering the system state at shutdown and recommence automatic operation. The recovery process shall automatically restart any Gateway devices which are necessary for reliable system operation.

5.15.1.1.3 The recovery process shall include the automatic re-connection of networked systems along with notifying the attached systems that the Gateway has returned to normal operation.

5.15.1.1.4 All systems shall be designed so that they may be started in any order without affecting the Gateway or regional hub operation.

5.15.1.1.5 Systems composing the Gateway or the regional hubs shall have a maximum shutdown and startup time not to exceed 10 minutes.

6. COMMERCIAL SOFTWARE

6.1 OVERALL REQUIREMENTS

6.1.1.1.1 The system shall make use of COTS (commercial off the shelf) products where possible.

6.2 OPERATING SYSTEM

6.2.1.1.1 The operating system used in the Gateway shall be one of the following operating systems:

- Various Unix implementations (Solaris, AIX, etc..)
- Microsoft Windows NT
- Microsoft Windows 95

6.2.1.1.2 If a Unix operating system is used, there shall be only one Unix variety used.

6.2.1.1.3 The operating system shall comply closely with POSIX standards.

6.2.1.1.4 Operating systems selected shall not be currently depreciated (discontinued or no longer supported by the vendor) or scheduled for depreciation by their vendors.

6.2.1.1.5 Newest versions of operating systems shall be used unless common opinion is that that newest version is unstable.

6.2.1.1.6 The main server operating system shall support the following characteristics:

- Preemptive multitasking
- Multi-user Support
- Optional C2 Security Level
- Virtual Memory
- Multiple process priorities
- Multithreading
- File system security

6.2.1.1.7 Any operating system selected shall operate using at least 32 bit memory addressing (for the most part, i.e., mixed addressing in Windows NT and 95 is acceptable because new code can be created in 32 bit mode).

6.2.1.1.8 The operating system selected must support the CORBA tools selected.

6.2.1.1.9 The system shall automatically support daylight savings time and standard time, the number of days in a month, century changes and leap years. It shall support the millennium change.

6.2.1.1.10 The Gateway server shall provide time services based on Greenwich Mean Time (GMT), including time synchronization, for all client workstations and processes.

6.2.1.1.11 Automatic procedures for monitoring and testing the operation of the server, all peripheral equipment, including modems and networking hardware/software shall be provided.

6.2.1.1.12 Monitoring and testing shall be conducted on a scheduled basis with the results, including corrective actions when a fault is found, identification of failed units or software, and reports of failures to be logged.

6.3 GRAPHICAL USER INTERFACE (GUI)

6.3.1.1.1 The system shall display its user interface using a standard graphical user interface package.

6.3.1.1.2 The GUI platform shall be one of the following:

- Browser based using HTML and Java
- X Windows (and extensions, such as COSE)
- Microsoft Win32

6.3.1.1.3 Standard “look and feel” practices shall be used in designing the operation of the GUI. These include windowing behavior, use of the mouse, standard icons and visual controls, etc.

6.4 NETWORKING SUPPORT

6.4.1.1.1 The Gateway shall perform network management using SNMP for the entire Gateway TIS. The Gateway shall be responsible for managing the routing parameters for the Corridor WAN.

6.4.1.1.2 The Gateway shall operate the master DNS (Domain Name Services) for the Corridor WAN.

6.4.1.1.3 The Gateway shall support a standard SMTP and POP3 based e-mail system for the Corridor WAN.

6.5 DATABASE

6.5.1.1.1 Depending upon the details of the design, the database component of the Gateway may either be a relational database with an object oriented front end or an object oriented database.

6.5.1.1.2 The database selected shall support the necessary transaction speed required by the incoming and outgoing data transaction requirements.

6.5.1.1.3 The database shall be scaleable (i.e., additional disk or memory shall increase database storage and throughput capabilities).

6.5.1.1.4 The database shall support and take advantage of operation on a symmetric multiprocessor (SMP) machine.

6.5.1.1.5 The database shall support the ability to coordinate data access among processes with data locking facilities.

6.5.1.1.6 The database shall support multiple, simultaneous transactions without corruption.

6.5.1.1.7 The database shall support extended transactions and shall not allow partial commits (i.e., will allow rollbacks of transactions).

6.5.1.1.8 The database shall support and take advantage of operation on a RAID storage unit.

6.5.1.1.9 The Gateway database architecture shall be capable of supporting a distributed data model including the following features:

- platform heterogeneity in that it shall perform transparent data management across different computing platforms;
- incorporate location independent data access; i.e., data items shall automatically be assigned unique identifiers which are independent of the data's physical location,
- support data migration or the ability to store and transparently migrate data across platforms.

6.5.1.1.10 The Gateway database architecture and DBMS shall be capable of supporting parallel queries and parallel servers.

6.5.1.1.11 The Gateway DBMS shall be capable of handling 10 operators accessing the database simultaneously without a significant perceived decrease in user response time.

6.5.1.1.12 The Gateway database architecture and DBMS shall be capable of supporting disk striping and RAID technologies.

6.5.1.1.13 The Gateway database shall have the ability to mirror a database and automatically switch to the backup database, if necessary. In the event of a disk failure, it shall be transparent and database transactions shall continue uninterrupted.

6.5.1.1.14 The DBMS shall maintain concurrency control or the ability to lock data to prevent inconsistent views of the data.

6.5.1.1.15 The system shall provide for the on-line addition of data volumes. This is the ability to add storage to the database without interruption of database transactions.

6.5.1.1.16 The DBMS shall provide for on-line space reclamation and reuse for the data which is no longer needed. The space that outdated data occupies shall be reclaimed and reused automatically for subsequent data storage.

6.6 RELATIONAL DATABASE REQUIREMENTS

6.6.1.1.1 Any relational database component of the Gateway shall be a common, commercially available, database management system.

6.6.1.1.2 The database shall be ODBC compliant.

6.6.1.1.3 It shall support the SQL2 standard and significant portions of the SQL3 standard.

6.7 OBJECT ORIENTED DATABASE REQUIREMENTS

6.7.1.1.1 Any object oriented database component of the Gateway shall be a common, commercially available, database management system.

6.7.1.1.2 The database shall support an independent query language based on the ODMG93 standard.

6.8 INTERPROCESS COMMUNICATION

6.8.1.1.1 Interprocess communication between Gateway developed programs shall exclusively use the CORBA standard.

6.8.1.1.2 An ORB server shall operate on each server machine.

6.8.1.1.3 Only the data access subsystem shall access data from the databases directly. All other subsystems shall use CORBA calls to the data access subsystem to obtain, add, delete, or modify data values.

6.8.1.1.4 If possible, a single vendor of CORBA software shall be used.

6.8.1.1.5 The system shall also support a range of CORBA Services including the following:

- Naming Service
- Event Service
- Security Service

6.8.1.1.6 The Naming (or the Trading) Service shall be used in designing the interfaces between systems in order to increase flexibility. Static object identifiers shall not be used, all object identifiers needed between internal subsystems and between the Gateway, regional hubs, and ITS subsystems shall be obtained through the Naming service.

6.8.1.1.7 The Event Service shall be used for appropriate event driven actions within the Gateway or regional hub programs.

6.8.1.1.8 The Security Service shall be used to insure the identity and authorizations of all transactions and requests within the system.

6.9 WEB SERVER

6.9.1.1.1 A COTS web server program shall be operated by the Gateway.

6.9.1.1.2 The web server machine shall be directly connected to the Internet.

6.9.1.1.3 An additional web server program shall be used to provide Intranet services for the Corridor.

6.9.1.1.4 The web server shall support the use of SSL (Secure Sockets Layer) data encryption.

6.9.1.1.5 The web server programs shall be operated on the Internet Server machine and the main processing machine.

6.9.1.1.6 The web server shall support “push” technology and the dynamic “war maps”.

6.10 PASS THROUGH

6.10.1.1.1 The system shall support the pass through of cooperative control messages between ITS subsystems for VMS and CCTV devices.

6.11 TESTING

6.11.1.1.1 All Gateway COTS software shall undergo a IDOT approved period of testing to determine if it meets Gateway functional and design requirements and implements its advertised features.

7. GATEWAY DEVELOPED SOFTWARE

7.1 IMPLEMENTATION LANGUAGE

7.1.1.1.1 The language selected for main implementation of the Gateway systems shall have the following characteristics:

- Proven capability
- Common usage
- Multiple compiler vendors
- Available maintenance support
- Support for object orientation
- Support for library creation
- Exception handling support
- Strong modularity

Examples of languages which fit these characteristics include (but are not limited to) C++ and Java.

7.2 IMPLEMENTATION MODEL

7.2.1.1.1 The Gateway system shall be implemented using the "layered" model. In this model, capabilities are built up in layers with the innermost layer being the hardware and the outermost being the application programs.

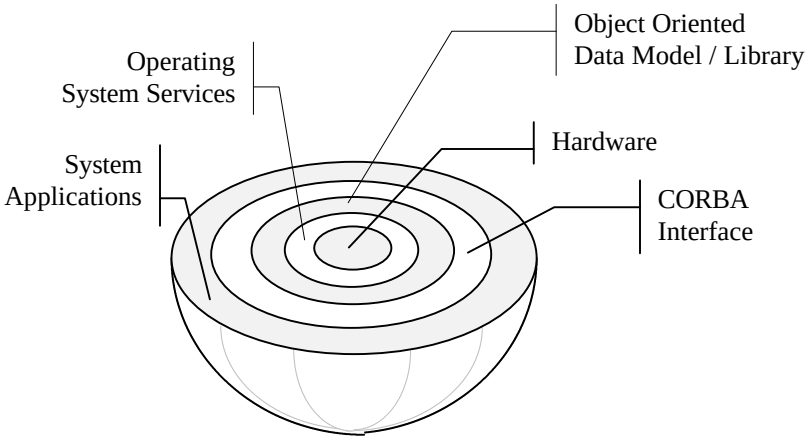

Figure 7-1 - Layered Model

7.2.1.1.2 Design of the system shall use object oriented strategies wherever possible.

7.2.1.1.3 A library of objects shall be created to support a range of applications within the system.

7.2.1.1.4 Data within the system shall be modeled using object oriented approaches.

7.3 SOFTWARE ENGINEERING REQUIREMENTS

7.3.1.1.1 Developed software shall follow characteristics of good software engineering. Many of these are called out in the General Requirements section (section 4) of this document.

7.3.1.1.2 The software shall be designed using exception handling techniques.

7.4 DESIGN PHASE REQUIREMENTS

The Gateway design shall produce the following system description documents:

- GCM Object Model and diagrams (using UML syntax)
- Database data model and diagrams (either standard entity-relationship diagrams or an object oriented variant)
- Gateway data flow diagram
- Illinois regional hub data flow diagram

7.5 TESTING

7.5.1.1.1 All Gateway developed software shall be thoroughly tested and subject to standard code reviews and analysis by independent analysts.

7.5.1.1.2 A series of tests shall be developed to ensure the operation of the Gateway under standard and extraordinary operating conditions.

7.5.1.1.3 Software shall be developed to simulate data overload, bad data formats, incorrect requests, etc. for purposes of testing the Gateway software and operation under these conditions.

7.5.1.1.4 Tests shall be made by taking various pieces of equipment or various communications links off-line to ensure the continued operation of the Gateway under these circumstances.

8. WEB INTERFACE

8.1.1.1.1 The Gateway shall support provision for a GCM Corridor home page and subsequent pages on the World Wide Web.

8.1.1.1.2 The Gateway Web Server shall support both public and protected Web pages with multiple area map displays showing traveler information as well as in textual format. There will be at least three sets of pages:

- Public pages
- ISP pages
- "war map" pages

8.1.1.1.3 Public pages shall be provided to the general public and shall not be password protected.

8.1.1.1.4 ISP page shall be provided to identified ISP organizations and broadcast media organizations. These pages shall provide more detailed information than provided to the public.

8.1.1.1.5 "War map" pages shall be provided to public agencies and emergency dispatch agencies within the Corridor. These pages shall provide all the information gathered by the Gateway and shall be operator selectable (i.e., the pages shall be layerable to show selective information).

8.1.1.1.6 The Gateway shall provide public web pages supporting standard HTML (with allowed CGI actions) and using GIF images. These pages shall include optional high or low resolution maps to support users with differing computer and modem speeds, specifically at least an IBM/IBM compatible 486 with 4 MB RAM and a 2400 bps modem. However, it is recommended that the user has at least a 9600 bps modem to decrease the download time.

8.1.1.1.7 The Gateway shall also include a more advanced and interactive set of public web pages using Java.

8.1.1.1.8 The basic web pages shall support a wide range of browsers. The appearance of the pages shall be checked on Netscape Navigator and Microsoft Internet Explorer browsers.

8.1.1.1.9 The Java based web pages shall support Netscape Navigator and Microsoft Internet Explorer. The appearance of the pages shall be checked on Netscape Navigator and Microsoft Internet Explorer browsers.

8.1.1.1.10 The GCM pages provided by the Gateway Web Server shall be available 24 hours per day, 7 days a week, 99% of the time from the server (not including outages based on Internet congestion).

8.1.1.1.11 The public page shall be capable of displaying the following information in both text and graphical formats:

- National Highway System (NHS) / Strategic Route Arterials (SRA) highways and road route numbers and common highway name,
- congestion data (indicated by color coded segments on the map),
- names of various cities and towns,
- incidents denoted by icon and general incident type,

- construction and maintenance information denoted by icon,
- travel times between major interchanges,
- a link to public transportation schedules and related information,
- VMS status and messages.

8.1.1.1.12 The private pages shall allow privileged users with password access, including separate connections for agencies to utilize the "war map" and different private media ISPs, access to additional features.

8.1.1.1.13 Private pages will show high resolution maps and will make use of Java or other approved equivalent to provide more interactive maps.

8.1.1.1.14 The ISP pages shall include the above plus the following:

- detailed incident type,
- incident duration.

8.1.1.1.15 The "war map" shall include the above plus the following:

- road surface conditions and atmospheric conditions for the corridor,
- any additional incident details,
- specific field device messages/status such as: ramp metering rates, signal timing plans, signal phasing plans, etc.

8.1.1.1.16 All GCM web pages shall be updated by the Gateway at least once every five minutes; however, an update frequency greater than this is desirable depending upon cost and technology available at the time of design and development.

9. COMMUNICATIONS REQUIREMENTS

The functional requirements of the communications system will be determined by the communications loading of the traveler information subsystems and the desired level of operation between the regional hubs and the Gateway.

Communications between the Illinois regional hub and Illinois ITS subsystems will be heavily dependent upon each application, many of which will be determined during the detailed design and implementation phase.

The communications can be classified into three types: data, video, and voice. Although the distinction between the three types is becoming less obvious with the push for integration, each type has unique characteristics that need to be addressed.

9.1 COMMUNICATION FUNCTIONS

9.1.1 VIDEO

Video by far is the most bandwidth intensive application, whether it is a closed circuit television camera monitoring traffic or a video conference session. The following functional requirements shall apply:

9.1.1.1.1 Each CCTV video signal input and output shall be compliant with National Television Standards Committee (NTSC) standards.

9.1.1.1.2 Each video signal input and output shall be a one volt peak-to-peak 75-ohm signal at a minimum bandwidth of 4.2 MHz with nominal 6 MHz channel spacing for full-motion analog video, as specified by NTSC standards.

9.1.1.1.3 Transmission quality of the video at full motion shall comply with Electronics Industry Association (EIA) standard, EIA RS-250C.

9.1.1.1.4 Full motion video shall be digitized and compressed using motion-JPEG or MPEG2 compression standards.

9.1.1.1.5 Motion-JPEG video shall be provided at compression data rates of at least 10 Mbps for normal full motion video viewing.

9.1.1.1.6 Motion-JPEG video shall be capable of operating over a range of 1.5 Mbps to 15 Mbps, via automatic and user initiated commands.

9.1.1.1.7 MPEG2 video shall be provided at compression data rates of at least 6 Mbps for normal full motion video viewing.

9.1.1.1.8 MPEG2 video shall be capable of operating over a range of 2 Mbps to 8 Mbps, via automatic and user initiated commands.

9.1.1.1.9 Video conferencing bandwidth shall range from 64 kbps to 1.544 Mbps, for each defined user.

9.1.2 VOICE

9.1.2.1.1 Voice communication shall be based around the North American Digital Hierarchy and the T-carrier standards.

9.1.2.1.2 A single voice channel shall occupy a 64 kbps slot (DS-0), one of 24 multiplexed slots within a DS-1 or T-1 carrier signal.

9.1.2.1.3 Voice channels shall be capable of transmitting a Group III and Group IV facsimile.

9.1.3 DATA

9.1.3.1.1 Data communications shall range from sub-rate 1200 bps to 155 Mbps and higher, dependent upon specific applications.

9.1.3.1.2 Links to interconnect local area networks or remote workstations shall be at 10Mbps, minimum, compliant with NTCIP protocol.

9.1.3.1.3 Local area networks shall be TCP/IP operating at a minimum bandwidth of 100Mbps.

9.1.3.1.4 Remote access shall be based on low speed links at 28.8 kbps to 64 kbps over PPP protocol.

9.2 GATEWAY REQUIREMENTS

9.2.1 Wide Area Network Requirements

9.2.1.1.1 The communications backbone, or wide area network, shall provide high speed communications between each regional hub and the Gateway.

9.2.1.1.2 The communications backbone shall be based on ATM (Asynchronous Transfer Mode).

9.2.1.1.3 The bandwidth between each regional hub and the Gateway shall be a DS3, 45 Mbps capacity channel, minimum.

9.2.1.1.4 The DS-3 to each regional hub may be leased, private, or hybrid.

9.2.1.1.5 Each regional hub shall have a capacity to transmit 4 full motion (30 frames per second) video channels in one direction, or 2 full motion video channels in two directions, minimum using current compression technology. In the future, improved compression algorithms or increased bandwidth may allow more channels to be transmitted.

9.2.1.1.6 The ATM backbone shall allow the bandwidth for the 4 full motion video channels to be reduced dynamically via network control to allow additional video channels at a reduced bandwidth to be viewed simultaneously, at a minimum bandwidth of 1.5 Mbps for each video.

9.2.1.1.7 Each regional hub shall be allocated a structured DS-1 for voice and fax communications.

9.2.1.1.8 The voice network shall be designed to route and/or switch voice/fax on demand between the hubs.

9.2.2 Local Area Network Requirements

9.2.2.1.1 The local area network for the Gateway shall be a network operating at a minimum of 100 Mbps.

9.2.2.1.2 The local area network shall be based on TCP/IP protocol.

9.2.2.1.3 The local area network shall be capable of displaying and routing full motion video through the network over ATM.

9.2.2.1.4 Each workstation shall be capable of displaying full motion video directly on the computer screen via direct ATM connection to each workstation.

9.2.2.1.5 Video over ATM on the workstation shall be processed through hardware decoders or video processor cards. Software decoding that relies on the workstation CPU for processing will not be permitted.

9.2.3 Internet Requirements

9.2.3.1.1 The Gateway shall be interconnected to the Internet at a minimum bandwidth of 1.5 Mbps.

9.2.3.1.2 Each video signal available at the Gateway shall be available for viewing over the Internet.

9.2.3.1.3 Video shall be available as a live, real-time video stream, capable of being viewed using commercially available Internet video software.

9.2.3.1.4 The Internet video shall be broadcast at a minimum frame rate of 10 frames per second, to a maximum of 30 frames per second, dependent upon the user link to the Internet.

9.2.3.1.5 The available video channels at the Gateway for Internet broadcast shall be equal to the number of channels coming in from each hub to the Gateway.

9.2.3.1.6 The Internet server or servers shall allow for individual digitization and compression of each available video signal at the Gateway, allowing simultaneous broadcast of all available channels over the Internet.

9.2.4 ISP Requirements

9.2.4.1.1 Each video signal available at the Gateway shall be available for viewing to the media via the Information Service Provider subsystem.

9.2.4.1.2 The communications from the Gateway ISP to any media outlet shall be provided and sized by each individual participant.

9.3 ILLINOIS REGIONAL HUB REQUIREMENTS

9.3.1 Wide Area Network

9.3.1.1.1 The communications backbone, or wide area network, shall provide high speed communications between the Illinois regional hub and select Illinois ITS subsystems.

9.3.1.1.2 The communications backbone shall be based on ATM.

9.3.1.1.3 The bandwidth between the Illinois regional hub and each Illinois ITS subsystem shall be designed based on the demand for each subsystem.

9.3.1.1.4 The communications between the Illinois regional hub and each ITS subsystem may be leased, private, or hybrid.

9.3.1.1.5 Each ITS subsystem requiring full motion video shall have a minimum capacity to transmit 4 full motion video channels in one direction, or 2 full motion video channels in two directions.

9.3.1.1.6 The ATM backbone shall allow the bandwidth for the 4 full motion video channels to be reduced dynamically via network control to allow additional video channels at a reduced bandwidth to be viewed simultaneously, at a minimum bandwidth of 1.5 Mbps for each video.

9.3.1.1.7 Each ITS subsystem shall be tied into the Gateway TIS voice network via local dial-up or dedicated access.

9.3.1.1.8 Video access at speeds lower than the specified Gateway requirements shall be via the Internet at speeds up to the capacity of the respective Internet link.

9.3.2 Local Area Network Requirements

9.3.2.1.1 The local area network for the Illinois regional hub shall be a network operating at a minimum of 100 Mbps.

9.3.2.1.2 The local area network shall be based on TCP/IP protocol.

9.3.2.1.3 The local area network shall be capable of displaying and routing the full motion video through the network over ATM.

9.3.2.1.4 Each workstation shall be capable of displaying full motion video directly on the computer screen via direct ATM connection to each workstation.

9.3.2.1.5 Video over ATM on the workstation shall be processed through hardware decoders or video processor cards. Software decoding that relies on the workstation CPU for processing will not be permitted.

9.3.3 Internet Requirements

9.3.3.1.1 No Internet access shall be provided directly from the Illinois regional hub. All information via the Internet shall be through the Gateway.

9.3.4 ISP Requirements

9.3.4.1.1 No ISP access shall be provided directly from the Illinois regional hub. All information via the ISP shall be through the Gateway through the ISP stand alone server.

10. ILLINOIS REGIONAL HUB

10.1.1.1.1 The Illinois regional hub shall serve as the intermediary between Illinois-based data sources and the Gateway.

10.1.1.1.2 The Illinois regional hub shall conform to the requirements in this document for the Gateway except:

- Disk storage and database storage requirements are lessened because the Illinois regional hub handles only Illinois data.
- The Illinois regional hub shall only distribute data to the Illinois ITS subsystems and shall not have an ISP or Internet server.
- The Illinois regional hub shall not operate a web server and shall not produce web pages.

10.1.1.1.3 The Illinois regional hub shall also conform to the following additional requirements:

- The Illinois regional hub shall support up to 10 operators and will be initially fielded with 3 workstations and support for up to 5 others..
- The Illinois regional hub shall use multiple communications techniques for sharing data (e-mail, fax, etc.) in addition to electronic communications.
- The Illinois regional hub shall support additional electronic communications options (where the Gateway shall only support ATM).
- The data acquisition subsystem shall perform a number of additional tasks:
    1. It shall provide the range of CORBA callable objects which allow Illinois data sources to send their data values (rather than from the hubs).
    2. It shall operate any modems or fax modems in the system.
    3. It shall analyze all e-mail and modem transmissions.
    4. It shall convert modem, e-mail, and such data to Gateway TIS standards including LRMS and GCOM.

11. ISP SERVER

11.1.1.1.1 The Gateway system shall include a separate ISP server to provide traveler information to Information Service Providers in the Corridor area.

11.1.1.1.2 The ISP server shall conform to the hardware and software requirements set out for the Gateway.

11.1.1.1.3 The ISP server shall support up to 120 connections.

11.1.1.1.4 It shall provide data to ISPs either through a scheduled update stream containing all information from the Gateway (the data stream) or through a set of CORBA object services which the ISP can query (the data server).

11.1.1.1.5 The ISP server shall not include information deemed sensitive (e.g., specific addresses of incidents).

11.1.1.1.6 The ISP server shall be firewalled off from the GCM Data Pipe.

11.1.1.1.7 Connections to the ISP server shall be through ATM and high speed lines (DS1 or greater).