CHAPTER 5

SYSTEM REQUIREMENTS

System requirements definition is an essential process in the development cycle of a system. The process produces a set of requirements defining in detail what the system has to perform and provide to meet its intended purpose. The requirements serve as a logical link between the system's goals and objectives and its design. Thus, to ensure an ability to trace this logic, system requirements must be derived from the system's goals and objectives.

The system requirements for the I-95 Corridor-wide Surveillance System were developed based on the results of the goals and objectives survey described in Chapter 2 of this report. The survey results imply that the Corridor-wide Surveillance System must perform the following top-level functions to support the multi-modal and intermodal transportation needs of the Corridor:

- Monitor traffic conditions, including incident.
- Monitor road weather conditions and their effects on driving conditions.
- Monitor air quality.
- Monitor road hazards.
- Monitor travel security.
- Monitor parking facilities.
- Monitor transportation law compliance.

To help define the detailed system requirements corresponding to these functions, an operational context of the surveillance system was formulated. This context was represented through the surveillance system's operational concepts and scenarios (refer to Sections 5.1 and 5.2). The operational concepts illustrate the surveillance system's ability to support the Coalition's desired ITS services while the operational scenarios provide a "visualization" of how the operational concepts are to be implemented.

The surveillance system needs identified by the survey, combined with the developed operational context, define the system requirements for the I-95 Corrfdor-wide Surveillance System. These requirements cover four major areas:

+ System-wide operational and performance requirements.
+ Functional requirements.
+ Communications requirements.
+ Interface, hardware, and software requirements.

The system-wide operational and performance requirements affect the overall system and are discussed in Section 5.3. The system functional requirements define what (not how) the surveillance system has to do to fulfill its objectives. A Computer-Aided Software Engineering (CASE) tool was employed to graphically represent the requirements model and to keep track of all functional relationships and their associated data. The functional requirements are described in Section 5.4.

To define the requirements for communications, interface, software, and hardware, a system hierarchical structure was defined. This structure is described in Section 5.5; Section 5.6 describes the communications and interface requirements; Section 5.7 describes the software requirements, and Section 5.8 describes the hardware requirements.

Knowing these technical system requirements, a framework establishing the surveillance operational responsibilities of participating Coalition member agencies was developed. This framework is summarized in Section 5.9. Finally, Section 5.10 summarizes and concludes the requirements definition process described in this Chapter.

5.1 OPERATIONAL CONCEPTS

The operational concepts define how the surveillance data will be utilized and shared among agencies, organizations, and jurisdictions within the I-95 Corridor Coalition (I-95 CC). They provide initial insight into the system requirements. In order to develop the operational concepts, it is necessary to address the Coalition's overall goals. As stated in the I-95 CC s Business Plan, the mission of the Coalition is a coordinated endeavor by the members to:

> "Work cooperatively to improve mobility, safety, environmental quality and efficiency of inter-regional travel in the Northeast through real-time communication and operational management of the transportation system. In doing so, the Coalition will seek to establish an economically beneficial, multi-modal framework for early implementation of appropriate IVHS technology."

Derived from the Coalition's stated mission, the ultimate goal of the SRT Project is to define the requirements and develop a conceptual design of a Corridor-wide surveillance and environmental monitoring system covering the Northeast I-95 Corridor from Virginia to Maine. This system is the cornerstone for implementing advanced and coordinated transportation management functions among Coalition members.

The system goals and objectives survey for this Project has identified eight candidate goals which are the premise for the operational concepts. These goals are:

- Enhance traffic incident management.
- Enhance real-time traffic control operations.
- Enhance traffic management during snow storms and other emergencies.
- Improve multi-modal and intermodal transportation operations.
- Support Traveler Information Services (TIS).
- Enhance the transportation systems planning database.
- Facilitate Travel Demand Management (TDM) strategy implementation.
- Support traffic law and regulation enforcement.

Each of these goals contains specific objectives which were identified and described in Chapter 2 of this report. These goals and objectives serve as the foundation for the surveillance system requirements. In order to logically connect the goals and objectives to the system requirements, operational concepts must be developed. The operational concepts show what the surveillance system should provide to fulfill the identified goals and objectives.

5.1 .1 Traffic Incident Management

Incident management systems use sensors, data processing, and communications capabilities to detect a variety of incidents, formulate a set of response actions to minimize the effects of these incidents on traffic, and support the initiation and ongoing coordination of response actions. In addition, the surveillance system may identify hazardous road conditions based on current or predicted weather, traffic, and facility conditions. While the ultimate beneficiary of traffic incident management is the traveling public, the traffic incident management system directly supports the emergency response teams and the responsible operating agency.

Typical surveillance data requirements for traffic incident management include incident location and time of occurrence, incident severity, roadway occupancy and volume, vehicle speed, travel times, origin-destination data, traffic signal data, and response vehicle locations. This surveillance data is utilized by the traffic incident management system to manage scheduled events and traffic incidents.

Scheduled events include activities such as construction and maintenance efforts, facility closures, and special events. Traffic incidents include occurrences such as traffic accidents, vehicle breakdowns, and loss of cargo situations. Some incidents may have only local impacts, others may produce area-wide effects. Therefore, early detection and verification of incidents is crucial for effective incident management. This is achieved by continuously monitoring the roadway using detection systems, integrating the data from various sources, and performing traffic data analysis to identify incidents and verify details regarding location, severity, and expected duration.

Agencies must cooperatively decide what actions will be taken and who is responsible for each action. A scheduled event and response should be scheduled well in advance and coordinated with all affected agencies. The best response to an unplanned incident can only be determined after the incident occurs. However, agencies must agree to response procedures in advance, especially for cross-jurisdictional events, to allow for a rapid and coordinated response.

The surveillance system should continuously collect, integrate, and evaluate data from many surveillance sources in order to identify possible incidents. Conditions corresponding to an incident can be detected by various electronic sensors that monitor traffic flow and environmental conditions. Computer-based incident detection algorithms may be used to monitor all incoming data for unusual conditions or reported incidents. The algorithms can only detect an incident when sufficient data is provided. Detected or reported incidents would be verified using either video or on-the-scene reports from officials. Notification of incidents may also come from several sources other than sensors, such as the police, fire department, National Weather Service, or from travelers themselves.

Integration and analysis of data from these different sources generally occurs at a single location, most likely a local traffic management center. The seamless flow of traffic information among inter-linking local traffic management centers will facilitate regional and Corridor-wide incident management.

Once an incident is confirmed, the severity of the incident is assessed to determine the best response. This includes which agencies, resources, and procedures to use. The response plan is developed based on the latest information on the status of the incident and of all potential responding agencies. Response plans for scheduled events are developed in advance, based on predicted traffic conditions and other scheduled incidents. In a fully developed incident management system, incident response plans are developed and implemented using a standard incident information and decision support system that links all potential responding agencies. This computerized system will integrate the communication, database, and data processing capabilities necessary for the incident management service.

When a recommended response plan has been generated, close coordination with the appropriate agencies is necessary to implement the plan. This requires an effective communication system to support the flow of information among all potential responding agencies and the traffic management center. Due to the dynamic nature of incidents and their impacts, ongoing contact among responding agencies must continue throughout the incident.

Since effective incident management requires a continuous and coordinated planning process, incident detection, verification, and response information should be stored for future use (e.g., for response plan improvement and training activities). In this regard, the surveillance system should provide its acquired information in the appropriate forms to ensure compatibility.

5.1.2 Real-Time Traffic Control Operations

The purpose of traffic control is to effectively and efficiently manage the movement of traffic on streets and highways. This includes controlling traffic flows to achieve specific objectives such as maximizing system throughput while minimizing traffic delays, energy use, and air quality impacts. Freeway control alternatives may include ramp and mainline metering, and lane use restriction. Street control alternatives may include techniques to optimize traffic signal operations at intersections, to restrict turning movements, or to enable reversible flow during peak periods. With advances in communications and control technologies, integrated control of freeways and street network signal systems becomes necessary to optimize traffic movement in the Corridor. In addition, integrated traffic control can significantly contribute to the people-carrying capacity of the roadway through preferential treatment for transit and other High Occupancy Vehicles (HOV).

Future signalization and ramp metering functions will have a real-time traffic adaptive control capability. These functions rely on real-time surveillance data to depict the operational conditions of a roadway network. In addition, through the use of historical traffic data and sophisticated prediction techniques, real-time traffic adaptive control systems can anticipate demand characteristics throughout the network to develop and implement optimal signalization and metering strategies. Although the traditional objectives for traffic signal control (such as delay and queue-length minimization) still exist, other objectives to minimize air pollution and emissions from vehicles or to maximize the flow of transit vehicles and HOVs will also be fulfilled.

To successfully support the implementation of these real-time traffic adaptive control strategies, the surveillance system should have the capability to provide accurate real-time data of traffic-flow (e.g., speed, volume, and density), traffic characteristics (e.g., queue-length, delay, traffic composition), and vehicle characteristics (e.g., vehicle type and occupancy). Furthermore, the surveillance system should have the capability to acquire data for developing traffic control strategies to improve air quality.

5.1.3 Traffic Management During Emergencies

Although the most common emergency situations in the Corridor are caused by snow, there are rare occasions where natural or man-made disasters would require evacuating the affected population. During such situations, inter-agency coordination at the regional level, and sometimes at the Corridor level, is necessary to maintain the operational status of the Corridor-wide highway network and to effectively manage the emergency.

To safely operate the roadway network during severe snow storms, coordinated planning and scheduling of snow removal operations are essential. Surveillance-related data to support the planning activities include predicted pavement conditions and road weather conditions, and current and historical traffic data. Offline analysis may be performed to prioritize snow removal operations along main routes and their associated alternate routes. Because multiple jurisdictions are usually affected by a snow storm, coordination of a snow removal schedule is also necessary to consistently maintain the inter-jurisdictional roadways.

Automated Vehicle Location (AVL) systems may be employed to track snow removal equipment. These would help to effectively dispatch resources to areas where sudden changes in snow accumulation occurs. The ability to track snow removal equipment should not be limited to one jurisdiction. Prior arrangement needs to be made to allow resources to be tracked within an inter-jurisdictional operating area.

The other side of snow emergency traffic management is the dissemination of road condition and advisory information to the traveler. The surveillance system should have the capability to monitor road conditions and traffic during snow storms to provide information to traveler information services and traffic incident management functions.

With respect to major emergency events requiring evacuation of the population, inter-jurisdictional coordination is necessary to identify evacuation routes and to control traffic along those routes. The surveillance information supporting these functions is similar to that for incident management planning. In addition, detection of road blockage due to pavement damage or debris (e.g., fallen trees) is essential for rerouting traffic.

5.1.4 Public Transportation Management

The Public Transportation Management operational concept includes the application of advanced vehicle electronic systems to various public transportation modes and uses the data generated by these modes to improve service to the public. Systems that enhance transit operations will contribute to the intermodal transportation goal of the Corridor. There are three categories that are relevant to surveillance functions:

+ Operation of Vehicles.
+ Planning and Scheduling.
+ Traveler Security.

In the Operation of Vehicles category, real-time vehicle location data is used to determine the schedule deviation status of a transit vehicle. If deviations are detected, a dispatcher is notified and plans to return the individual vehicle or fleet to the schedule are determined. For example, if a bus is ahead of schedule, the dispatcher may advise the driver to slow down to avoid "bunching of vehicles" at downstream stops. If a bus is behind schedule, signal priority requests may be activated to reduce the travel time or to take an alternate route if the downstream of the current route is heavily congested.

Transit vehicle operations may also be enhanced by sharing information with the traffic operations function. Traffic condition information for the transit route plays a major role in enabling real-time route diversion and in estimating vehicle arrival time at a transit stop. The availability of accurate arrival time information to the transit users is very important in attracting riders because it contributes to the reduction of wait time. The transit tracking data, on the other hand, may be used as probe data in traffic surveillance.

The Planning and Scheduling category includes the offline storage and analysis of transit data. These data include information on passenger loading, origin and destination along bus routes, bus running times, transit vehicle miles of travel, etc. The analysis of these data is performed periodically to revise and improve transit schedules and routes.

The Traveler Security operational concept incorporates surveillance data applications to improve the security of public transportation. Surveillance data includes the detection, identification, and notification of security incidents. Devices may be placed at transit stations, in parking lots, and at bus stops to monitor the surroundings and generate alarms. The alarm signals would be monitored by a central dispatch or local police. For in-vehicle security, drivers could be assisted by onboard silent alarms and connected microphones (or even CCTV) which allow central dispatch to monitor onboard incidents.

5.1.5 Traveler Information Services

Traveler Information Services (TIS) provide the traveler with access to information regarding a variety of travel-related services and facilities. The information will be accessible to the traveler in the home or office to support trip planning and while en-route, either in the vehicle or at pubic facilities, such as transit terminals or highway rest stops. In order to generate real-time traveler information, surveillance data must be analyzed and incorporated into the TIS system. Typical surveillance data requirements include traffic condition information, roadway condition information, and transit information.

TIS would provide the traveler, including the commercial vehicle operator, with Pre-Trip Traveler Information. Pre-Trip Traveler Information utilizes surveillance data to provide an overview of the roadway conditions at a particular moment in time along a chosen path. Pre-Trip Traveler Information also calculates travel times and provides mode choices for the traveler based on real-time travel conditions and parameter variables provided by the traveler. Time of departure, time of arrival, total travel time, maximum number of mode transfers, preferred routes and modes, intermediate stops, weather conditions, and other such information are included.

To provide travelers with a common information medium for all transportation modes, integration of intermodal information must occur. Traffic control systems generating data about highway conditions must be integrated with public transportation systems providing transit location and route information. Paratransit and ride matching systems must also be included. Integration of this service with electronic payment systems will allow travelers to pay transportation-related fees as part of the trip-planning process, and will also provide transportation pricing information that could affect mode choice and departure times.

5.1.6 Travel Demand Management

The goals of Travel Demand Management (TDM) are to reduce vehicle demands on the roadway by developing and encouraging travel modes other than the Single Occupancy Vehicle (SOV), to decrease congestion by altering the timing and/or location of a trip, or to eliminate a trip altogether.

Because of the growing problem of congestion and air pollution, many areas in the U.S. have already implemented TDM programs. Besides addressing environmental goals, TDM programs allow employers to better accommodate the needs and lifestyles of employees, improving their productivity and mobility choices through staggered work hour programs, compressed work weeks, and ride matching.

TDM can be achieved through the incorporation of three user services:

- Pre-Trip Traveler Information.
- Ride Matching and Reservation.
- Demand Management and Operations.

It should be noted that although the following paragraphs discuss the implementation of TDM through the use of ITS systems, non-ITS actions such as development of land use, zoning, and other transportation policies are crucial to deploying successful TDM strategies. The surveillance data collected with ITS technology will be useful for planning and implementing these strategies.

Pre-Trip Traveler Information, as previously discussed, is essential to TDM, providing the traveler with travel mode options and travel times. The service generates information from various transportation modes and presents it to the user through electronic communications or public information centers.

The Ride Matching and Reservation service is a key TDM strategy for reducing roadway vehicle demand by developing and encouraging ridesharing as an alternative form of travel. TDM goals are addressed by linking together all travel modes including bus, rail, air, vanpool, carpool, express bus, and specialized services. TDM must balance demand across all available modes and provide sufficient information to allow better route choice. The primary assumption for this service is that adequate transportation resources exist in the selected areas and across jurisdictions. These resources would provide the information infrastructure and market mechanisms needed to connect consumers with suitable providers. The system would offer users information on available transportation options through a single point of contact.

Through surveillance monitoring of traffic conditions, the Travel Demand and Operations portion of TDM generates and coordinates operational, management, and control strategies that will support and facilitate the implementation of programs, policies, and regulations designed to do the following:

+ Reduce SOV volumes.

+ Affect and increase the number of SOVs to HOVs for certain areas.

+ Provide a wide variety of mobility options for those who wish to travel at a different time or to a different location.

Once a program, policy, or regulation is established, specific implementation strategies are required. Specific TDM strategies are discussed in the following paragraphs.

+ HOV facility (lane, ramp, or parking lot) management and control. HOV lanes will be operated and enforced to respond to each jurisdiction's current conditions and situations. Occupancy requirements could be adjusted by the time of day or to reflect current demand and congestion levels, incidents, and enforcement criteria. For example, these requirements could be increased in response to pollution alerts or could be reduced in response to an incident on a parallel roadway. Preferential treatment at ramp-meters and signalized intersections for HOVs will result in reduction in travel time and make ridesharing more attractive to SOV drivers. However, special enforcement requirements will then become an issue for both of these operations.

+ Congestion/roadway pricing. Financial incentives and services for toll booths, parking areas, and HOV modes could be used to encourage mode changes and reduce vehicle demand. Additionally, congestion pricing could be used during peak hours in urban areas.

+ Parking management and control. The allocation, price, and availability of parking spaces can be managed and controlled to accomplish a mode change to HOVs. Working from a central point, fee collection equipment, variable message signs, and detection equipment could be used to respond to events by implementing TDM strategies by time of day or in a dynamic manner.

+ Mode change support This strategy will provide the public with greater flexibility when carpooling or using public transportation. For example, a traveler could ask to be included at a specific time in a carpool going to meet a train, and a central management center would find a carpool willing to carry an additional passenger.

+ Alternative work schedules. Alternative work schedules, such as compressed work weeks, provide viable and economically sound alternatives to driving to work during peak hours.

Surveillance data is required for TDM strategic planning in order to determine what the problem areas and linkages are, analyze what action should be taken, and track the impact of these plans once they are implemented. Examples of surveillance data requirements include air quality monitoring, traffic volume and flow, travel times, traffic conditions, origin-destination data, and transit vehicle tracking.

5.1.7 Traffic Law and Regulation Enforcement

The recommended objectives of traffic law and regulation enforcement, as stated in Chapter 2 of this report, are to provide commercial vehicle weight, height, and width measurements, determine vehicle occupancy for HOV regulation, and provide speed measurements. These objectives must be divided into commercial vehicle regulatory operational concepts and traffic law enforcement operations for privately owned vehicles.

Today, commercial vehicles are required to stop at check points where they undergo routine weight, credential, cargo, and safety checks. For lengthy trips, this means that the vehicles must stop and undergo similar checks several times. Electronic clearance would allow commercial vehicles, whether operating under interstate or intrastate registration, to continue past the check points without stopping. The information used for electronic clearance will need to include the following:

+ Weigh-in-Motion (WIM) data for weight compliance.

4 Motor carriers' safety fitness ratings.

+ Vehicle/driver inspection and maintenance data, including last date of inspection and out-of-service verification.

+ Credentials information, including annual registration, fuel use tax, operating authority, insurance, and oversize/overweight permits.

+ Cargo information, including Hazardous Materials (HAZMAT) listings and registration.

+ Driver information, including citation records and certification.

When a participating carrier with a transponder-equipped vehicle approaches a mobile or fixed checkpoint, it will cross a reader and WIM sensors upstream of the facility. The vehicle will be identified, classified, and weighed. Information will be sent, via communication link, to the checkpoint. Safe and legal vehicles will bypass the checkpoint. If any of the information warrants an inspection, the vehicle will be signaled to pull into the checkpoint. The system will then alert the official to the reason for inspection, so that the check will focus on the specific problem area. If the facility is closed or at capacity, the system will be overridden, and the vehicle will continue, uninterrupted. If the vehicle is stopped, the information will be updated in the system.

Utilizing ITS surveillance devices and data for law enforcement of privately owned vehicles must be considered very carefully to avoid the volatile subject of privacy infringement. To obtain public acceptance of ITS, the general public must be educated and made aware of the benefits that ITS can provide. The benefits to public safety, commerce, and the environment must not be jeopardized by the public perception that ITS equipment will be used against them. Monitoring HOV lane restrictions and vehicle speed are possible using police and human surveillance.

5.2 OPERATIONAL SCENARIOS

Surveillance needs have traditionally centered on collecting traffic information for detecting and mitigating the effects of incidents and recurring congestion. The I-95 CC, with its diverse members operating various transportation modes, presents a challenge and an opportunity to broaden the focus of a Corridor-wide surveillance system. Each transportation mode has its own information needs and capabilities to contribute to the Corridor-wide surveillance system. Thus, to properly develop and define functional and operational surveillance system requirements, it is essential to explore and understand the operational scenarios for which this system will be designed.

The intent of this section is to identify realistic operational scenarios which address the goals and objectives of the surveillance system. These operational scenarios will support the development of the conceptual design requirements and provide a reference for verifying the system's functional requirements.

In the following paragraphs, scenarios for various conditions are described. Data collection and dissemination needs for local, regional, and Corridor-wide surveillance are discussed based on each scenario. Visualized scenarios assure that the operational concepts reflect real-world limits and constraints. As recommended in the National ITS Program Plan, the first step in developing an ITS conceptual design is to summarize operational scenarios and concepts. This step allows for the verification and validation of the design requirements and enables the user to visualize how the end product will benefit them.

In order to develop these scenarios, certain assumptions were made. These assumptions are as follows:

- Specific surveillance devices are not defined in the scenarios (e.g., loop detectors versus microwave detectors), only the data which is required is defined.
- These scenarios do not address the existing surveillance technologies and communication systems currently deployed in each member's jurisdiction. Instead, they describe a basic operational scenario and how the situation is handled, so that the initial design requirements can be derived.
- These scenarios do not address surveillance gaps or communication system availability on the roadway or between jurisdictions. The conceptual design and deployment plan will address these issues.
- Local area surveillance is restricted to well-defined geographic areas, such as the sections of roadway within a city's limits.
- Regional area surveillance includes more than one member agency; that is, regional surveillance includes the coordination of more than one agency in an area to meet the Coalition's goals.
- Corridor-wide surveillance includes all member agencies.

+ A logical system information architecture for the local, regional, and Corridor-wide systems will be implemented within the Coalition (i.e., there are local, regional, and Corridor-wide Traffic Management Centers).

5.2.1 Roadway Incident

It is late afternoon on a weekday, and peak hour traffic is beginning to build up at a location on I-95. Operators at the local Traffic Management Center (TMC) are observing roadway conditions and watching for incidents using roadway vehicular data (i.e., volume, occupancy, and speed) collected by Vehicle Presence Detectors (VPD) and CCTV cameras. No incidents are currently active and all traffic control devices are set to their default settings (i.e., blank VMS, green lane use signs, ramp metering inactive, and speed limits posted to their maximum).

An inattentive driver collides with the panel truck ahead of him. This collision not only causes the driver injury, but the force of the collision causes both vehicles to come to rest blocking two travel lanes. The high volume of traffic quickly begins to queue behind the incident as drivers merge into the open lane. Unfortunately, due to the heavy congestion, three other vehicles collide while attempting to merge into the open lane. The only open lane is partially blocked. Roadway capacity is now less then 25 percent of its original capacity.

The VPD data quickly reflects the traffic changes on the roadway. An automatic incident detection algorithm interprets these changes in the TMC. As the incident is severe, the incident detection algorithm quickly identifies a potential location for the incident and sends an alarm to the TMC operators. One operator stops his manual incident detection activities and switches his attention to the incident alarm to perform confirmation.

The operator directs the nearest CCTV (as indicated by the alarm) toward the potential incident site. At the same time, a service patrol vehicle passes the incident while traveling in the opposite direction on the freeway. The service patrol driver informs her dispatch that there has been an incident. Since the patrol vehicle is equipped with a Global Positioning System (GPS), dispatch quickly determines the vehicle's rough location. The driver estimates that she will be able to arrive at the scene in five minutes. Meanwhile, the dispatch contacts the local police for their response. Additionally, the operator confirms that there is an incident based on the CCTV image and communications with the police dispatch. Closer examination of the incident site using the zoom capability of the CCTV camera reveals that one driver may be injured. Fortunately, the panel truck does not appear to be marked as a HAZMAT carrier.

The operator quickly assesses the incident in order to develop the incident response. He knows the location and the following characteristics:

- ♦ Multi-vehicle accident severely hindering traffic flow.
- ♦ Physical injury suspected.
- ♦ No HAZMAT vehicles are included.
- ♦ Roadway capacity is reduced to 25 percent of its normal capacity.
- ♦ Removal of the blockage is estimated at a minimum of 2 hours.

The Local TMC has a fixed response plan to deal with this situation (major incident during peak-hour):

- + Notify emergency response crews and vehicles.
- + Notify Emergency Medical Services (EMS) vehicles.
- + Adjust ramp metering rates.
- + Activate speed advisories.
- + Activate lane closures.
- + Communicate incident information to commercial radio, HAR, and VMSs.
- + Activate diversion advisories.

Due to the severe reduction in roadway capacity, it is determined that a coordinated regional response is required. Route diversion, travel information services, and coordinated removal plans are enacted in close coordination with the regional TMC.

The operator sends requests to activate the traffic control devices as required. He sends a request to an emergency response facility to dispatch a crew to the site. The nearest EMS vehicle to the site (determined by estimated travel time) is redirected from returning to its base. By this time, a police officer and the service patrol vehicle have arrived and verified that a driver is injured and that medical attention is required. At this point, the police officer takes control of the response activities at the site, leaving the operator to focus on the traffic device response activities.

All information available to the operator is recorded to assist with planning and future policy. This information includes incident details, response details, incident duration, and traffic data describing the impacts of both the incident and the response.

Local Surveillance Information Reauirements

Based on the scenario description, the following local surveillance information requirements must be satisfied to allow the operations to transpire as described:

- Speed, occupancy, and volume data for all highways, local arterials, and ramps for incident detection and traffic condition assessment.
- Emergency vehicle locations for allocating response vehicles and estimating origin-destination data and travel times.
- Control system status to verify that control commands are functioning properly, and to perform maintenance planning if a failure occurs.
- Video image and communications for incident confirmation and initial severity assessment.
- Communications with emergency units, both locally and regionally operated, for coordination, planning, and incident status tracking.
- On-site HAZMAT recognition for prompt HAZMAT clean-up and tracking.
- Response details for coordination across jurisdictions and for strategic planning.

Regional Area Surveillance Information Requirements

In most cases, the combination of estimated incident duration (i.e., between 2 and 4 hours), capacity restrictions, and time of day will affect other agency jurisdictions. That is, an incident response may include alternative route diversions onto roadways operated by a different agency, thereby affecting traffic in other jurisdictions. When a severe local disturbance may impact neighboring local jurisdictions, the following surveillance requirements exist:

+ Traffic flow data for highways, local arterials, and ramps for assessing traffic conditions on alternate routes and incident impact.

+ Emergency vehicle locations for allocating response vehicles and estimating origin-destination data and travel times.

+ Communications with emergency units for response tracking and route guidance.

+ Control system status to verify that control commands are functioning properly and for maintenance planning.

+ Response details for regional coordination and strategic planning.

Corridor-Wide Surveillance Information Requirements

Regional incidents do not require Corridor-wide responses; however, data detailing the impacts of both the incident and the response are useful to all members of the Coalition and allow historical information to be incorporated into the database for future planning and studies.

Other Corridor-related incidents might include major special events, HAZMAT events, severe weather, long-term construction operations, and major traffic re-routing for construction projects. Therefore, the following items represent general incident data requirements for the Corridor:

+ Estimated travel times and delays.

+ Traffic flow data on highways, local arterials, and ramps for historical data collection, database maintenance, and determination of alternate routes.

- + Weather sensors for collecting emergency weather data used to determine the necessity of roadway closure due to severe conditions and for regional weather incident coordination.

- + Response details for Corridor-wide incident coordination and strategic planning.

5.2.2 Recurring Congestion

During the morning peak hour, both directions of I-95 become quite congested near beltways of metropolitan areas. Since this recurring congestion is quite similar each day, the local and regional TMCs have developed a response strategy to optimally relieve the congestion. Historical traffic data has been analyzed to develop an integral set of control policies, including ramp metering to mitigate bottlenecking, TIS for congestion avoidance and route guidance, and park-and-ride lots and HOV lanes to encourage carpooling. Scheduled congestion relief plans also include utilization of reversible lane operations over bridges and in toll areas during peak hours. Unfortunately, the congestion does not start at the same time each day, nor does it exist with the same severity at all times. As a result, the operators in the TMC observe the congestion indicators manually (using CCTV images, system history, and operator experience) and automatically (i.e., with indicators developed from VPD data) to optimize the congestion relief plans.

Recurring congestion response plans involve the following planned activities during peak hours:

- + Provide real-time traffic adaptive signal control.

- + Monitor ramp metering rates.

- + Post speed advisories.

- + Disseminate congestion information (i.e., by commercial radio, HAR, and VMSs).

- + Post route diversion advisories.

As recurring congestion will impact neighboring local TMC operations, the plan is implemented with regional coordination in mind. For example, congestion detected in one local jurisdiction may require that certain components of the complete plan be implemented in more than one local jurisdiction.

Post implementation evaluations have shown the majority of these plans to be beneficial. Traffic flow data, travel time estimates, origin-destination data, and link travel times have been utilized in generating the Measure of Effectiveness (MOE) for evaluating the implemented policies. The overall effectiveness of these policies was not immediate; however, after several weeks, the TMCs did notice improvement. Notably, recurring congestion in the most severe areas declined rapidly once the full complement of these policies was implemented. Regular evaluation of these policies and traffic flow data is required for optimal effectiveness.

Local Surveillance Information Requirements

Control policies for mitigating recurring congestion involve the use of processed traffic data for planning purposes. The following surveillance data is required to implement recurring congestion operations:

- Speed, occupancy, and volume data for all highways, local arterials, and ramps to determine problem areas and to set ramp metering rates.
- Video image to confirm congestion and monitor the roadway.
- Travel time and origin-destination data.
- Traffic count data from discretely located traffic counting facilities for congestion planning.
- Traffic volumes and queues to set optimal traffic signal timing and characterize traffic demand levels.
- Response details for coordinating and evaluating effectiveness.
- Control system status to verify that control commands are functioning properly and to perform maintenance planning if a failure occurs.

Regional Area Surveillance Information Requirements

At the regional level, the generation of a response plan to mitigate recurring congestion requires coordination between neighboring agencies. As a result, coordinating the following surveillance requirements is necessary:

+ Speed, occupancy, and volume data for all highways, local arterials, and ramps to determine problem areas and to set ramp metering rates.
+ Travel time and origin-destination data.
+ Traffic count data from discretely located traffic counting facilities for congestion planning.
+ Traffic volumes and queues to characterize traffic demand levels.
+ Response details for coordinating and evaluating effectiveness.

Corridor-Wide Surveillance Information Requirements

Locally and regionally recurring congestion do not necessarily require Corridor-wide responses; however, data detailing the impacts of both the congestion and the response are useful to all members of the Coalition and are required for long-term TDM strategies. As a result, the following represent data requirements for the Corridor:

+ Speed, occupancy, and volume data for all highways, local arterials, and ramps to determine problem areas.
+ Travel time and origin-destination data.
+ Traffic count data from traffic discretely located counting facilities for congestion planning and formulating TDM strategies.
+ Traffic volumes and queues to characterize traffic demand levels.
+ Response details for coordinating and evaluating effectiveness.

5.2.3 Blizzard Emergency

A severe blizzard is about to hit the east coast of the U.S. It is expected to creep north and batter most of the coast. The National Weather Service is providing up-to-date tracking information to the I-95 TMCs. The TMCs, in conjunction with the National Weather Service, are attempting to predict where snow accumulation and ice will occur. All agencies are working together to determine how these conditions will impact the Corridor road network.

Traffic conditions, roadway surface conditions, and visibility will be monitored and responded to in the same manner as incidents and congested conditions. Regionally and locally, TMC staff are preparing for the anticipated traffic difficulties. Local jurisdictions are assessing their abilities to keep the Corridor roads operational while still maintaining local roads. It is determined that a coordinated response will be required. Neighboring jurisdictions will coordinate their snow-removal and de-icing operations to ensure that the Corridor roads are continuously usable throughout the affected areas. The TMC's planning includes the following tasks:

+ Identify critical routes for snow removal operations.
+ Use ATIS resources to inform the public of weather warnings and emergency routes.
+ Mobilize resources (e.g., crews and vehicles) to maintain operations.
+ Coordinate plowing schedules and routes.
+ Increase service patrol frequency on emergency routes.

During the storm, the prepared plan is implemented upon verification of actual conditions by TMC staff using road surface condition data, CCTV camera images, and weather information collected from the Corridor Coalition TMC.

TMC personnel coordinate snow removal and de-icing activities both as planned and on a real-time basis. Snow removal and de-icing vehicles are tracked using AVL technology, enabling the TMCs to track and dispatch resources quickly based on dynamic changes in road surface conditions. VMSs are used to warn drivers of the snow removal activities.

A coordinated data exchange of roadway status and incident information between adjacent jurisdictions is integral to the response. All activities and incidents will be recorded for future planning, analysis, and policy.

Local Surveillance Information Requirements

The following surveillance requirements will assist in emergency weather operations:

- Speed, occupancy, and volume data for all on highways, local arterials, and ramps to determine traffic flow, incidents, and congestion.
- Vehicle location data to determine removal rates for scheduling and resource tracking.
- Emergency vehicle locations for resource tracking.
- Communication with snow removal and emergency units for coordination and re-routing.
- Response details for coordination between jurisdictions.
- Road surface data to allocate resources and post travel advisories.

Regional Area Surveillance Information Requirements

Regionally, generation of a response plan for emergency weather conditions, such as snow removal, requires coordination between neighboring agencies. As a result, coordinating the following surveillance requirements is necessary:

- Traffic flow data for highways, local arterials, and ramps for traffic-coordinated snow removal and traffic monitoring.
- Vehicle location data to determine removal rates for scheduling and resource tracking.

+ Emergency vehicle locations for resource tracking and coordinating snow removal operations.

+ Communication with snow removal and emergency units for coordination and re-routing.

+ Response details for coordination between jurisdictions.

+ Road surface data to allocate resources and past travel advisories.

Corridor-Wide Surveillance Information Requirements

During an event that disrupts the entire Corridor, Corridor-wide coordinated surveillance and response is critical. For this reason, more real-time local and regional data must be made available at the Corridor-wide level. The following is a set of surveillance information requirements:

+ Origin-destination information, travel time estimates, and delay times.

+ Response details for coordinating and evaluating optimal responses.

+ Emergency vehicle locations for Corridor-wide coordination.

+ Traffic flow data.

+ Weather sensor information for roadway and surface conditions.

+ Response details for coordinated planning and database maintenance.

5.2.4 Intermodal Transportation

In the morning peak hour, local and regional TMC operators observe the congestion building up on the freeway. Suddenly, a major accident causes the freeway to be closed for an estimated period of 3 hours. If motorists do not utilize alternate modes, traffic congestion will spill over into neighboring jurisdictions, thereby paralyzing the highway network for the entire morning. Fortunately, the freeway parallels the commuter railway line.

As part of the TDM strategy to coordinate efforts for encouraging motorists to seek various modes of travel, the local Transit Authority has been supplying the TMC with schedule adherence information for congestion/intermodal support response planning. Because of this accident, the use of the existing intermodal transportation must be increased to relieve the anticipated traffic congestion.

This regional response involves activation of ATIS resources to make travelers aware of the opportunity to switch modes for their commute. Additionally, a coordinated response with the transit authorities is required to prepare for the increased transit demand. Specifically, this response includes the following:

- Provide equipped motorists with in-vehicle information explaining the accident and increased transit services available.
- Provide route guidance to vehicles equipped with navigational GPSs.
- Provide VMS messages on the freeway indicating a travel time differential and the significant savings available on transit.
- Disseminate travel advisory information to TIS.
- Display HAR messages, detailed Park-and-Ride status, and travel time comparisons.
- Update phone-in services and cable information sources.

The increased transit support, advanced warning of substantial delay times, and Park-and-Ride lot information prompt many drivers to use public transportation that morning. Drivers who choose to change modes while en-route, but who are not equipped with navigational GPS equipment, are provided with fixed signs guiding them to Park-and-Ride lots. Pre-trip traveler information provides travelers at home with parking lot and commuter rail locations. As a driver pulls up to a parking lot, sensors identify the vehicle automatically and deduct the parking fee from the drivers Corridor-wide traveler account. Variable message signs indicate open areas within the parking lot, and the driver parks the car and heads to the train station. The driver presents his intelligent transit pass, and the transit fee is deducted automatically from the passenger’s account.

From the platform, a large monitor depicting the rail system status graphically indicates that an approaching commuter train is only 10 minutes away and confirms the estimated travel time. The passenger relaxes, purchases a local newspaper, and enjoys the ride into town.

Local Surveillance Information Reauirements

The following surveillance information requirements will assist in intermodal operations:

- Speed, occupancy, and volume data for all highways, local arterials, and ramps for incident detection, traffic flow, congestion level, and alternate routing determination.
- Transit schedule and travel time.
- Control system status to verify that all commands are functioning properly.
- Video image at transit locations and parking lots for traveler security.
- Communication with transit operations for route guidance allowing for schedule adherence and coordination.
- Vehicle entrance/exit data for parking lot monitoring and availability information.
- AVI data in transit vehicles for signal priority.
- Passenger loading information for resource allocation.
- Response details for planning and coordination.

Regional Area Surveillance Information Requirements

Regionally, generation of a response plan to encourage motorists to alter their travel mode requires coordination between neighboring agencies and transit authorities. As a result, coordinating the following surveillance requirements is necessary:

- Traffic flow data for highways, local arterials, and ramps for alternate route determination and congestion monitoring.

+ Transit schedule and travel time.
+ Communication with transit operations for route guidance allowing for schedule adherence and coordination.
+ Vehicle entrance/exit data for parking lot monitoring and availability information.
+ AVI data in transit vehicles for signal priority.
+ Response details for planning and coordination.

Corridor-Wide Surveillance Information Requirements

Long-term, intermodal transportation strategies should be developed considering the entire Corridor transportation infrastructure. The following represent informational requirements for the Corridor:

+ Origin-destination, travel time, and delay time data.
+ Traffic flow data to characterize travel demand levels.
+ Response details for coordination and strategic planning.

5.2.5 Travel Demand Management

A recent declining trend in the air quality surrounding metropolitan areas has prompted Regional Transportation Agencies to re-assess their TDM policies. A Regional TDM Committee has been formed to analyze data describing traffic congestion locations and severity in the local jurisdictions. Continual monitoring and analysis of traffic conditions and air quality have been performed over 6 months to identify high priority locations for congestion and air pollution mitigation.

Many options for SOV trip reduction and congestion mitigation have been developed and evaluated. These options include responses such as:

+ Initiate programs to promote variable work hours (e.g., a compressed work week, or staggered work hours).

+ Initiate programs to promote carpooling.

+ Initiate programs to promote transit usage.

+ Implement congestion pricing policies.

Strategies that encourage people to carpool by providing free HOV parking in predetermined areas and increased HOV parking availability at public transit parking lots are implemented. Additionally, travel time comparisons between HOV and non-HOV facilities are provided to travelers through TIS to further promote HOV facility usage. Congestion pricing is also implemented: when using toll and parking facilities, users pay variable rates based on the time of day and vehicle occupancy.

This TDM plan includes informing the public of hazardous air quality conditions via the radio and television. Reports notify the public of dangerous levels of smog and encourage people to stay home.

Within the Coalition there is a strong desire to monitor the effectiveness of the implemented TDM policies in terms of traffic congestion reduction and air quality improvement. Therefore, a planning database is developed to collect traffic flow and air quality data to determine if improvements are made when these plans are implemented. Corridor member agencies may monitor the TDM benefits and optimize strategic planning.

<u>Local Surveillance Information Requirements</u>

The following surveillance requirements will assist in TDM operations:

+ Speed, occupancy, and volume data for highways, local arterials, and ramps for congestion detection and identifying problem areas.

+ Travel time data, origin-destination data, and congestion pricing impact evaluation.

+ Video image at transit stops and HOV parking facilities for traveler security.

- Air quality monitoring for strategic planning purposes.
- TDM strategies for effectiveness evaluation and coordination.

Regional Area Surveillance Information Requirements

Regionally, generation of a response plan to provide TDM requires coordination between neighboring agencies. Coordinating the following surveillance requirements is necessary:

- Traffic flow data for highways, local arterials, and ramps for congestion detection and identifying problem areas.
- Travel time data, origin-destination data, and congestion pricing impact evaluation.
- Air quality monitoring for strategic planning.
- TDM strategies for effectiveness evaluation and coordination.
- Vehicle occupancy information to determine the effectiveness of the strategy.

Corridor-Wide Surveillance Information Requirements

Corridor-wide activities will benefit from standardization and coordination between regions so that seamless operations will ensue. The following is a set of surveillance requirements for Corridor-wide TDM.

- Traffic flow data for highways, local arterials, and ramps for congestion detection and identifying problem areas.
- Travel time data, origin-destination data, and congestion pricing impact evaluation.
- Air quality monitoring for strategic planning.
- TDM strategies for effectiveness evaluation and coordination.

5.2.6 Regulatory Operations

A tanker full of chlorine is making a long-distance trip through the Corridor. Before beginning this trip, the driver has completed all necessary HAZMAT permits and encoded this information, including the truck weight, his driving credentials, the company name, and verification of payments on the trucks electronic tag. This allows the driver to travel past inspection sites without cutting precious time from his schedule.

Before beginning his trip, the driver refers to the in-vehicle guidance system providing origin, destination, and cargo information. The route guidance system suggests a route between Delaware and Maine, excluding links on which hazardous materials are not allowed.

During the trip, the driver periodically refers to the in-vehicle route guidance system on a more detailed scale to provide travel directions. In New Jersey, an incident on the freeway causes a severe backup, and the driver uses the vehicle route guidance system to navigate unfamiliar routes.

As the transponder-equipped vehicle approaches each checkpoint, it crosses a reader and WIM sensors upstream of the facility. The vehicle is identified, classified, and weighed. Information is sent, via communication link, to the checkpoint. The information used for electronic clearance includes:

- WIM data for weight compliance.
- Motor carriers' safety fitness ratings.
- Vehicle/driver inspection and maintenance data, including the last date of inspection and out-of-service verification.
- Credentials information, including annual registration, fuel use tax, operating authority, insurance, and oversize/overweight permits.
- Cargo information, including HAZMAT listings and registration.
- Driver information, including citation records and certification.

The truck is making good time. It does not have to stop at weigh stations or test stations, and it passes through dedicated electronic toll collection lanes on the various turnpikes along the route. Because the truck satisfies the height requirements for the roads on which it is traveling, the over-height vehicle detectors do not detect the truck, and no alarms are sent to the driver. To verify the information on the electronic tag, WIM sensors and over-height vehicle detectors are utilized along the route. The ITS technology supporting commercial vehicle operation allows the commercial vehicle's travel time and speed information to be relayed to regional and Corridor-wide databases.

Local Surveillance Information Requirements

The following surveillance requirements will assist in regulatory operations:

- Traffic flow data for highways, local arterials, and ramps for route guidance.
- AVI data for origin-destination data, travel time, link travel time, and electronic clearance.
- WIM data for electronic clearance and regulatory adherence.
- HAZMAT tracking for regulatory adherence and safety monitoring.
- Over-height vehicle detection for route avoidance, roadway structure safety, and regulatory adherence.
- Upstream inspection station data or electronic clearance data for coordination and verification.

Regional Area Surveillance Information Requirements

Regionally, generation of a response plan to assist in regulatory operations requires coordination between neighboring agencies and the entire I-95 CC. As a result, coordinating the following surveillance requirements is necessary:

- Traffic flow data for highways, local arterials, and ramps for route guidance.

- AVI data for origin-destination data, travel time, link travel time, and electronic clearance.
- WIM data for electronic clearance and regulatory adherence.
- HAZMAT tracking for regulatory adherence and safety monitoring.
- Over-height vehicle detection for route avoidance, roadway structure safety, and regulatory adherence.
- Upstream inspection station data or electronic clearance data for coordination and verification.
- Regulatory policies dictated by adjacent regions for coordination.

Corridor-Wide Surveillance Information Requirements

Surveillance requirements for Corridor-wide regulation will require both coordination and standardization at a Corridor-wide level. The following surveillance data are candidate components for such standardization:

- Traffic flow data for highways, local arterials, and ramps for route guidance.
- AVI data for origin-destination data, travel time, link travel time, and electronic clearance.
- WIM data for electronic clearance and regulatory adherence.
- HAZMAT tracking for regulatory adherence and safety monitoring.
- Over-height vehicle detection for route avoidance, roadway structure safety, and regulatory adherence.
- Regulatory policies dictated by all regions for Corridor-wide coordination.

5.3 SYSTEM-WIDE REQUIREMENTS

System-wide requirements were derived from an overall Corridor-wide surveillance system perspective and cover both the operational and performance aspects of the system. Relevant information from the four National ITS Architecture Phase I studies sponsored by the FHWA was incorporated. The system-wide requirements are as follows:

- The surveillance system shall provide accurate and reliable information. This requires the system to minimize system malfunction and failures.
- The surveillance system shall provide timely information. To provide timely information, the system shall minimize processing and communication time.
- The data generated by the surveillance system shall be transparent to system users. The system shall be able to transport the necessary surveillance data to appropriate locations. This means that the communication capability shall provide connectivity to all necessary users (nodes), including TMCs, TIS centers, etc. The processing capability of the system shall include selecting appropriate data to be transported to each node.
- Surveillance data format and contents, including geographic references, shall be compatible throughout the Corridor. The data compatibility may be maintained by using the same data format or by using different, but predefined, data formats.
- The system shall provide the information required to support all relevant ITS applications. This implies that the system shall process and format raw surveillance data from the sensor to derive the required information. The processing shall include a capability for fusing data from multiple sources.
- The surveillance sensors shall perform satisfactorily under various environmental and traffic conditions. These conditions include weather (temperature, humidity, etc.), lighting, and traffic conditions. Since the Corridor includes a large geographic area with varying environmental and traffic conditions, the selection of sensors shall be based on the conditions of the specific geographic location.

+ The surveillance system shall have the capability to detect malfunctioning or failed sensors. processors. and communication components. System malfunctions and failures shall be reported to a control center for corrective action.

+ The system shall have openness. modularity and scalability features, Openness will support the incorporation of the future sensor technologies by providing industry-standard interfaces. System modularity will enable an evolutionary deployment of the surveillance system. It will also provide flexibility in maintenance. Scalability will allow the system to accommodate future growth.

+ The existing infrastructure shall be preserved to the maximum extent possible. Tailored interfaces shall be provided in order to accommodate the existing system as needed.

+ Data security shall be provided to protect the privacy of the individuals and oraanizations participating in the collection of surveillance data.

+ The system shall be reliable, Necessary redundancies shall be built into the system design to prevent single-node failure.

The communication system supporting the various surveillance functions include the following features:

+ Flexibility. Flexibility is defined here as the ability of the communication system to accommodate different communication standards without compromising the data flow of the system. The surveillance communication system shall be flexible, so that a mixture of communication techniques may be used todistribute and disseminate data.

  Communication standards shall be fully compatible with the National Traffic Control/lVHS Communications Protocol (NTCIP), for the areas to which it applies. The NTCIP is currently being developed by the National Electrical Manufacturers Association (NEMA), eventually, will replace the existing TS-2 Standards for traffic control hardware.

  At a minimum, surveillance communications shall be compatible with the following communication standards:

- RS232
- HDLC
- RS449
- RS485
- NTSC Analog Video
- FM and PSK Radio
- RS422
- DS1
- RS530
- Synchronous Optical Network (SONET)
- Fiber Distribution Data Interface (FDDI)
- Integrated Services Digital Network (ISDN)
- Asynchronous Transfer Mode (ATM)
- H.261 Compressed Video
- Cellular Radio
- Ethernet (IEEE 802.3)
- VSAT
- X.25 Data Packetizing

To maintain flexibility, incompatible data formats are to be avoided when using a common media. The surveillance communications network shall preclude the use of a proprietary communication protocol which excludes the use of other communications protocols sharing the same transmitting media. Subnetworks using a particular communications protocol exclusively are allowed. However, if the data is to be shared on a broadband network, a communications gateway shall be used to convert the protocol to the broadband media-compatible protocol.

+ Adaptability The first issue of adaptability is the ability of the communication system to accommodate jurisdictional requirements and to be technologically contemporary. This implies that critical data services through the network shall not be interrupted due to the addition of new equipment or changes in system topologies. The second issue is the communication system's compatibility with the needs of the local TMC. This accommodates the differences in requirements for each local TMC. These differences include the number and types of sensors used, the amount of video data used, whether the area is rural or urban, and the level of traffic demand.

+ Long-Term Growth. The-long term growth of the surveillance communications environment is based on the adaptability, flexibility, and design margin of the system. Therefore, provisions shall be made within the communications link budget to accommodate redundancy, frequency, and fractional time slot use within a TDM signal. These provisions are as follows:

  - Critical data interfaces shall be hot-spared.
  - Sufficient design margin shall be included to accommodate anticipated growth within a link.

- Provisions shall be made to increase the number of repeaters as data throughput increases.

While these requirements dictate overall system performance and operations, the requirements to be described in the next two sections influence specific aspects of the system design. These requirements include the system functional requirements and interface, and hardware and software requirements.

5.4 SYSTEM FUNCTIONAL REQUIREMENTS

This section describes the functional requirements for the Corridor-wide surveillance system based on the goals and objectives described in Chapter 2 of this report. The primary functions of the system are to sense or acquire data from the transportation environment; process the data to produce information necessary for the operation and management of the Corridor's transportation systems; and transmit this information to appropriate external systems for application. Development of the system functional requirements followed a top-down approach. It began with a definition of the context within which the surveillance system will operate. The context identifies the physical entities that interact with the surveillance system and the associated data that the surveillance system is required to produce. From this system context, top-level functions were defined and then decomposed into lower-level functions (see Figure 5-l). At each level of the functional hierarchy, requirements for system functions and data were defined.

To facilitate the above structured approach to functional requirements definition, a Computer-Aided Software Engineering (CASE) tool was used. This CASE tool (called MacAnalyst™) has helped to draw the Data Flow Diagrams (DFD), track definition of the data items in a data dictionary, and maintain data consistency from one level of the hierarchy to the next. A complete set of the DFDs representing the requirements model for the Corridor-wide surveillance system is contained in Appendix H, and the associated Data Dictionary in Appendix I. In the following sections, an overview of the Corridor-wide surveillance system's functional requirements is provided, followed by a detailed description of the required functions and data (both input and output from the surveillance system processes).

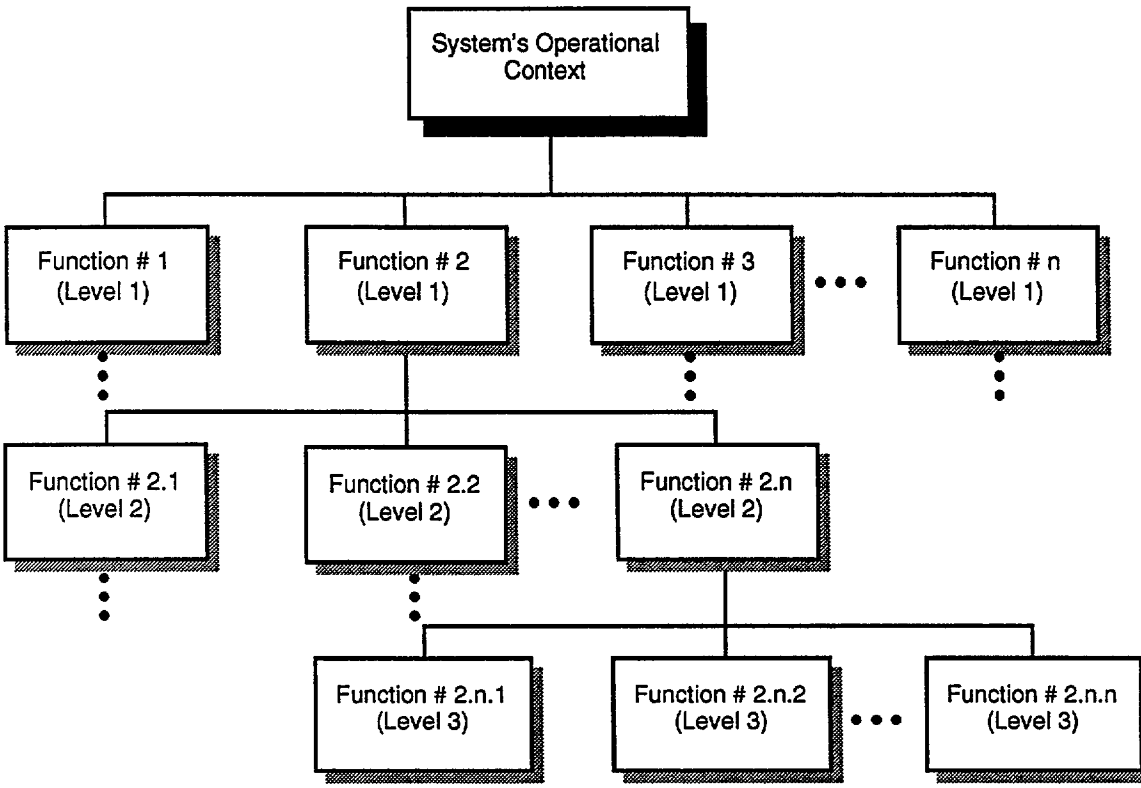

Figure 5-1. System Hierarchy Used in Functional Decomposition

5.4.1 Overview of Functional Requirements

Based on the hierarchy illustrated in Figure 5-1, the surveillance system's functional requirements were defined for each level. At the system context level, the requirements were defined according to the external entities with which the system must interact. These external entities were divided into two categories: information source and information sink. Information sources include the following external entities: the Road, the Traffic Stream, the Vehicle, the Transportation Environment, People, and External Services and Support Systems. Information sinks include the following external systems: Incident Management, Traffic Control, Law Enforcement, Travel Demand Management, Snow Removal Management, Traveler Information, Intermodal Management, Transportation Planning, and Toll Collection. All identified information sinks, except the Toll Collection System, correspond to the functional goals of the surveillance system, which were:

- To enhance traffic incident management.
- To enhance real-time traffic control operations.
- To support traffic law and regulation enforcement.
- To enhance traffic management during snow storms and other emergencies.
- To facilitate TDM strategy implementation.
- To improve multi-modal and intermodal transportation operations.
- To enhance the transportation systems planning database.
- To support TIS.

The relationships between the Corridor-wide surveillance system and its external entities are identified in Figure 5-2 and are described as follows (for definition of data items, refer to Appendix I):

+ Road. The Road External Entity represents the physical attributes of the roadway. The Corridor Surveillance System shall have the capability to sense the real-world road conditions and acquire the associated data directly from the road. Road condition data may include the physical status of the pavement or bridge structures, pavement temperature, presence of debris on the road, presence of animals in the right-of-way, and any weather effects (e.g., fog) along the road.

+ Traffic Stream. The Traffic Stream External Entity provides the real-world traffic conditions of the roadway. Essentially, the traffic conditions are composed of both traffic and incident parameters. The traffic parameters allow actual traffic flow measures to be obtained, including the traffic speed, volume, and density. Incident parameters are attributes including the number of vehicles involved, the type of damage, and human injuries. The surveillance system shall have the capability to acquire these real-world traffic data.

+ Vehicle. The Vehicle External Entity represents the physical attributes of a vehicle. The real-world vehicle attributes include both observable vehicle parameters and vehicle communications. Observable vehicle parameters are vehicle speed,

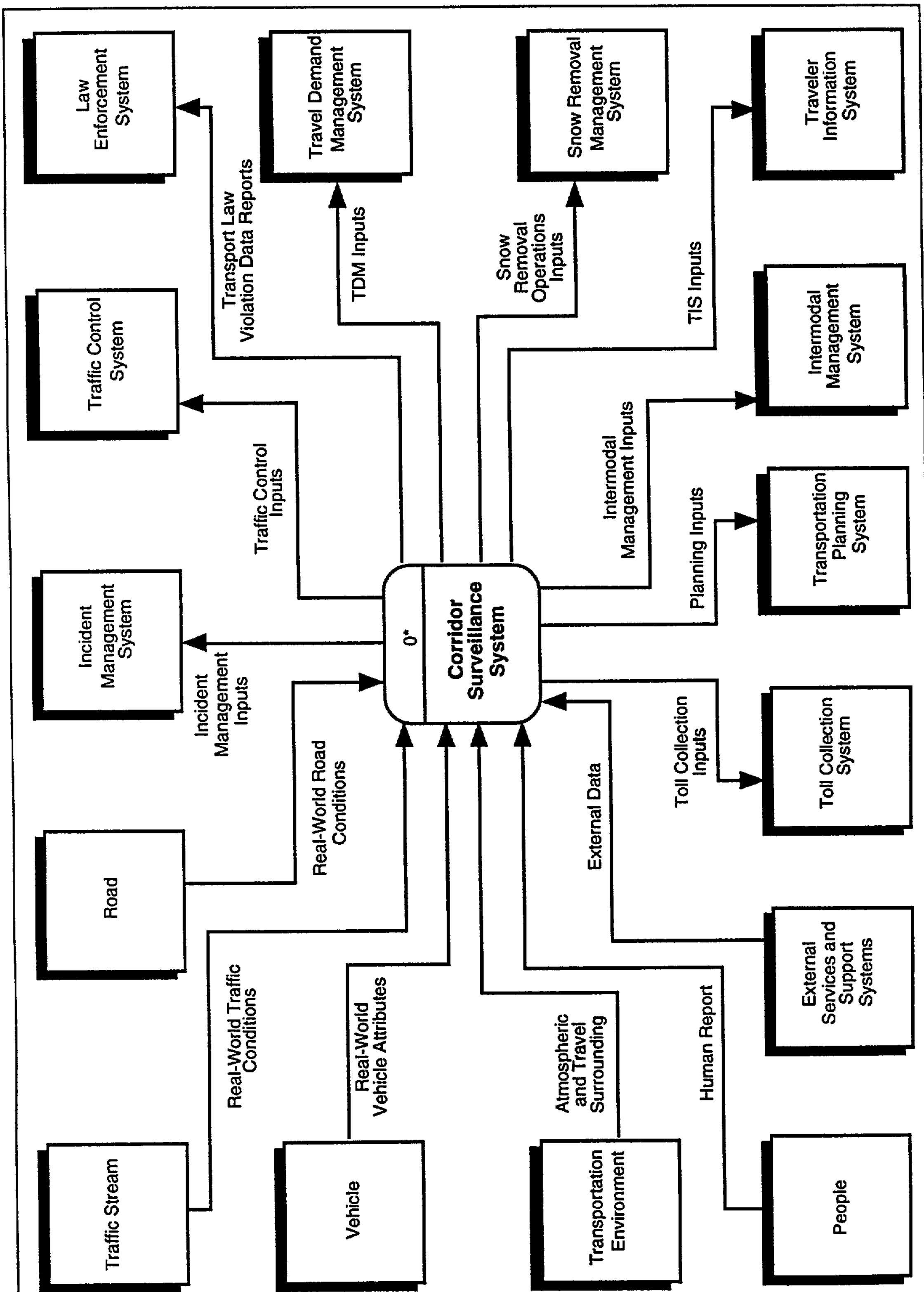

Figure 5-2. Operational Context of the Corridor-Wide Surveillance System

occupancy, location, emissions, dimension, weight, travel direction, and identification (e.g., license plate number). Vehicle communications are messages that the vehicle transmits to the surveillance system deliberately. These messages may include elements of the observable vehicle parameters or other attributes, such as vehicle priority, vehicle identification, or Mayday signals. The surveillance system shall have the capability to acquire these real-world vehicle attributes.

+ Transportation Environment. The Transportation Environment External Entity provides both atmospheric and travel surrounding data. Atmospheric data is composed primarily of air pollution and weather conditions data. Travel surrounding data contains information related to the travel environment at parking facilities, at intermodal transfer points, and in public transit vehicles for travel security monitoring. The surveillance system shall have the capability to acquire this data of the transportation environment.

+ People provide to the Corridor Surveillance System verbal reports (e.g., People using the telephone) on traffic conditions and incidents. Human reports can be initiated by drivers, travelers (e.g., transit users), or citizens (people who are not traveling). Drivers and travelers may include people who are involved in an incident or who just witness a condition that should be reported. The surveillance system shall have the capability to receive and process human reports.

+ External Services and Support Svstems. The External Services and Support Systems External Entity is the mechanism for receiving data from agencies and organizations that are external to the surveillance system. Typical data would include external traffic data (e.g., probe data from a private vehicle fleet), map data (e.g., new GIS data), facility data (e.g., parking location and highway geometric data), tracked vehicle identification (e.g., transit vehicles), and route data (e.g., transit and truck routes). The surveillance system shall have the capability to receive and process supporting data provided by external sources.

+ Incident Management System. The Incident Management System External Entity accept input from the Corridor Surveillance System for managing traffic incident and congestion. Incident management input includes traffic incident, performance (e.g., queue length and delay), and flow data, road hazard reports, travel security events, and emergency response vehicle, maintenance vehicle, and HAZMAT carrier location and tracking data. The surveillance system shall have the capability to generate these incident management input parameters based on the acquired information.

+ Traffic Control System. The Traffic Control System External Entity accepts input from the Corridor Surveillance System for traffic control. Traffic control input includes traffic incident, performance, and flow data, signal priority requests, and road hazard reports. The surveillance system shall have the capability to generate these traffic control input parameters based on the acquired information to support traffic control operations, including real-time, adaptive control.

+ Law Enforcement System. The Law Enforcement System External Entity accepts input from the Corridor Surveillance System for enforcing various transportation laws. The surveillance system shall have the capability to generate transportation law violation data reports to the Law Enforcement System, including speed, vehicle weight, vehicle dimension, emission, HOV, and designated route violations (e.g., for commercial vehicles), and unsafe vehicle status (e.g., brake failure, loss of cargo integrity, etc.).

+ Travel Demand Management System. The TDM System External Entity accepts input from the Corridor Surveillance System for developing, evaluating, and implementing TDM policies. The surveillance system shall have the capability to generate and provide air quality monitoring data (including reports of high pollution areas), traffic flow, traffic performance, vehicle occupancy, and parking usage data to support the development of various TDM policies. These data items shall include statistics that may be used to analyze the performance trends of the transportation system. Data on other transportation modes are to be provided by other systems external to the surveillance system.

+ Snow Removal Management System. The Snow Removal Management System External Entity accepts input from the Corridor Surveillance System for coordinating, scheduling, and planning snow removal activities. Snow removal operations input shall include traffic flow, traffic performance, snow and ice prediction, and maintenance vehicle location and tracking data. This input shall be suitable for use in both real-time operations and planning.

+ Traveler Information System. The TIS External Entity accepts input from the Corridor Surveillance System to formulate information for the travelers. The surveillance system shall have the capability to provide traveler information input, including traffic incident, traffic performance, parking (e.g., availability), and road hazard detection data. The data shall be suitable for formulating both real-time and predicted traveler information.

+ Intermodal Management Svstem. The Intermodal Management System External Entity accepts data from the Corridor Surveillance System to assist in managing intermodal activities. Intermodal management input includes data for both vehicle fleet and intermodal transfer operations. Vehicle fleet operation data shall include traffic flow, performance, and incident data, vehicle occupancy, and transit vehicle location and tracking data. All traffic-related data shall be route specific to support applications such as vehicle routing and prediction of vehicle arrival time at a predetermined location (e.g., a transit transfer point). Intermodal transfer operation data shall include parking usage data and parking fee determination input.

+ Transportation Planning System. The Transportation Planning System External Entity receives data from the Corridor Surveillance System to support various planning functions such as facility planning, pavement management, safety improvement, and evacuation due to natural disasters. The surveillance system shall have the capability to generate and provide planning data on traffic flow and performance, and vehicle weight, emissions, and occupancy.

+ Toll Collection System. The Toll Collection System External Entity accepts vehicle-specific parameters from the surveillance system to formulate toll rates. The surveillance system shall acquire and provide vehicle weight, dimension, identification, and occupancy data.

To satisfy these system-level functional requirements, the surveillance system shall perform eight core functions, whose relationships and data flows are illustrated in Figure 5-3.

The following eight functions are designated as Level-l functions according to the system hierarchy illustrated in Figure 5-1:

+ Monitor Traffic Conditions.

+ Acquire Individual Vehicle Information.

+ Monitor Environmental Conditions.

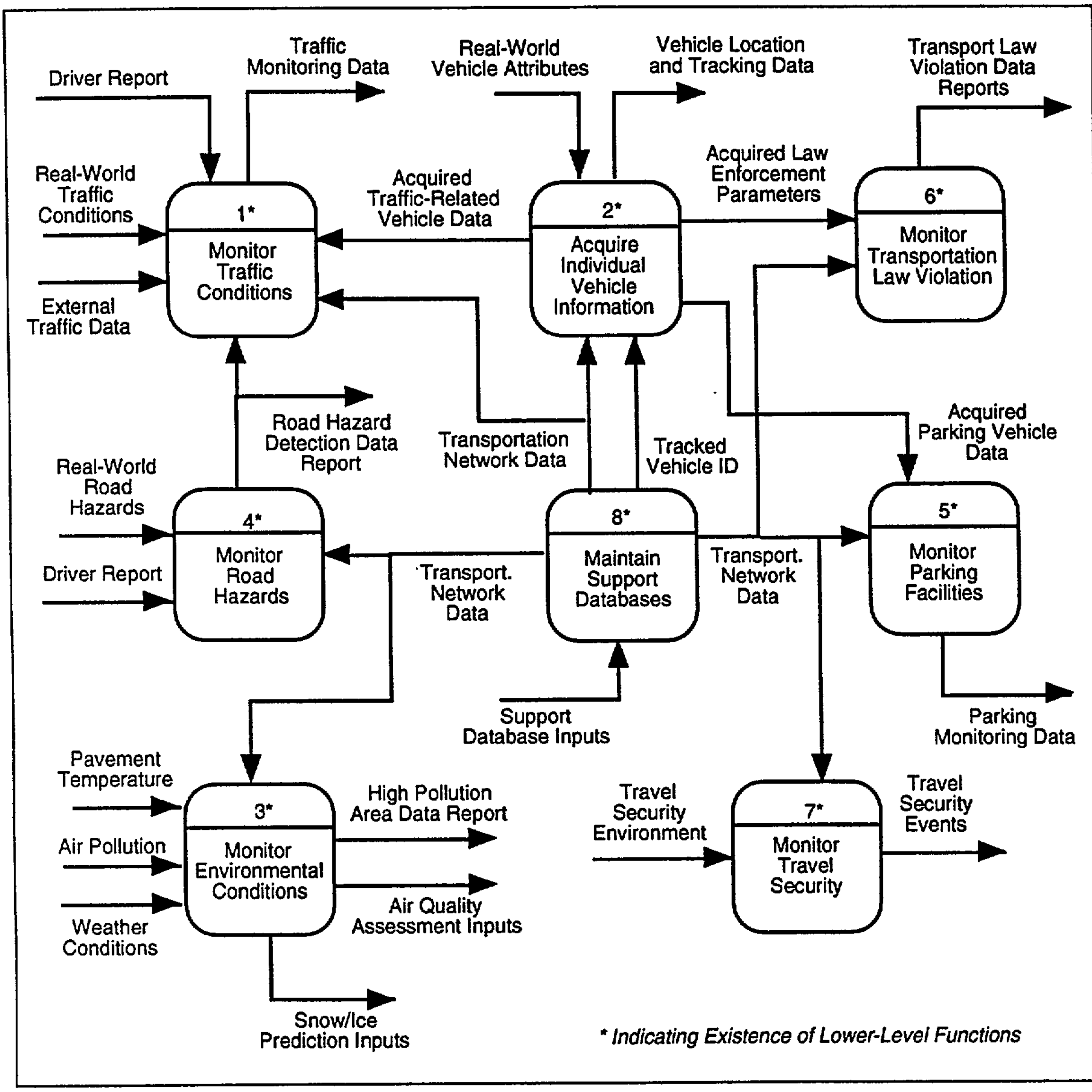

Figure 5-3. The System's Level-1 Functional Requirements Include Eight Functions

- Monitor Road Hazards.
- Monitor Parking Facilities.
- Monitor Transportation Law Violation.
- Monitor Travel Security.
- Maintain Support Databases.

These functions were decomposed into lower-level functions as summarized in Table 5-l. A detailed description of the Level-1 functions, their associated lower-level functions, and the system functional requirements follows in Section 5.4.2.

Table 5-1. Summary of Lower-Level Surveillance Functions

1. Monitor Traffic Conditions 1.1 Acquire Traffic Data* 1.2 Assess Traffic Performance* 1.3 Detect Traffic Incident and Congestion* 1.4 Confirm Traffic Incident and Congestion* 1.5 Acquire Incident Assessment Data 2 Acquire Individual Vehicle Information 2.1 Determine Vehicle Speed and Direction 2.2 Determine Vehicle Weight and Dimension 2.3 Determine Vehicle Occupancy 2.4 Determine Vehicle Identification 2.5 Determine Vehicle Location 2.6 Determine Vehicle Emissions 2.7 Determine Vehicle Safety 2.8 Receive Vehicle-to-Infrastructure Communications 3 Monitor Environmental Conditions 3.1 Monitor Road Weather Conditions 3.2 Monitor Pavement Temperature 3.3 Formulate Snow/Ice Prediction Data 3.4 Monitor Roadway Air Pollution 3.5 Identify High Pollution Areas 3.6 Formulate Air Quality Assessment Data 4. Monitor Road Hazards 4.1 Detect Debris on Road 4.2 Detect Pavement/Bridge Damage 4.3 Detect Animal Entering Roadway 4.4 Receive Road Hazard Reports 4.5 Identify Low Visibility Conditions 4.6 Detect Slippery Road Conditions 4.7 Detect Hazardous Cross Wind Conditions 4.8 Verify Road Hazard Detection 4.9 Generate Road Hazard Detection Report	5. Monitor Parking Facilities 5.1 Determine Parking Entries and Exits 5.2 Determine Parking Usage 5.3 Formulate Parking Charge input 6. Monitor Transportation Law Violation 6.1 Determine Speed Violation 6.2 Determine Weight Violation 6.3 Determine Height and Width Violation 6.4 Determine HOV Occupancy Violation 6.5 Determine Designated Route Violation 6.6 Determine Vehicle Emissions Violation 6.7 Determine Unsafe Vehicle Status 7. Monitor Travel Security 7.1 Monitor Intermodal Transfer Points 7.2 Detect Transfer Point Security Events 7.3 Monitor Public Transit Vehicle 7.4 Detect Transit Vehicle Security Events 7.5 Monitor Parking Facility Security 7.6 Detect Parking Facility Security Events 8. Maintain Support Databases 8.1 Maintain Road Network Database 8.2 Maintain Route Database 8.3 Maintain Transfer Point Database 8.4 Maintain Parking Database 8.5 Maintain Surveillance Asset Database 8.6 Maintain Tracked Vehicle Database

* This function is further decomposed to one more level of detail as shown in Section 5.4.2.

5.4.2 Description of Functional Requirements

5.4.2.1 Function #1: Monitor Traffic Conditions

The function of the *Monitor Traffic Conditions* process is to formulate traffic monitoring data, such as traffic flow, performance, and incident data, and signal priority requests. Data gathered by this process shall include real-world traffic conditions, driver reports, external transportation data, traffic-related vehicle data, road hazard reports, and transportation network data. All traffic monitoring data shall be provided to and suitable for applications by other internal processes and external systems identified in the system context. The traffic conditions monitoring functions include the five Level-2 functions shown in Figure 5-4.

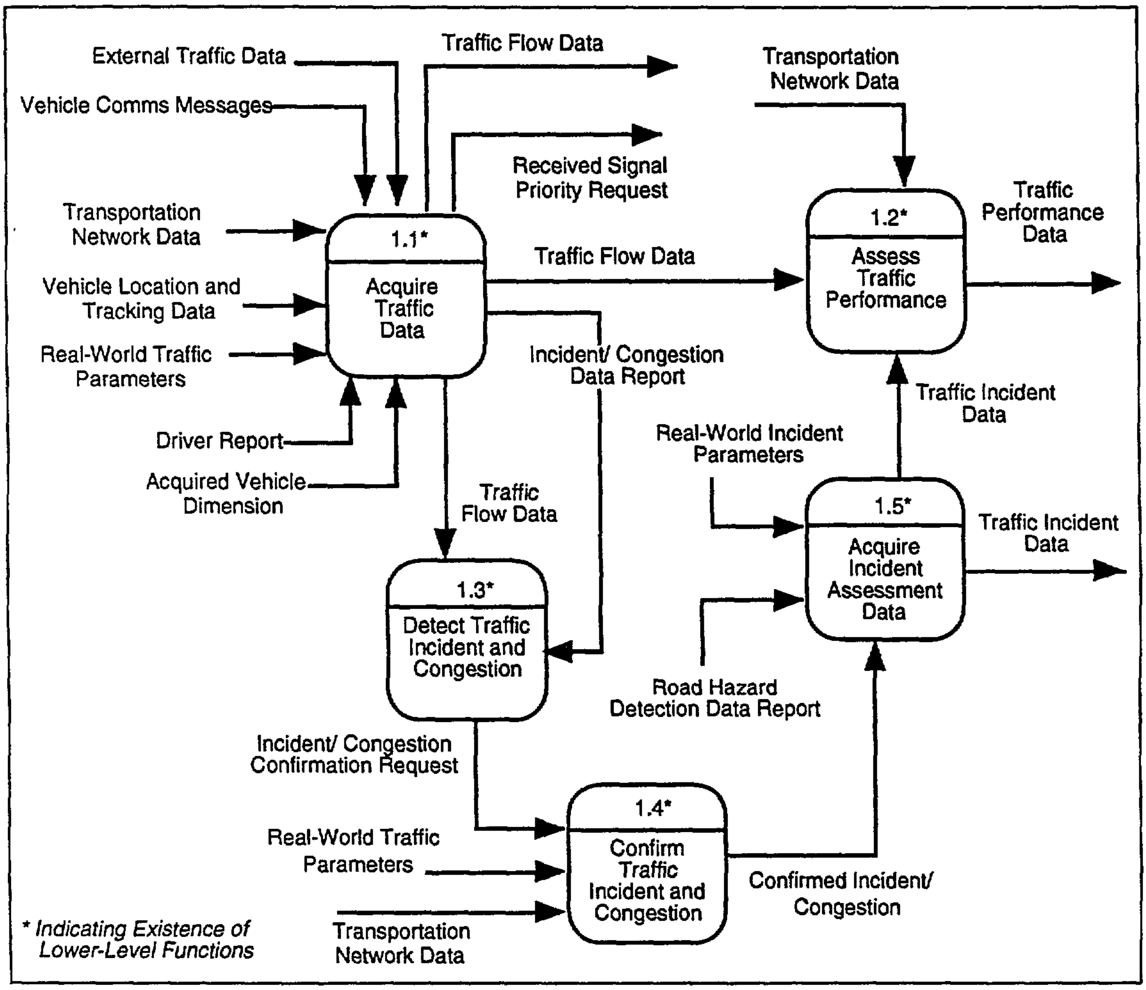

Figure 5-4. Required Traffic Condition Monitoring Functions

Function #1.1: Acquire Traffic Data

The *Acquire Traffic Data* process is primarily responsible for acquiring the data regarding the flow of the traffic in real time (see Figure 5-5). This data includes measures such as traffic speed, volume, density, headways, and vehicle classes, location, and tracking data. The *Acquire Traffic*

Input Processing Requirements

- This process shall have the capability to acquire all traffic parameters that are observable from the road network.
- This process shall accept driver reports on traffic incidents or congestion, and motorist call-ins for assistance.
- This process shall receive vehicle tracking and location data for estimating traffic stream parameters (e.g., speed and travel time).
- This process shall accept vehicle dimensions (e.g., height and width) acquired by other processes for determining vehicle classification and composition.
- This process shall accept vehicle communication messages, such as a Mayday message or a signal priority request.
- This process shall accept transportation network data for location referencing of acquired traffic data.
- This process shall accept traffic data from external sources such as the Corridor's non-member agencies and private service providers.

Process and Control Requirements

- This process shall determine traffic speed based on the acquired traffic parameters.
- This process shall determine traffic volume based on the acquired traffic parameters.
- This process shall determine traffic density based on the acquired traffic parameters.
- This process shall determine traffic headway based on the acquired traffic parameters.
- This process shall be capable of classifying a vehicle based on its dimensions.
- This process shall fuse the acquired and received data to generate traffic flow data. The fused data shall be in a predefined format suitable to the required applications.

Input Processing Requirements

+ This process shall have the capability to acquire all traffic parameters that are observable from the road network.

+ This process shall accept driver reports on traffic incidents or congestion, and motorist call-ins for assistance.

+ This process shall receive vehicle tracking and location data for estimating traffic stream parameters (e.g., speed and travel time).

+ This process shall accept vehicle dimensions (e.g., height and width) acquired by other processes for determining vehicle classification and composition.

+ This process shall accept vehicle communication messages, such as a Mayday message or a signal priority request.

+ This process shall accept transportation network data for location referencing of acquired traffic data.

+ This process shall accept traffic data from external sources such as the Corridor's non-member agencies and private service providers.

Process and Control Requirements

- This process shall determine traffic speed based on the acquired traffic parameters.
- This process shall determine traffic volume based on the acquired traffic parameters.
- This process shall determine traffic density based on the acquired traffic parameters.
- This process shall determine traffic headway based on the acquired traffic parameters.
- This process shall be capable of classifying a vehicle based on its dimensions.
- This process shall fuse the acquired and received data to generate traffic flow data. The fused data shall be in a predefined format suitable to the required applications.

+ This process shall correlate driver reports and vehicle communication messages to create an incident/congestion data report.

+ This process shall acquire signal priority requests from emergency-response and transit vehicles having such capabilities.

Output Processing Requirements

- ♦ This process shall be capable of transmitting the formatted traffic flow data to predetermined internal and external systems.
- ♦ This process shall be capable of transmitting an incident/congestion data report in a required format to other processes and systems.
- ♦ This process shall be capable of relaying the received signal priority request to appropriate traffic control systems.

Function #1 .2: Assess Traffic Performance

The *Assess Traffic Performance* process shall determine the performance of the road traffic based on dynamic (e.g., traffic flow data, incident data) and static data (e.g., transportation network data). The primary traffic performance assessment functions are shown in Figure 5-6.

Input Processing Requirements

+ This process shall accept traffic flow data (e.g., traffic speed, volume, etc.).

+ This process shall accept transportation network data (e.g., road network geographic and geometric data).

+ This process shall accept traffic incident data (e.g., lane blockage, location, etc.).

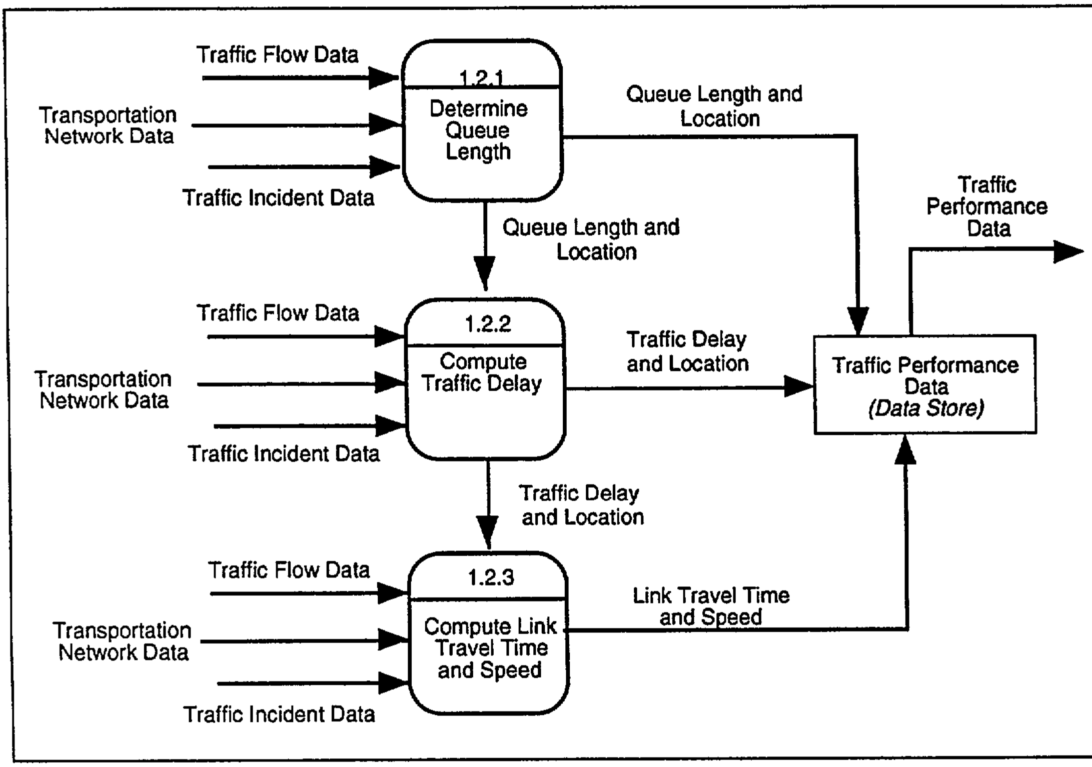

Figure 5-6. Required Traffic Performance Assessment Functions

Process and Control Requirements

- This process shall determine the queue length and location based on the traffic flow data, traffic incident data, and the transportation network data.
- This process shall determine the traffic delay and location based on the traffic flow data, traffic incident data, transportation network data, and the queue length and location.
- This process shall determine the link travel time and speed based on the traffic flow data, traffic incident data, transportation network data, and the traffic delay and location.
- The queue length and location, traffic delay and location, and the link travel time and speed shall all be stored and accessible for other applications.

- The queue length and location, traffic delay and location, and the link travel time and speed shall all be combined to generate the traffic performance data for the Corridor's road network.

Output Processing Requirements

- This process shall be capable of disseminating the traffic performance data to other processes and external systems.
- This process shall have the capability to display traffic performance information.

Function #1.3: Detect Traffic Incident and Congestion

The *Detect Traffic Incident and Congestion* process is responsible for analyzing the current traffic flow data and any incident/congestion reports to detect traffic incidents or congestion. If an incident or congestion is detected, a confirmation request shall be generated. The traffic incident and congestion detection functions are shown in Figure 5-7.

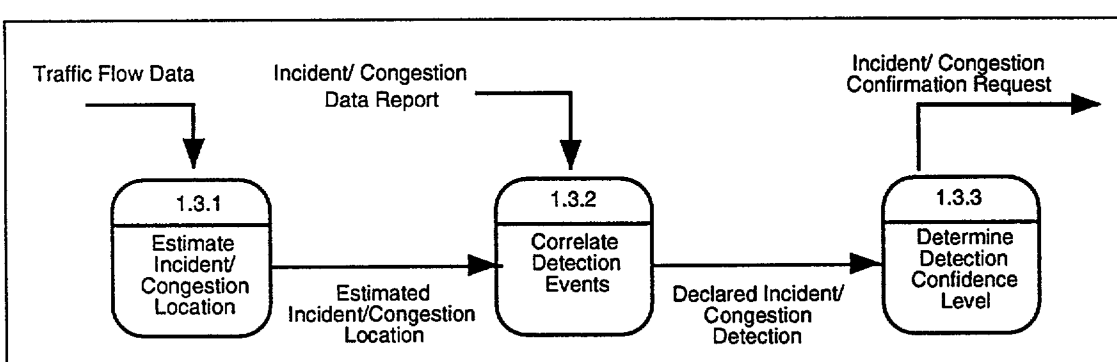

Figure 5-7. Required Traffic Incident/Congestion Detection Functions

Input Processing Requirements

- This process shall accept traffic flow data (e.g., traffic speed, volume, etc.) for automated incident and congestion detection.

- This process shall accept incident/congestion data reports (received from human surveillance sources).

Process and Control Requirements

- This process shall estimate incident/congestion location based on the current traffic flow data.

- Using the estimated incident/congestion location and the incident/congestion report, this process shall correlate the data to either detect a false alarm or declare an incident/congestion detection.

- Once an incident/congestion event has been detected, this process shall determine the level of confidence for the detected incident/congestion. The level of confidence shall be based on a set of predetermined criteria.

Output Processing Requirements

- This process shall be capable of generating an incident/congestion confirmation request according to a predefined format.

- This process shall be capable of transmitting an incident/congestion confirmation request to another process.

Function #1.4: Confirm Traffic Incident and Congestion

The Confirm Traffic Incident and Congestion process shall confirm the occurrence or existence of an incident or congestion event based on the provided time and location information in the confirmation requests. It shall perform the three functions shown in Figure 5-8.

Input Processing Requirements

- This process shall accept incident/congestion confirmation requests from the incident/congestion detection process.

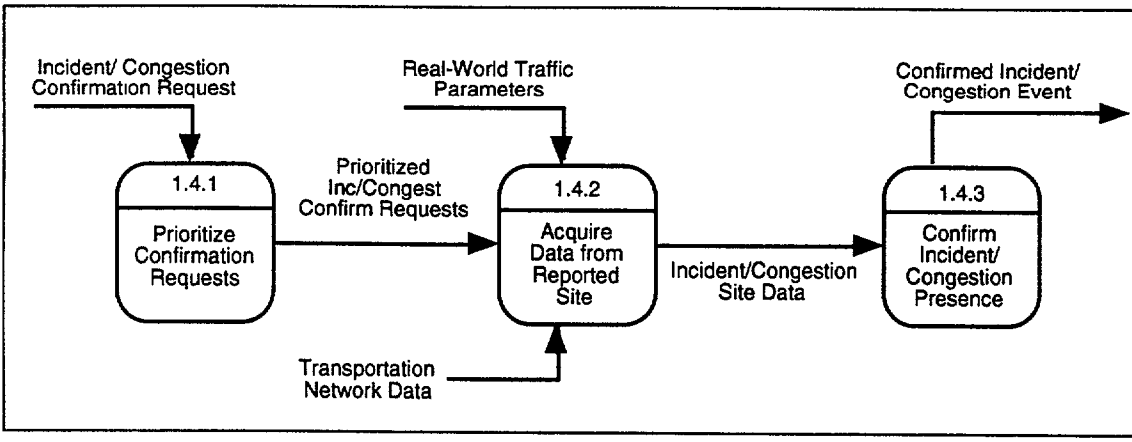

Figure 5-8. Required Traffic Incident and Congestion Confirmation Functions

- This process shall have the capability to acquire real-world traffic parameters related to the incident or congestion event.
- This process shall accept transportation network data for location references.

<u>Process and Control Requirements</u>

- This process shall have the capability to prioritize all confirmation requests based on their associated level of confidence and status.
- After the incident requests are prioritized, this process shall acquire the incident or congestion data from the reported site.
- Once the incident or congestion data at the site has been acquired, this process shall assess the situation to determine the presence of the incident or congestion.

<u>Output Processing Requirements</u>

- This process shall be capable of formulating a data report of the confirmed incident or congestion event according to a predefined format.
- This process shall be capable of transmitting the data report of a confirmed incident or congestion event to other processes.

Function #1.5: Acquire Incident Assessment Data

The *Acquire Incident Assessment Data* process is responsible for gathering information for determining the appropriate responses to an incident. It shall acquire information pertaining to traffic lane blockage, medical assistance needs, HAZMAT control needs, and incident removal needs. This information shall be combined with the incident confirmation information that the *Acquire Incident Assessment Data* process receives to create a packet of the traffic incident data. The incident assessment data acquisition functions are shown in Figure 5-9.

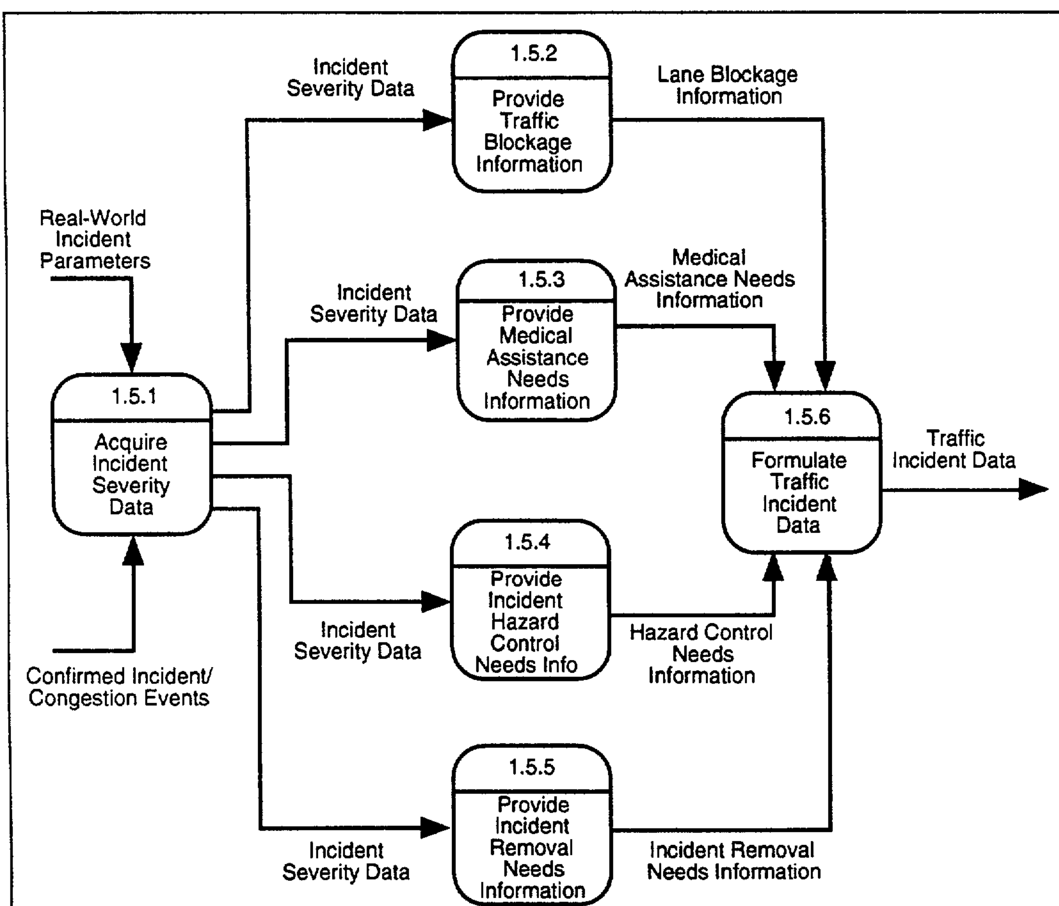

Figure 5-9. Required Incident Assessment Data Acquisition Functions

<u>Input Processing Requirements</u>

- This process shall acquire real-world incident parameters.
- This process shall accept a confirmed incident/congestion data report.

Process and Control Requirements

- This process shall use a confirmed incident/congestion data report to locate and acquire the real-world incident parameters to form incident severity data.
- The incident severity data shall be assessed to provide lane blockage information.
- The incident severity data shall be assessed to provide medical assistance needs information.
- The incident severity data shall be assessed to provide hazard control needs information (e.g., fire and explosion suppression).
- The incident severity data shall be assessed to provide incident removal needs information (e.g., heavy tow trucks or HAZMAT cleanup).
- The lane blockage, medical assistance needs, hazard control needs, and incident removal needs information shall be combined with incident location and time of occurrence to generate a traffic incident data report.

Output Processing Requirements

+ This process shall be capable of formulating traffic incident data according to a predetermined format.
+ This process shall be capable of disseminating traffic incident data to other processes and external systems.

5.4.2.2 Function #2: Acquire Individual Vehicle Information

The *Acquire Individual Vehicle Information* process receives real-world vehicle attributes, transportation network data, and tracked vehicle identifications. This input is needed to acquire vehicle-specific information, such as speed, direction, weight, dimension, occupancy, identification, location, emissions, safety status reports, and communication messages. These attributes are then used by several external systems, including Traffic Law Enforcement, Toll

Collection, TDM, and Transportation Planning. The individual vehicle information acquisition functions are shown in Figure 5-10.

Function #2.1: Determine Vehicle Speed and Direction

The *Determine Vehicle Speed and Direction* process is responsible for determining the speed and direction of travel of a vehicle.

Process and Control Requirements

+ This process shall determine the vehicle speed.

+ This process shall determine the vehicle travel direction.

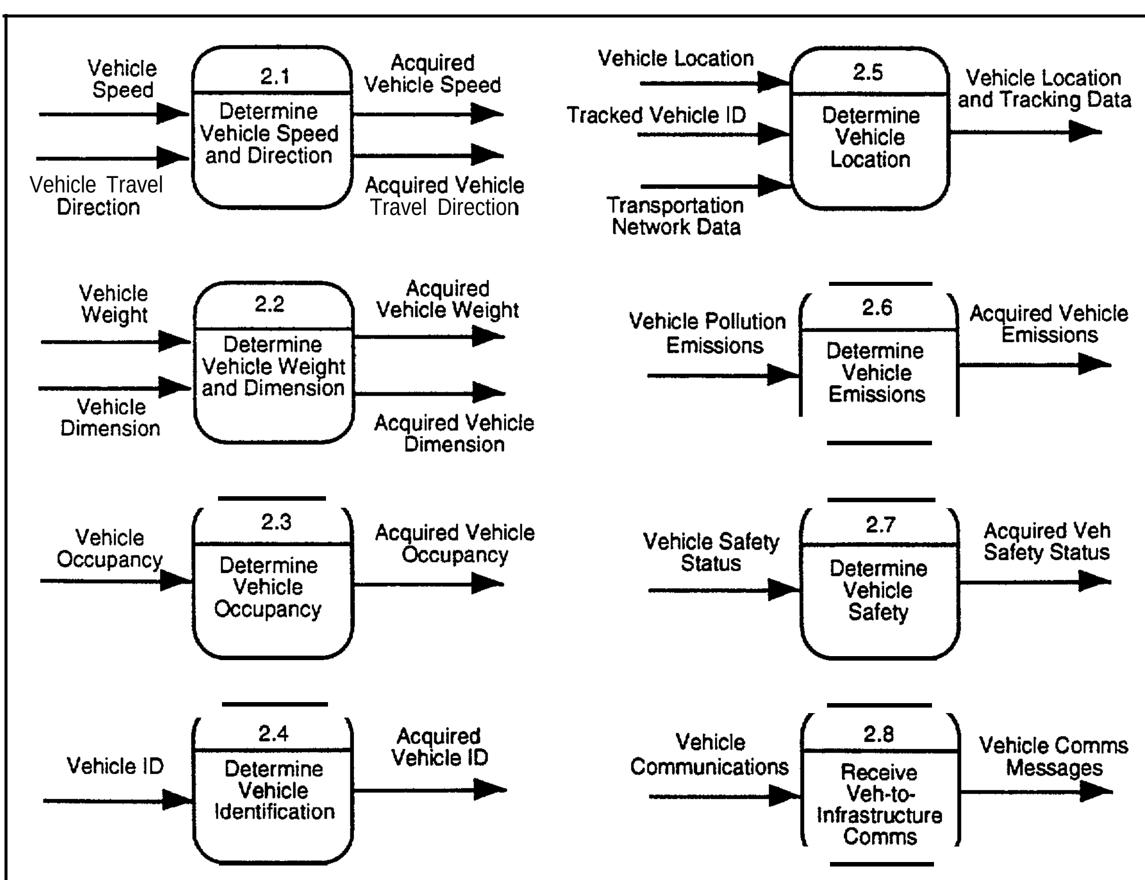

Figure 5-10. *Required Individual Vehicle Information Acquisition Functions*

Output Processing Requirements

+ This process shall be capable of disseminating the acquired vehicle speed to other processes.

+ This process shall be capable of disseminating the acquired vehicle travel direction to other processes (e.g., vehicle entry and exit at a parking facility).

Function #2.2: Determine Vehicle Weight and Dimension

The *Determine Vehicle Weight and Dimension* process is responsible for determining the weight and dimensions of a vehicle.

Process and Control Requirements

+ This process shall determine the vehicle weight including axle weight and gross vehicle weight while the vehicle is in motion.

+ This process shall determine the vehicle dimensions while the vehicle is in motion.

Output Processing Requirements

+ This process shall be capable of transmitting the acquired vehicle weight to other processes, such as transportation law violation determination and planning data compilation, and external systems, such as electronic toll collection.

+ This process shall be capable disseminating the acquired vehicle dimensions to other processes for safety warning (external) and traffic composition determination,

Function #2.3: Determine Vehicle Occupancy

The *Determine Vehicle Occupancy* process is responsible for determining the number of people in a vehicle.

Process and Control Requirements

This process shall determine the vehicle occupancy for both transit and non-transit vehicles.

Output Processing Requirements

This process shall be capable of disseminating the acquired vehicle occupancy data to appropriate processes for planning, control, and law enforcement purposes.

Function #2.4: Determine Vehicle Identification

The *Determine Vehicle Identification* process is responsible for determining the unique identification of a vehicle.

Process and Control Requirements

This process shall identify a vehicle using the communications messages from the vehicle or its physical features (e.g., license plate number).

Output Processing Requirements

This process shall be capable of providing the acquired vehicle identification to other processes and external systems for other applications.

Function #2.5: Determine Vehicle Location

The *Determine Vehicle Location* process is responsible for determining the location of a vehicle in the road network if it has been designated as a tracked vehicle. Examples could include police cars, fire trucks, EMS vehicles, ambulances, and transit vehicles. The vehicle locations shall have the same geographic references as those of the transportation network.

Input Processing Requirements

+ This process shall identify the tracked vehicle.

+ This process shall accept the transportation network data from the transportation network database.

Process and Control Requirements

+ This process shall determine the location of the tracked vehicle.

+ This process shall locate the tracked vehicle in the transportation network or sub network (e.g., transit route).

+ This process shall generate vehicle tracking data based on the required location update rate and time window (application dependent).

Output Processing Requirements

+ This process shall provide location data for the tracked vehicles to other processes.

+ This process shall provide tracking data for the tracked vehicles to other processes.

Function #2.6: Determine Vehicle Emissions

The *Determine Vehicle Emissions* process is responsible for determining the air pollution emissions from a vehicle.

Process and Control Requirements

This process shall have the capability to measure the vehicle emissions while the vehicle is in motion.

Output Processing Requirements

This process shall provide the acquired vehicle emissions data to other processes.

Function #2.7: Determine Vehicle Safety

The *Determine Vehicle Safety* process is responsible for determining the safety status of a vehicle (e.g., braking performance, cargo/trailer integrity).

Input Processing Requirements

This process shall acquire the operational safety attributes of a vehicle.

Process and Control Requirements

This process shall assess the safety status of a vehicle based on a specified set of safety criteria.

Output Processing Requirements

This process shall be capable of transmitting the acquired vehicle safety status to other processes.

Function #2.8: Receive Vehicle-to-Infrastructure Communications

The *Receive Vehicle-to-Infrastructure Communications* process is responsible for accepting communications messages from a vehicle. These messages could be of various forms and technologies, including automated Mayday transmitters, cellular phones, RF tags, etc.

Process and Control Requirements

+ This process shall receive the vehicle-to-infrastructure messages.
+ This process shall determine the message type.
+ This process shall assess and filter the contents of the received communications and determine the appropriate receiver(s) of the message.

Output Processing Requirements

This process shall be capable of relaying the received messages to other processes.

5.4.2.3 Function #3: Monitor Environmental Conditions

The *Monitor Environmental Conditions* process gathers environmental information, such as air pollution, weather conditions, and pavement temperatures. Transportation network data shall be used by this process to provide location references for the acquired information. The *Monitor Environmental Conditions* process uses the acquired data to determine high pollution areas, create input for air quality assessments, and formulate input for snow and ice predictions along the road. This environmental information shall be provided to other external entities, including TDM and snow removal management. The environmental conditions monitoring functions are shown in Figure 5-11.

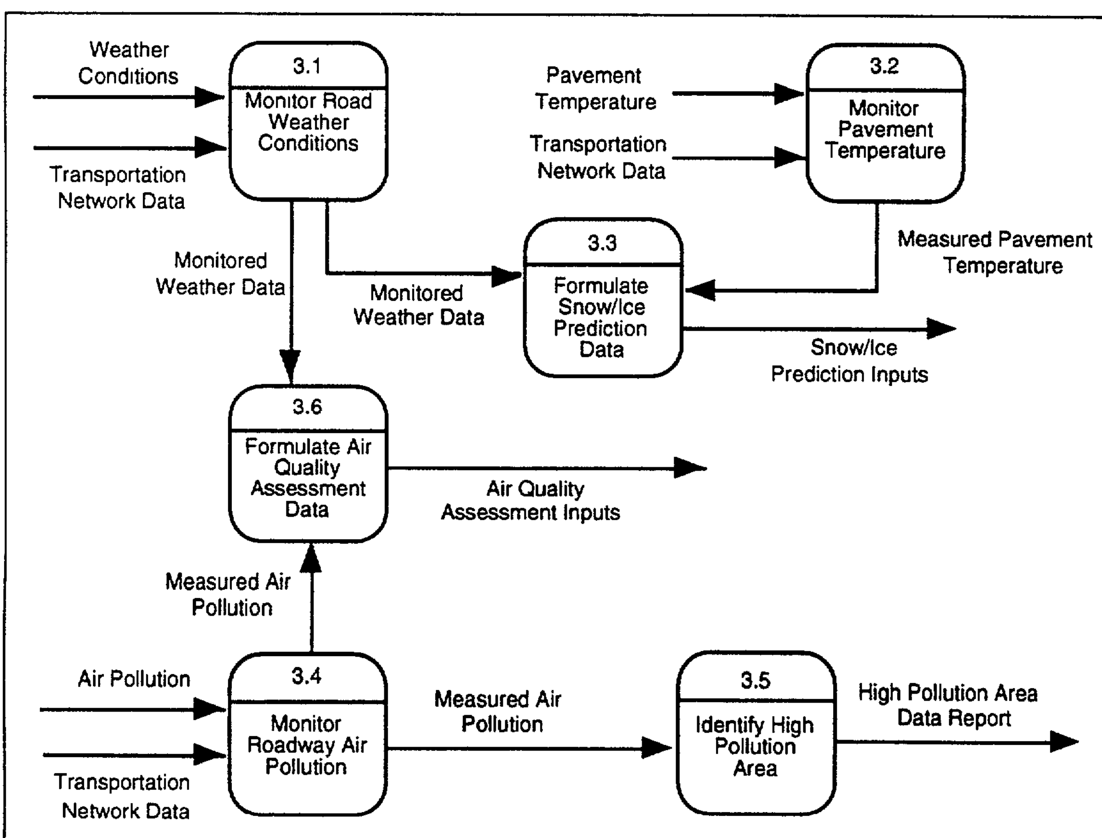

Figure 5-11. Environmental Conditions Monitoring Functions

Function #3.1: Monitor Road Weather Conditions

The *Monitor Road Weather Conditions* process is responsible for monitoring the actual weather conditions along the roads in the Corridor transportation network.

Input Processing Requirements

+ This process shall acquire weather conditions along the designated roads.
+ This process shall accept the transportation network data from a transportation network database.

Process and Control Requirements

This process shall map the weather conditions data to the location reference of the transportation network for road weather conditions monitoring.

Cutout Processing Requirements

This process shall be capable of transmitting the monitored road weather conditions data to other designated processes.

Function #3.2: Monitor Pavement Temperature

The *Monitor Pavement Temperature* process is primarily responsible for determining the temperature of the pavement. These measurements will be used to assist in formulating snow and ice prediction data.

Input Processing Requirements

+ This process shall acquire pavement temperature.
+ This process shall use the transportation network data for location references.

Process and Control Requirements

- This process shall provide measurements of pavement temperature for specified sections of the roadway.
- This process shall organize the pavement temperature measurements according to the transportation network references.

Output Processing Requirements

This process shall be capable of transmitting the measured pavement temperature data to other processes.

Function #3.3: Formulate Snow/Ice Prediction Data

The *Formulate Snow/Ice Prediction Data* process is responsible for compiling the weather and pavement temperature conditions to use for snow/ice predictions.

Input Processing Requirements

- This process shall accept monitored weather data.
- This process shall accept the measured pavement temperature data.

Process and Control Requirements

- This process shall use the monitored weather data and the measured pavement temperature data for roadway snow/ice predictions.
- This process shall generate input for snow/ice predictions according to a predetermined format.

Output Processing Requirements

This process shall be capable of transmitting the snow/ice prediction input data to snow removal management systems (external).

Function #3.4: Monitor Roadway Air Pollution

The *Monitor Roadway Air Pollution* process is responsible for determining the air pollution along the roadway. These measurements shall be used to formulate air quality assessment input.

Input Processing Requirements

+ This process shall acquire air pollution data from the roadway environment.
+ This process shall use the transportation network data for location references.

Process and Control Requirements

+ This process shall provide air pollution measurements at specified roadway locations.
+ This process shall generate roadway air pollution data according to the geographical reference of the transportation network.

Output Processing Requirements

This process shall be capable of transmitting the acquired air pollution data to other processes and external systems.

Function #3.5: Identify High Pollution Areas

The *Identify High Pollution Areas* process is responsible for analyzing the measured air pollution data to identify areas where air pollution concentration exceeds a predetermined threshold.

Input Processing Requirements

- This process shall accept the measured air pollution data.
- This process shall accept and store an air pollution concentration threshold.

Process and Control Requirements

- This process shall analyze the measured air pollution data to identify areas where the air pollution concentration exceeds the threshold.
- This process shall prepare a data report summarizing the location and concentration of air pollution for high pollution areas.

Output Processing Requirements

This process shall be capable of disseminating the high air pollution data report.

Function #3.6: Formulate Air Quality Assessment Data

The *Formulate Air Qualify Assessment Data* process is responsible for providing weather and air pollution data as input to the air quality assessment process (external).

Input Processing Requirements

- This process shall accept monitored weather data.
- This process shall accept the measured air pollution data.

Process and Control Requirements

- This process shall compile all monitored weather data into a format required for air quality assessment.

+ This process shall compile all measured air pollution data into a format required for air quality assessment.

Output Processing Requirements

This process shall be capable of disseminating the air quality assessment input data to external systems.

5.4.2.4 Function #4: Monitor Road Hazards

The *Monitor Road Hazards* process is primarily responsible for detecting the presence of and extracting information regarding hazards that appear in the roadway. Road hazards are grouped as follows: natural and man-made debris hazards (e.g., fallen rocks, mud slides, cargo spillage), pavement/bridge damage hazards (e.g., potholes, surface cracks), and animal hazards (e.g., a deer entering the roadway). Also, externally generated hazard reports (e.g., cellular phone calls) are another mechanism for detecting road hazards. Once the detected hazard is verified, the *Monitor Road Hazards* process shall generate a roadway hazard report to be distributed to appropriate external entities. The road hazards monitoring functions are shown in Figure 5-12.

Function #4.1: Detect Debris on Road

The *Detect Debris on Road* process is responsible for providing the data to determine the existence of debris on the monitored roadway.

Input Processing Requirements

This process shall acquire debris data from the roadway environment.

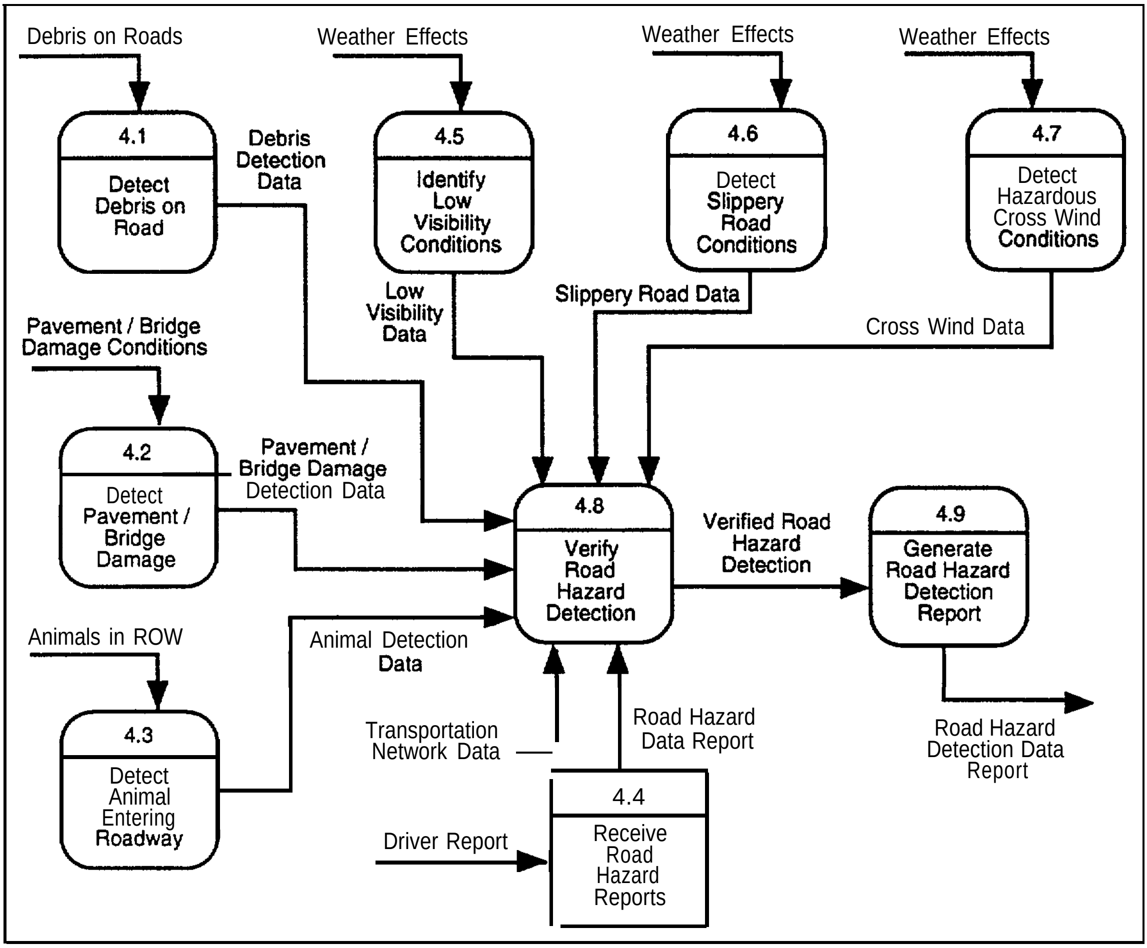

Figure 5-12. Required Road Hazards Monitoring Functions

<u>Process and Control Requirements</u>

+ This process shall be capable of detecting the existence of roadway debris based on the sensed roadway environment data.

+ This process shall be capable of determining and recording the time, location, size, and type of debris.

Output Processing Requirements

+ This process shall generate debris detection data according to a predefined format.

+ This process shall be capable of transmitting the debris detection data to other processes for verification, if necessary.

Function #4.2: Detect Pavement/Bridge Damage

The *Detect Pavement/Bridge Damage* process is responsible for providing the data to determine the existence of pavement/bridge damage that could impede the flow of traffic or pose a potential hazard to the traveling public.

Input Processing Requirements

This process shall acquire pavement/bridge damage data from the roadway.

Process and Control Requirements

+ This process shall be capable of detecting pavement/bridge damage based on the sensed roadway environment data.

+ This process shall be capable of determining and recording the time, location, size, and type of the pavement/bridge damage.

Output Processing Requirements

+ This process shall generate pavement/bridge damage detection data according to a predefined format.

+ This process shall be capable of transmitting the pavement/bridge damage detection data to other processes for verification, if necessary.

Function #4.3: Detect Animal Entering Roadway

The *Detect Animal Entering Roadway* process is responsible for providing data to determine the presence of animals within the right-of-way of the monitored roadway.

Inout Processing Requirements

This process shall acquire animal presence data from the roadway environment.

Process and Control Requirements

+ This process shall be capable of detecting animals in dangerous proximity to the roadway based on the sensed roadway environment data.
+ This process shall be capable of determining and recording the time, location, and frequency of animal detection.

Output Processing Requirements

+ This process shall generate animal detection data according to a predefined format.
+ This process shall be capable of transmitting the animal detection data to other processes for verification, if necessary.

Function # 4.4: Receive Road Hazard Reports

The *Receive Road Hazard Reports* process is responsible for accepting and formatting road hazard reports originating from sources other than the surveillance sensors (e.g., phone calls from work crews or motorists).

Input Processing Requirements

This process shall accept road hazard reports from people.

Process and Control Requirements

- This process shall be capable of accepting and organizing the road hazard report data to fit a predefined format.

- This process shall be capable of recording the time, location, and type of the road hazard that is reported.

Output Processing Requirements

- This process shall create road hazard report data according to a predefined format.

- This process shall be capable of transmitting the road hazard report data to another process for verification, if necessary.

Function #4.5: Identify Low Visibility Conditions

The *Identify Low Visibility Conditions* process is responsible for determining the location along the roadway where visibility conditions are dangerous for driving.

Input Processing Requirements

- This process shall sense the weather and environmental conditions (dust, fog, etc.) along the roadway.

- This process shall determine the weather and environmental parameters that affect driving visibility.

Process and Control Requirements

- This process shall be capable of assessing visibility based on acquired weather and environmental conditions data.

+ This process shall be capable of comparing measured visibility data with a pre-set threshold to aid in determining low visibility conditions.

+ This process shall be capable of recording time, location, and measured visibility data.

Output Processing Requirements

+ This process shall generate low driving visibility data according to a predefined format.

+ This process shall be capable of transmitting low visibility condition data to other processes for verification, if necessary.

Function #4.6: Detect Slippery Road Conditions

The *Detect Slippery Road Conditions* process is responsible for detecting and locating slippery road conditions (e.g., wet or icy road surface, or spillage of oil and other chemicals).

Input Processing Requirements

This process shall sense the road surface and weather conditions for detecting slippery road conditions.

Process and Control Requirements

+ This process shall determine the road surface conditions (surface temperature, moisture measurement, etc.) based on the acquired road surface and weather data.

+ This process shall be capable of comparing the road surface conditions data with a pre-set threshold to determine the presence of slippery areas on the roadway.

Output Processing Requirements

+ The slippery road data shall include the assessed road surface conditions data and location reference data.

+ This process shall organize slippery road data to a predefined format.

+ This process shall be capable of transmitting the slippery road data to other processes for verification, if necessary.

Function #4.7: Detect Hazardous Cross Wind Conditions

The *Detect Hazardous Cross Wind Conditions* process is responsible for determining crosswind locations, speeds, and directions that are potentially hazardous to traffic.

Input Processing Requirements

This process shall acquire wind conditions data along the roadway.

Process and Control Requirements

+ This process shall measure the wind speed and wind direction at designated locations along the roadway.

+ This process shall be capable of comparing the measured cross wind conditions data with pre-set thresholds to determine the presence of dangerous cross wind areas along the roadway.

Output Processing Requirements

+ This process shall generate dangerous cross wind conditions data according to a predefined format.

- The cross wind conditions data shall include the measured wind speed, estimated wind direction, and the affected location along the roadway.

- This process shall be capable of transmitting the dangerous cross wind detection data to other processes for verification, if necessary.

Function #4.8: Verify Road Hazard Detection

The *Verify Road Hazard Detection* process is responsible for verifying all incoming data and reports to ensure the validity of the road hazard before further responses are undertaken.

Input Processing Requirements

- This process shall accept the following road hazard detection data: animal entering roadway, debris on roadway, pavement damage, reports from people, low visibility, slippery road, and cross wind.

- This process shall be capable of simultaneously accepting road hazard data from multiple sources.

- This process shall accept transportation network data from the transportation network database.

Process and Control Requirements

- This process shall be capable of locating the detected road hazards within the transportation network.

- This process shall verify all road hazard detection reports data through internal (e.g., correlation of available data) and external means (e.g., a call from the police).

Output Processing Requirements

- This process shall produce verified road hazard detection data according to a predefined format.

- The verified road hazard detection data shall include hazard type, location, time of detection, and potential traffic and safety impacts.

- This process shall be capable of providing verified road hazard detection data to another process for generating a road hazard detection data report.

Function #4.9: Generate Road Hazard Detection Report

The *Generate Road Hazard Detection Report* process is responsible for creating a road hazard detection data report based on the verified road hazard detection data.

Input Processing Requirements

- This process shall accept verified road hazard detection data.

- This process shall be initiated only when verified road hazard detection data is received.

Process and Control Requirements

- This process shall organize the verified road hazard detection data according to a predefined format for reporting purposes.

- At the time of reporting, this process shall combine all available road hazard detection data into a single data packet, if appropriate.

Output Processing Requirements

- The verified road hazard detection data report shall include hazard type, location, and time of detection for each hazard detected.

- This process shall be capable of transmitting the road hazard detection data report to other systems for generating traveler advisory information or initiating hazard removal responses.

5.4.2.5 Function #5: Monitor Parking Facilities

The *Monitor Parking Facilities* process is responsible for gathering the parking facility usage data and parking charge input data. Parking facility usage data is based primarily on the parking entry and exit counts and times, as well as transportation network data and vehicle occupancy information. Parking charge input is formulated from the vehicle's entry and exit times, occupancy, and vehicle identification. Some of these vehicle attributes may be contained in the vehicle communication messages (e.g., RF tags). The parking monitoring data shall be provided to external entities such as the Transportation Planning System, Intermodal Management System, and the TIS. The parking facility monitoring functions are shown in Figure 5-13.

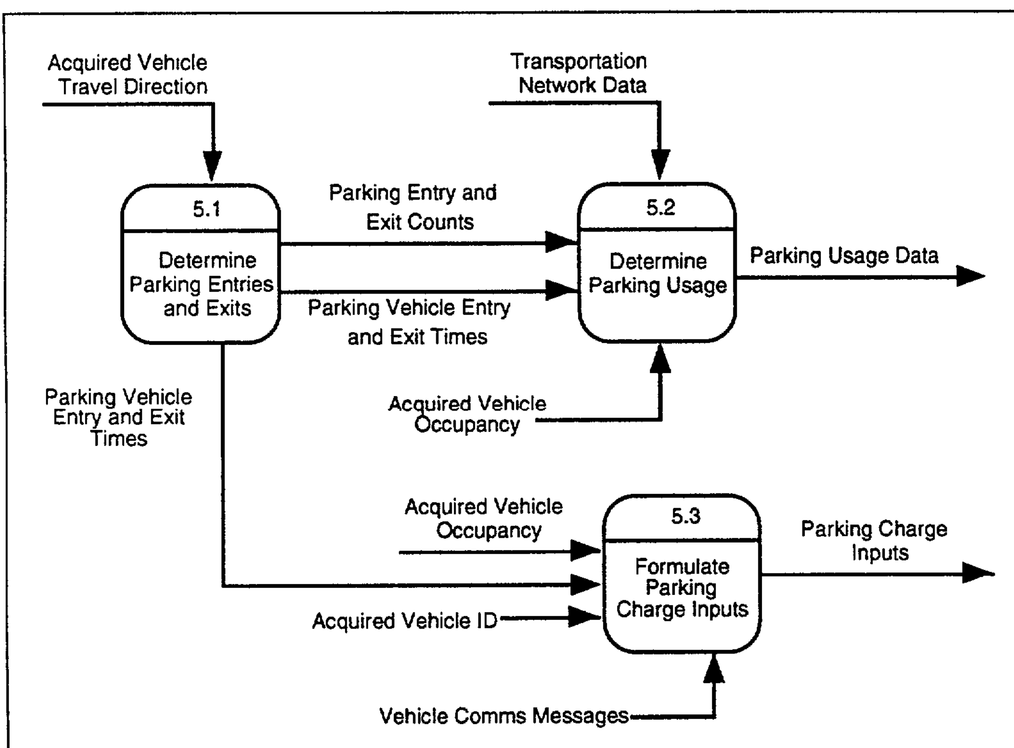

Figure 5-13. Required Parking Facility Monitoring Functions

Function #5.1: Determine Parking Entries and Exits

The *Determine Parking Entries and Exits* process is primarily responsible for detecting and counting vehicles entering and exiting parking facilities.

Input Processing Requirements

This process shall accept the acquired vehicle travel direction provided by another process to determine the number of vehicle entries and exits.

Process and Control Requirements

- This process shall detect an entry by a vehicle to the parking facilities.
- This process shall detect an exit by a vehicle from the parking facilities.
- When an entry by a vehicle to the parking facilities is detected, this process shall record the time of entry.
- When an exit by a vehicle to the parking facilities is detected, this process shall record the time of exit.
- This process shall keep a current record of the parking entry and exit counts.
- This process shall keep a current record of the parking entry and exit times.

Output Processing Requirements

+ This process shall be capable of providing the parking entry and exit counts to other processes.
+ This process shall be capable of providing the parking entry and exit times to other processes.

Function #5.2: Determine Parking Usage

The *Determine Parking Usage process* is responsible for generating parking usage statistics (parking availability, parking vehicle occupancy, time of use, etc.) for use in TDM, transportation planning, intermodal coordination, and TIS.

Input Processing Requirements

- This process shall accept parking entry and exit counts.
- This process shall accept parking entry and exit times.
- This process shall accept the transportation network data from the transportation network database.

Process and Control Requirements

- This process shall determine (in real time) parking availability for each monitored parking facility.
- The process shall generate parking usage data, including parking demand and availability by time of day, and parking vehicle occupancy.

Output Processing Requirements

- This process shall organize and store parking usage data according to a predefined format.
- This process shall be capable of providing the parking usage data to other systems.

Function #5.3: Formulate Parking Charge Input

The *Formulate Parking Charge Input* process is responsible for gathering vehicle-related information to be input to parking fees determination for a vehicle.

Input Processing Requirements

- This process shall accept the acquired vehicle occupancy (persons per vehicle) data.
- This process shall accept the acquired vehicle identification data.
- This process shall accept the vehicle communications data (e.g., electronic tags).
- This process shall accept the vehicle parking entry and exit time data.

Process and Control Requirements

This process shall formulate parking charge input according to a predefined format using the acquired vehicle occupancy, identification, communications, and parking entry and exit time data.

Output Processing Requirements

This process shall be capable of providing the parking charge input data to external systems.

5.4.2.6 Function #6: Monitor Transportation Law Violation

The *Monitor Transportation Law Violation* process shall accept the acquired attributes of a vehicle (speed, weight, occupancy, etc.), law enforcement parameters, and transportation network data to determine if a transportation law is violated. All outputs from this process are data reports (speed violation data report, weight violation data report, etc.) which are then provided to the law enforcement external entity. The transportation law violation monitoring functions are shown in Figure 5-14.

Function #6.1: Determine Speed Violation

The *Determine Speed Violation* process is responsible for determining if a vehicle has exceeded the speed limit.

Input Processing Requirements

+ This process shall accept the acquired vehicle speed data.

+ This process shall accept the acquired vehicle identification data.

+ This process shall accept the acquired vehicle travel direction data.

+ This process shall accept the acquired vehicle location data.

+ This process shall accept the regulated vehicle speed limit data.

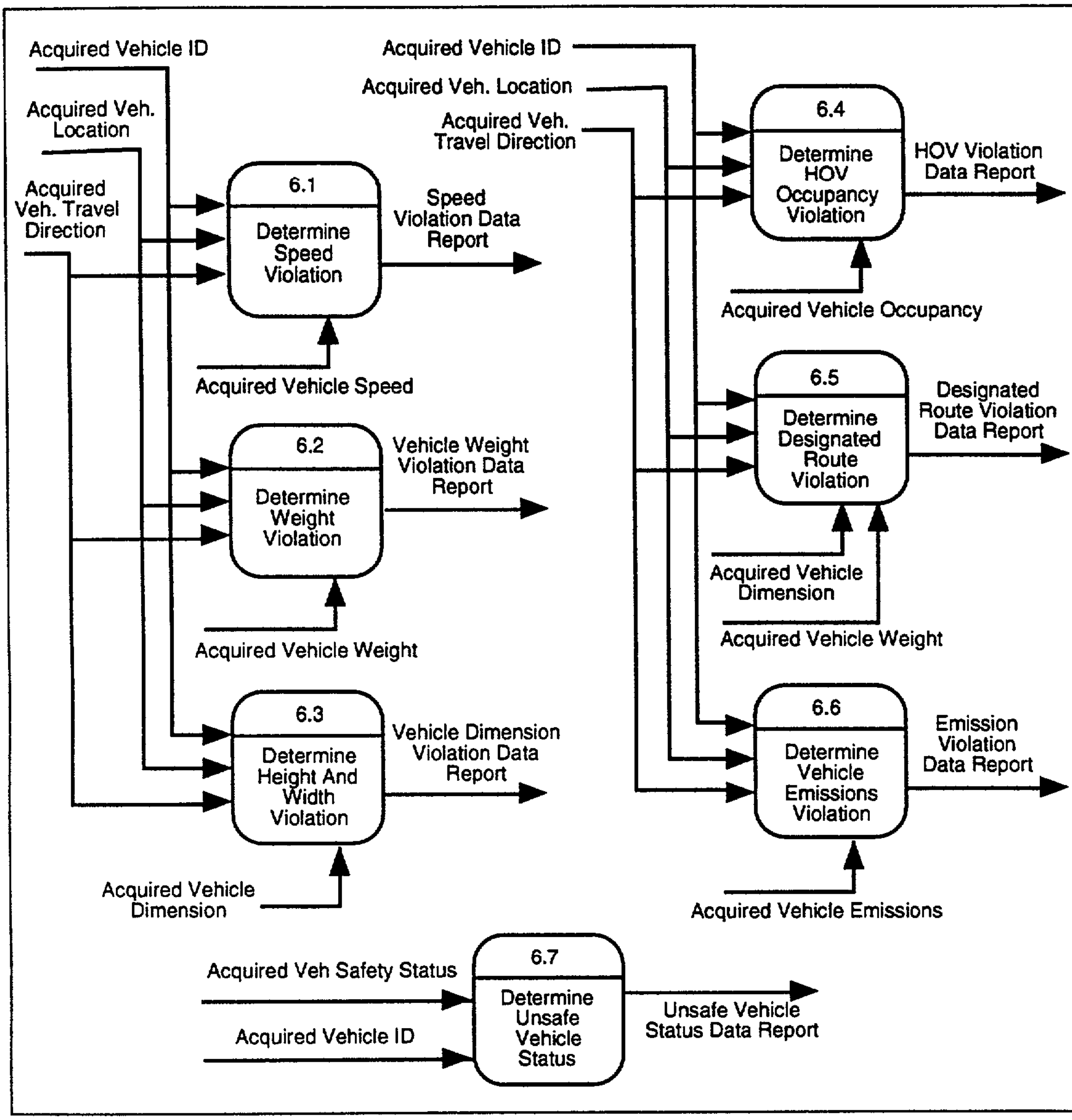

Figure 5-14. Required Transportation Law Violation Monitoring Functions

<u>Process and Control Requirements</u>

- This process shall determine if the vehicle has violated speed limit laws.
- If a speed limit violation occurs, this process shall generate a vehicle speed violation data report which includes the acquired vehicle speed, identification, the acquired travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the vehicle speed limit violation data report to an external law enforcement system.

Function #6.2: Determine Weight Violation

The Determine Weight Violation process is responsible for determining if a vehicle has violated weight limit laws.

Input Processing Requirements

+ This process shall accept the acquired vehicle weight data.
+ This process shall accept the acquired vehicle identification data.
+ This process shall accept the acquired vehicle travel direction data.
+ This process shall accept the acquired vehicle location data.
+ This process shall accept the regulated vehicle weight limit data.

Process and Control Requirements

+ This process shall determine if the vehicle has violated weight limit laws.
+ If a weight limit violation occurs, this process shall generate a vehicle weight violation data report which includes the acquired vehicle weight, identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the vehicle weight limit violation data report to an external law enforcement system.

Function #6.3: Determine Height and Width Violation

The *Determine Height and Width Violation* process is responsible for determining if a vehicle has violated any dimension-related traffic laws.

Input Processing Requirements

+ This process shall accept the acquired vehicle dimension data.
+ This process shall accept the acquired vehicle identification data.
+ This process shall accept the acquired vehicle travel direction data.
+ This process shall accept the acquired vehicle location data.
+ This process shall accept the regulated vehicle dimension limit data.

Process and Control Requirements

+ This process shall determine if the vehicle has violated dimension limit laws.
+ If a dimension limit violation occurs, this process shall generate a dimension violation data report which includes the acquired vehicle dimensions, identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the height and width violation data report to an external law enforcement system.

Function #6.4: Determine HOV Occupancy Violation

The Determine *HOV* Occupancy *Violation* process is responsible for determining if a vehicle has violated any occupancy-related traffic laws.

Input Processing Requirements

+ This process shall accept the acquired vehicle occupancy data.
+ This process shall accept the acquired vehicle identification data.
+ This process shall accept the acquired vehicle travel direction data.
+ This process shall accept the acquired vehicle location data.
+ This process shall accept the regulated vehicle occupancy limit data.

Process and Control Requirements

+ This process shall determine if the vehicle has violated any vehicle occupancy laws.
+ If an HOV violation occurs, this process shall generate an HOV violation data report which includes the acquired vehicle occupancy, identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the HOV violation data report to an external law enforcement system.

Function #6.5: Determine Designated Route Violation

The *Determine Designated Route Violation* process is responsible for determining if a vehicle has violated any designated route traffic laws.

Inout Processing Requirements

+ This process shall accept the acquired vehicle weight data.
+ This process shall accept the acquired vehicle dimension data.

+ This process shall accept the acquired vehicle identification data.

+ This process shall accept the acquired vehicle travel direction data.

+ This process shall accept the acquired vehicle location data.

+ This process shall accept the special route data.

Process and Control Requirements

+ This process shall determine if the vehicle has violated any designated route laws.

+ If a designated route violation occurs, this process shall generate a designated route violation data report which includes the acquired vehicle weight, dimensions, identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the designated route violation data report to an external law enforcement system.

Function #6.6: Determine Vehicle Emissions Violation

The *Determine Vehicle Emissions Violation* process is responsible for determining if a vehicle has violated any emissions-related laws.

Input Processing Requirements

+ This process shall accept the acquired vehicle emissions data.

+ This process shall accept the acquired vehicle identification data.

+ This process shall accept the acquired vehicle travel direction data.

+ This process shall accept the acquired vehicle location data.

+ This process shall accept the regulated emissions limit data.

Process and Control Requirements

- This process shall determine if the vehicle has violated any emissions laws.
- If an emissions violation occurs, this process shall generate a vehicle emissions violation data report which includes the acquired vehicle emissions (quantity and type), identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the vehicle emissions violation data report to an external law enforcement system.

Function #6.7: Determine Unsafe Vehicle Status

The *Determine Unsafe Vehicle* Status process is responsible for determining if the operational status of a vehicle is unsafe (e.g., failing braking system).

Input Processing Requirements

- This process shall accept the acquired vehicle safety status data.
- This process shall accept the acquired vehicle identification data.
- This process shall accept the acquired vehicle travel direction data.
- This process shall accept the acquired vehicle location data.
- This process shall accept the vehicle safety criteria data.

Process and Control Requirements

- This process shall determine if the vehicle fails to meet any safety criteria.

+ If a safety criterion is not met, this process shall generate an unsafe vehicle status data report which includes the acquired vehicle safety status, the violated safety criteria, and the acquired vehicle identification, travel direction, and location.

Output Processing Requirements

This process shall be capable of providing the unsafe vehicle status data report to an external law enforcement system.

5.4.2.7 Function #7: Monitor Travel Security

The *Monitor Travel* Security process primarily is responsible for monitoring and detecting any traveler security events at intermodal transfer points, on public transit vehicles, and at parking facilities. The detected security event data is then provided to an external incident management entity for further analysis and response. The travel security monitoring functions are shown in Figure 5-I 5.

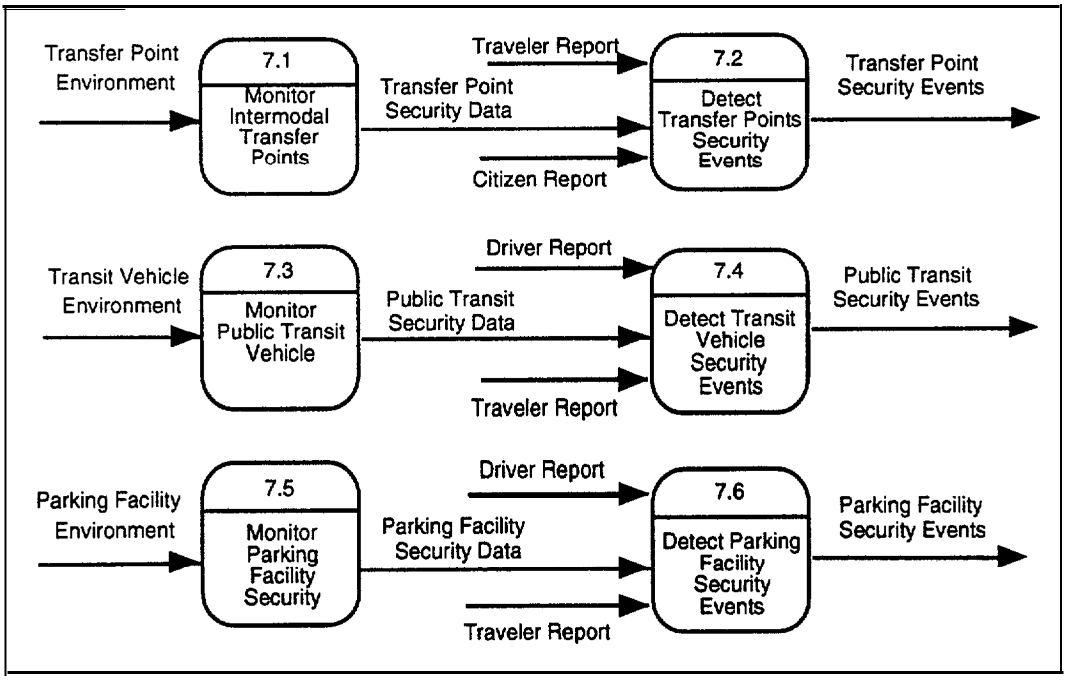

Figure 5-15. Required Travel Security Monitoring Functions

Function #7.1: Monitor Intermodal Transfer Points

The *Monitor Intermodal* Transfer *Points* process is responsible for monitoring the physical environment at intermodal transfer facilities for detecting traveler security incidents.

Input Processing Requirements

This process shall continuously acquire travel surrounding data from intermodal transfer facilities.

Process and Control Requirements

+ This process shall provide specific location references to the travel surrounding data acquired from intermodal transfer facilities.
+ In the event of a security incident, this process shall have the capability to acquire detailed information about the incident and provide continuous updates of the incident progress.

Output Processing Requirements

+ This process shall be capable of providing the travel surrounding data at transfer points to the security incident detection process.
+ This process shall be capable of continuously providing transfer point security event updates to a traveler security incident management system.

Function #7.2: Detect Transfer Point Security Events

The *Detect Transfer Point Security Events* process is responsible for detecting any traveler security incidents at an intermodal transfer point.

Input Processing Requirements

+ This process shall accept the transfer point security monitoring data.

+ This process shall accept security incident report (or notification) from a traveler who may or may not be the victim.

+ This process shall accept security incident report (or notification) from a citizen.

Process and Control Requirements

+ This process shall analyze the transfer point security monitoring data to detect any security incidents at intermodal transfer points.

+ This process shall be capable of recording specific information regarding security incidents, including time and location of occurrence, and type of incident.

Output Processing Requirements

This process shall be capable of providing the transfer point security event data to a traveler security incident management system.

Function #7.3: Monitor Public Transit Vehicle

The *Monitor Public Transit Vehicle* process is responsible for monitoring the physical environment on public transit vehicles for the purpose of detecting traveler security incidents.

Input Processing Requirements

This process shall continuously acquire travel surrounding data on public transit vehicles.

Process and Control Requirements

- ♦ This process shall provide specific location references, as appropriate, to the travel surrounding data acquired from public transit vehicles (e.g., rail car number).
- ♦ This process shall provide the exact location of the incident vehicle within the transportation network.
- ♦ In the event of a security incident, this process shall have the capability to acquire detailed information about the incident and provide continuous updates of the incident progress.

Output Processing Requirements

- + This process shall be capable of providing the travel surrounding data on public transit vehicles to the security incident detection process.
- + This process shall be capable of continuously providing transit vehicle security event updates to a traveler security incident management system.

Function #7.4: Detect Transit Vehicle Security Events

The *Detect Transit Vehicle Security Events* process is responsible for detecting any security incidents on a public transit vehicle.

Input Processing Requirements

- + This process shall accept the public transit vehicle security monitoring data.
- + This process shall accept security incident report (or notification) from the driver.
- + This process shall accept security incident report (or notification) from a traveler (i.e., a transit user) who may or may not be the victim.

Process and Control Requirements

- This process shall analyze the public transit vehicle security monitoring data to detect any security incidents on the vehicle.
- This process shall be capable of recording specific information regarding security incidents, including time and location of occurrence, type of incident, and location of the vehicle.

Output Processing Requirements

This process shall be capable of providing the public transit vehicle security events data to a traveler security incident management system.

Function #7.5: Monitor Parking Facility Security

The *Monitor Parking Facility Security* process is responsible for monitoring the physical environment at parking facilities for detecting traveler security incidents.

Input Processing Requirements

This process shall continuously acquire travel surrounding data from parking facilities.

Process and Control Requirements

- This process shall provide specific location references to the travel surrounding data acquired from parking facilities.
- In the event of a security incident, this process shall have the capability to acquire detailed information about the incident and provide continuous updates of the incident progress.

Output Processing Requirements

- This process shall be capable of providing the travel surrounding data at parking facilities to the security incident detection process.
- This process shall be capable of continuously providing security event updates at parking facilities to a traveler security incident management system.

Function #7.6: Detect Parking Facility Security Events

The Detect Parking Facility Security Events process is responsible for detecting any traveler security incidents at a parking facility.

Input Processing Requirements

- This process shall accept the parking facilities' security monitoring data.
- This process shall accept security incident report (or notification) from a traveler who may or may not be the victim.
- This process shall accept security incident report (or notification) from a driver.

Process and Control Requirements

- This process shall analyze the parking facilities' security monitoring data to detect any security incidents at those facilities.
- This process shall be capable of recording specific information regarding the security incidents, including time and location of occurrence, and type of incident.

Output Processing Requirements

This process shall be capable of providing the parking facility security events data to a traveler security incident management system.

5.4.2.8 Function #8: Maintain Support Databases

The *Maintain Support Databases* process shall accept and perform updates to the road, route, parking, transfer point, surveillance asset, and transportation network databases. Typical updates include map, transit route, truck route, parking facility, surveillance asset, and transfer point facility data. The updated data are stored in the transportation network database to be used by many Corridor Surveillance System processes. This process is also responsible for updating and maintaining the tracked vehicle database, which contains the tracked vehicle identification data used to acquire vehicle location and tracking data. The support database maintenance functions are shown in Figure 5-16.

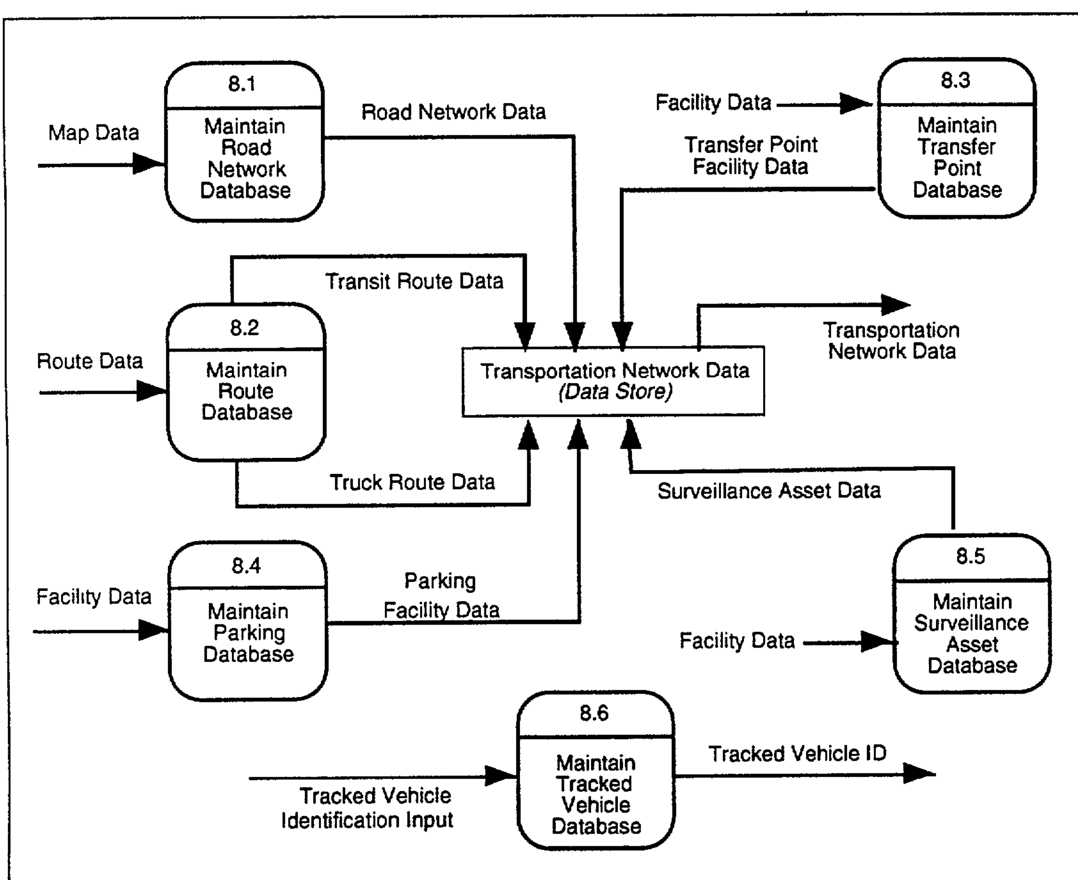

Figure 5-16. Required Support Database Maintenance Functions

Function #8.1: Maintain Road Network Database

The *Maintain Road Network Database* process is responsible for receiving updated road network data and maintaining the road network database for use by other processes in the system.

Input Processing Requirements

This process shall accept new or updated map data (updated road geometric and geographic information, construction areas, etc.).

Process and Control Requirements

+ This process shall update the road network database using the new map data.
+ This update shall occur whenever new map data is available.

Output Processing Requirements

+ This process shall provide the road network data to specified internal processes.
+ This process shall update the transportation network database with the road network data.

Function #8.2: Maintain Route Database

The *Maintain Route Database* process is responsible for updating and maintaining the route database including, but not limited to, transit and truck route data.

Input Processing Requirements

This process shall accept new or updated route data.

Process and Control Requirements

- This process shall update the route database using the new route data.
- This process shall distinguish route data by mode and/or application.
- This update shall occur whenever new route data is available.

Output Processing Requirements

- This process shall provide the transit route data to specified processes.
- This process shall provide the truck route data to specified processes.
- This process shall update the transportation network database with the transit route data.
- This process shall update the transportation network database with the truck route data.

Function #8.3: Maintain Transfer Point Database

The *Maintain Transfer Point Database* process is responsible for updating and maintaining the transfer point database which includes geographical location and identification data, and a facility description.

Input Processing Requirements

This process shall accept new or updated transfer-facility data.

Process and Control Requirements

- This process shall update the transfer point database using the new data.
- This update shall occur whenever new transfer-facility data is available.

Output Processing Requirements

- This process shall provide the transfer point data to specified internal processes.
- This process shall update the transportation network database with the new transfer-facility data.

Function #8.4: Maintain Parking Database

The *Maintain Parking Database* process is responsible for updating and maintaining the parking database which includes facility location, identification, capacity, and fee-determination criteria data.

Input Processing Requirements

This process shall accept new or updated parking data.

Process and Control Requirements

- This process shall update the parking database using the new data.
- This update shall occur whenever new parking data is available.

Output Processing Requirements

- This process shall provide the parking facility data to specified internal processes.
- This process shall update the transportation network database with the new parking data.

Function #8.5: Maintain Surveillance Asset Database

The *Maintain Surveillance Asset Database* process is responsible for updating and maintaining the surveillance asset database which includes equipment type, location, and operational status data.

Input Processing Requirements

This process shall accept new or updated surveillance asset data.

Process and Control Requirements

- This process shall update the surveillance asset database according to the new data.
- This update shall occur whenever new surveillance asset data is available.

Output Processing Requirements

- This process shall provide the surveillance asset data to specified internal processes.
- This process shall update the transportation network database with the new surveillance asset data.

Function #8.6: Maintain Tracked Vehicle Database

The *Maintain Tracked Vehicle Database* process is responsible for updating and maintaining the tracked vehicle database which includes vehicle identification and type.

Input Processing Requirements

This process shall accept new or updated tracked vehicle identification input.

Process and Control Requirements

+ This process shall update the tracked vehicle database using the tracked vehicle identification input.

+ This update shall occur whenever new tracked vehicle data are available.

Output Processing Requirements

This process shall provide the tracked vehicle identification to specified processes.

These eight functional requirements of the I-95 Corridor-wide Surveillance System form a foundation upon which communications, interface, hardware, and software requirements were developed. Because the latter requirements were more technology- and design-oriented, a definition of a surveillance system hierarchy for the Corridor was needed to facilitate their development. This system hierarchy is presented in Section 5.5.

5.5 SYSTEM HIERARCHY

To define the communications, hardware and software, and interface requirements, a hierarchical structure of the I-95 Corridor-wide Surveillance System was developed. This section describes an assumed system hierarchical structure based on the study team's knowledge of the Corridor's plan for creating regional communications centers, the existing traffic management system structures of some Corridor-member agencies, and the directions in national traffic management system development. The system hierarchical structure consists of three levels (field, state and local operations center, and Corridor) as shown in Figure 5-17. The details of each level are described below.

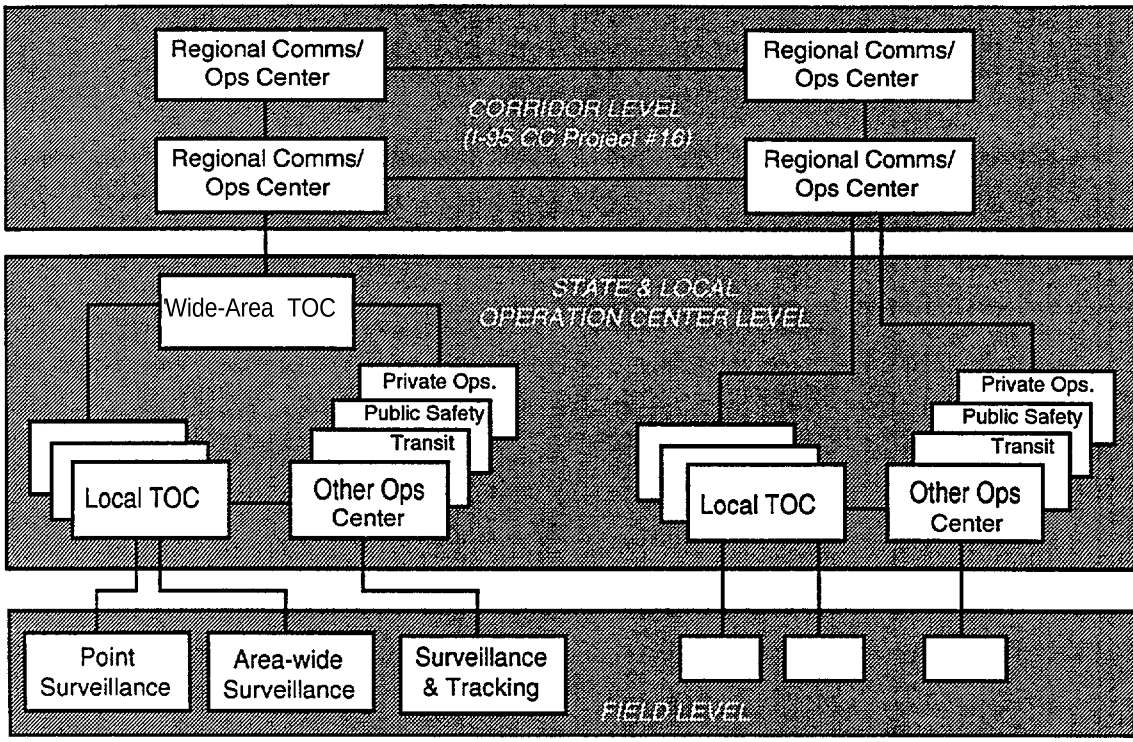

Figure 5-17. I-95 Corridor-Wide Surveillance System Hierarchy

5.5.1 Field Level

This lowest level component includes the various traffic and environmental sensors deployed in the field. The sensors may generate point or wide-area information. Point information is defined as the individual data supplied by point detectors (e.g., traffic detectors or pavement temperature sensors). Wide-area information is defined as any information for an extended section of the roadway, such as link travel speed from vehicle probes, or information provided by an aerial surveillance platform.

Within the field, a communication network brings the sensor data from the field to the local TMC as shown in Figure 5-18. The raw data are processed at the field level, and transported to the local TMC, either directly (e.g., aerial surveillance data) or through intermediate nodes of controllers. Some of these nodes may be collection points where several controllers are connected together and transmit data to the TMC through a trunk line.

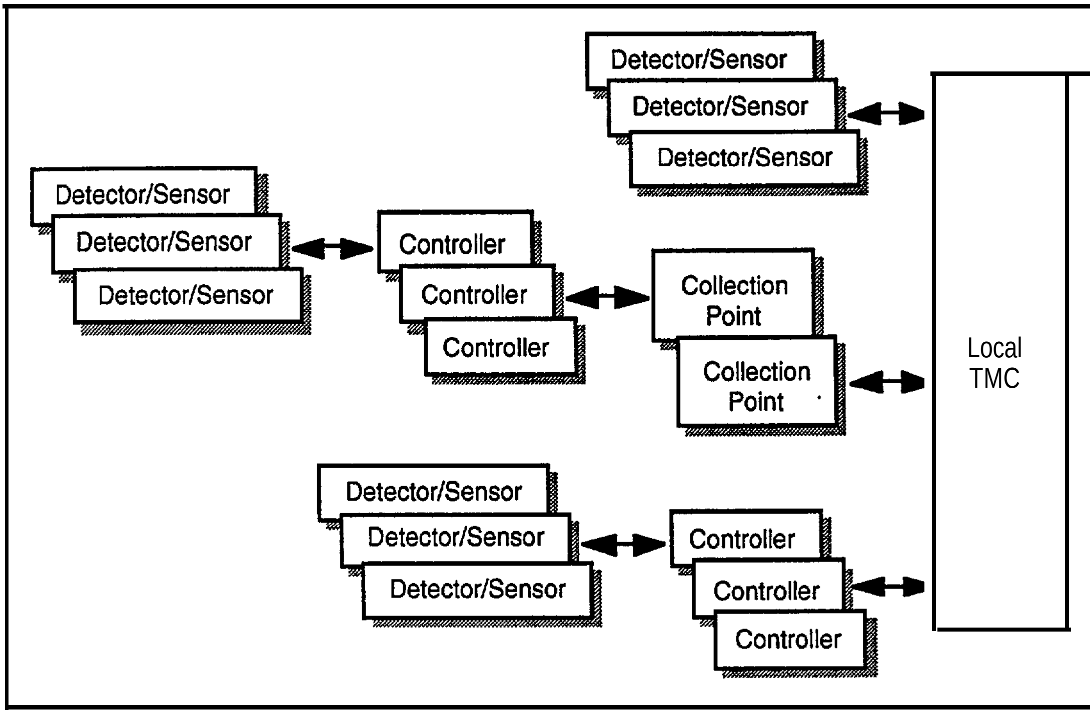

Figure 5-18. Functional Hierarchy of a Field-Level System

5.5.2 State and Local Operations Center Level

State and Local operations centers acquire and process surveillance data from the field. Depending on the functions of the operations center, the acquired data may be directly applied to traffic management (e.g., traffic sensor data collected by the local TMC), or may be utilized as surveillance information (e.g., vehicle tracking data acquired by public transit or commercial fleet operators). From the perspective of the local TMC, the various sources of information are shown in Figure 5-19.

The system hierarchy at this level may inculde two configurations as shown in Figure 5-18. The first configuration may be a wide-area TMC (e.g., state-wide or a metropolitan-wide TMC) **that** receives information from the local TMC or modal operations centers and coordinates activities with these local centers. The wide-area TMC is linked with a regional communications/operations center and shares regional information with its local peers. The Maryland State-wide Operations Center (SOC) is one such facility. Physically, a wide-area TMC may be a separate facility or a local TMC. Such a center is supposed to encourage cooperation among different jurisdictions through information sharing and coordinated traffic management strategies.

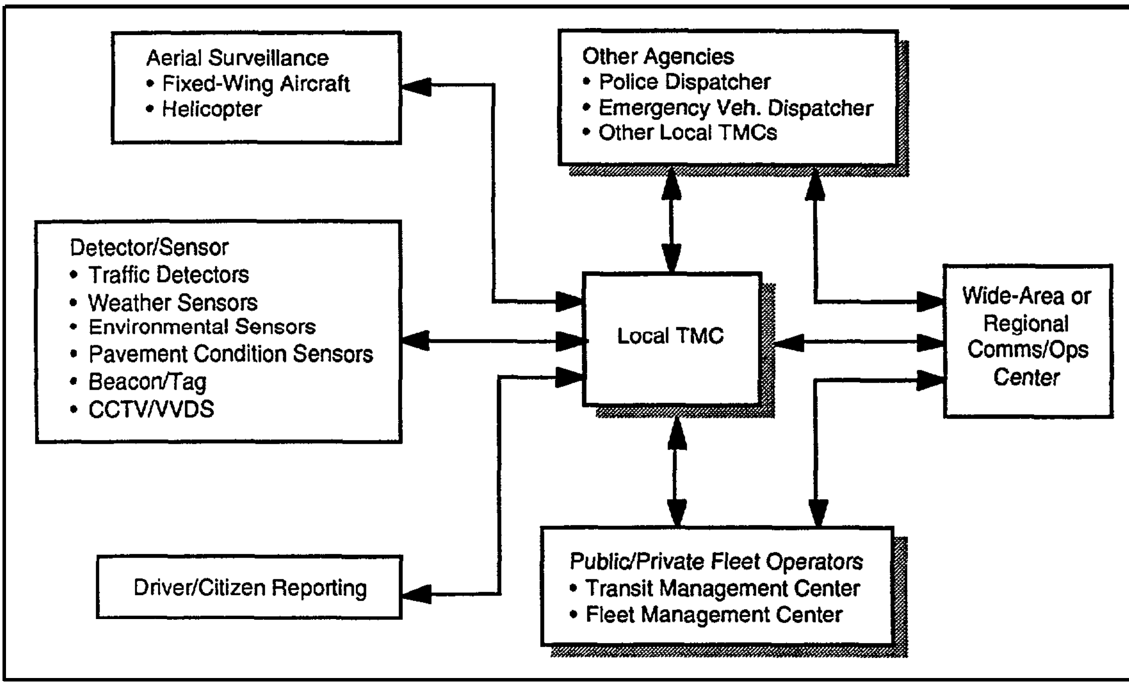

Figure 5-19. TMC Interfaces with Other Entities

This concept of a wide-area TMC is consistent with the FHWA's architecture for ATMS (under the "Design of ATMS Support Systems" Contract being performed by Loral). This architecture defines an ATMS to be an integration of TMCs in a metropolitan area. Each TMC acts as an individual node of a regional Wide Area Network (WAN) and has peer-to-peer communications with other TMCs. The architecture identifies a Wide Area Traffic Management (WATM) node to be located at one of the peer TMCs. The WATM is responsible for:

+ Prediction of region-wide traffic.

+ Development of area-wide strategies for a proactive traffic control.

+ Transmission of demand forecasts and control strategies to other participating nodes.

Figure 5-20 illustrates the concept of WATM, where five cooperating TMCs in a region form a network for data exchange. Only one TMC is provided with the WATM capability for inter-jurisdictional coordination.

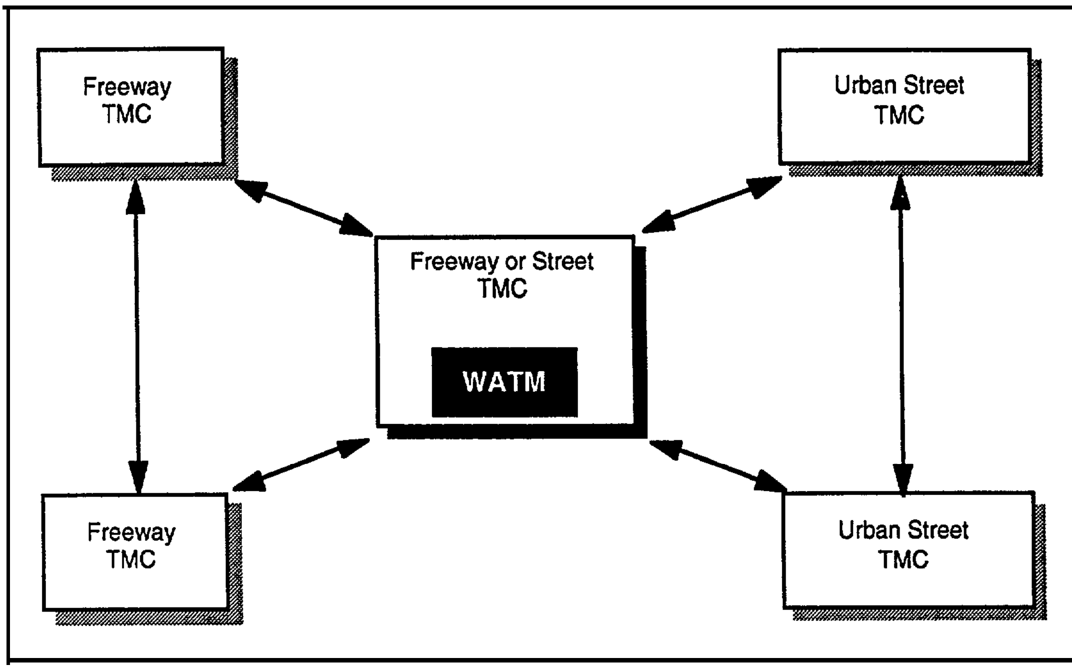

Figure 5-20. Wide Area Traffic Management Concept

The second system hierarchy configuration is a direct communication between a local TMC or a modal agency's operations center and the regional communications/operations center. This configuration may be found in areas that are near a regional communications/operations center.

5.5.3 Corridor Level

At the Corridor level, the highest level of the system hierarchy, the Corridor will have regional information exchange centers. These centers will be initiated by implementing of the l-95 CC Project 16 (Feasibility of Regional Communications/Operations Centers). As described in the Coalition's *Business f/an,* Project 16 will include a feasibility study of four regional communications/operations centers that cover the following regions:

+ New York/New Jersey.
+ Washington/Baltimore/Northern Virginia.
+ Philadelphia/Camden/Wilmington.
+ Boston/Providence.

Each regional communications/operations center will exchange information with local and wide-area operations centers within its region, and with other regional centers either inside or outside of the Corridor. The surveillance information collected from the field level must, therefore, be processed and transmitted appropriately through this system hierarchy to be used at the Corridor level.

5.6 COMMUNICATIONS AND INTERFACE REQUIREMENTS

The I-95 Corridor-wide Surveillance System will require the support of many different elements, beginning with the field and ending at a control center. The field elements include traffic count and flow detector, weather and pavement condition, and WIM stations, video surveillance units, and so on. The control center includes mainly computers, workstations, and communication interface equipment.

In general, two types of information will be transmitted over a surveillance communications network - data and video images. The transmission requirements for each type dictate the interface, software, hardware, and communications requirements for the system as follows:

+ Data Traffic control system data communications have traditionally been low-speed (i.e., 1200 baud or less) using relatively inexpensive, special-purpose communication and control interface devices. The data requirements for the system will include detector and control data. Detector data, such as traffic count and speed, plus detector status information will be transmitted to the control center from each station once every 30 seconds. Approximately 16 detector stations can be supported by a single, 1200 bps, full-duplex channel. Control data, such as those that enable the pan, tilt, zoom, focus, and iris functions of CCTV cameras, will be transmitted through a full-duplex channel for near real-time operations.

+ Video Images. Real-time, video images from CCTV cameras place the heaviest load on the communications network. Specifically, full-motion video requires a service channel with 4.5 MHz (or 45 Mbps) of bandwidth per camera, compared to an analog bandwidth requirement of only 0.4 MHz for each‘ 1200 bps data channel. Additionally, video is an analog source while data (and sometimes voice) communications are digital.

Data and video images are collected at local field sensors, passed along to a local controller, and transmitted to a TMC for further processing or direct application. This chain of events defines the communication links and nodes within a communications network supporting the surveillance system (see Figure 5-21), and has been used to describe the communications and interface requirements in this section, and the software and hardware requirements in Section 5.7.

To provide background information supporting definition of the communications and interface requirements, the following paragraphs briefly describe the limitations, advantages, and disadvantages of commonly used communication media. These media include twisted wire pair, coaxial cable, fiber optics, microwave, spread spectrum radio, cellular phone, and leased lines.

5.6.1 Communications Media

Twisted Pair Cable

The twisted pair cable is useful only for low-speed data communications in the traffic surveillance field. The common types of interfaces used with twisted pair cable are the serial interfaces RS232 and RS449. The RS232 interface is the older of the two types and has disadvantages in both transmission speed and transmission distance. The data transmission speeds can be up to 20 thousand bits per second (Kbps) only and the transmission distance up to 50 feet. The RS232 interface, however, offers three advantages:

+ The data flow is bi-directional.
+ It is usually compatible with computers used for data gathering or control devices.
+ The interface equipment and software are inexpensive.

This interface is generally used for connecting roadside sensors to trunk communication systems and for intracabinet connections.

The RS449 interface, with a balanced interface defined as RS422, provides much the same service as the RS232 interface but with higher transimission speeds and distances. Typical data transmission speeds of the RS449 interface are 10 million bits per second (Mbps) at a distance of

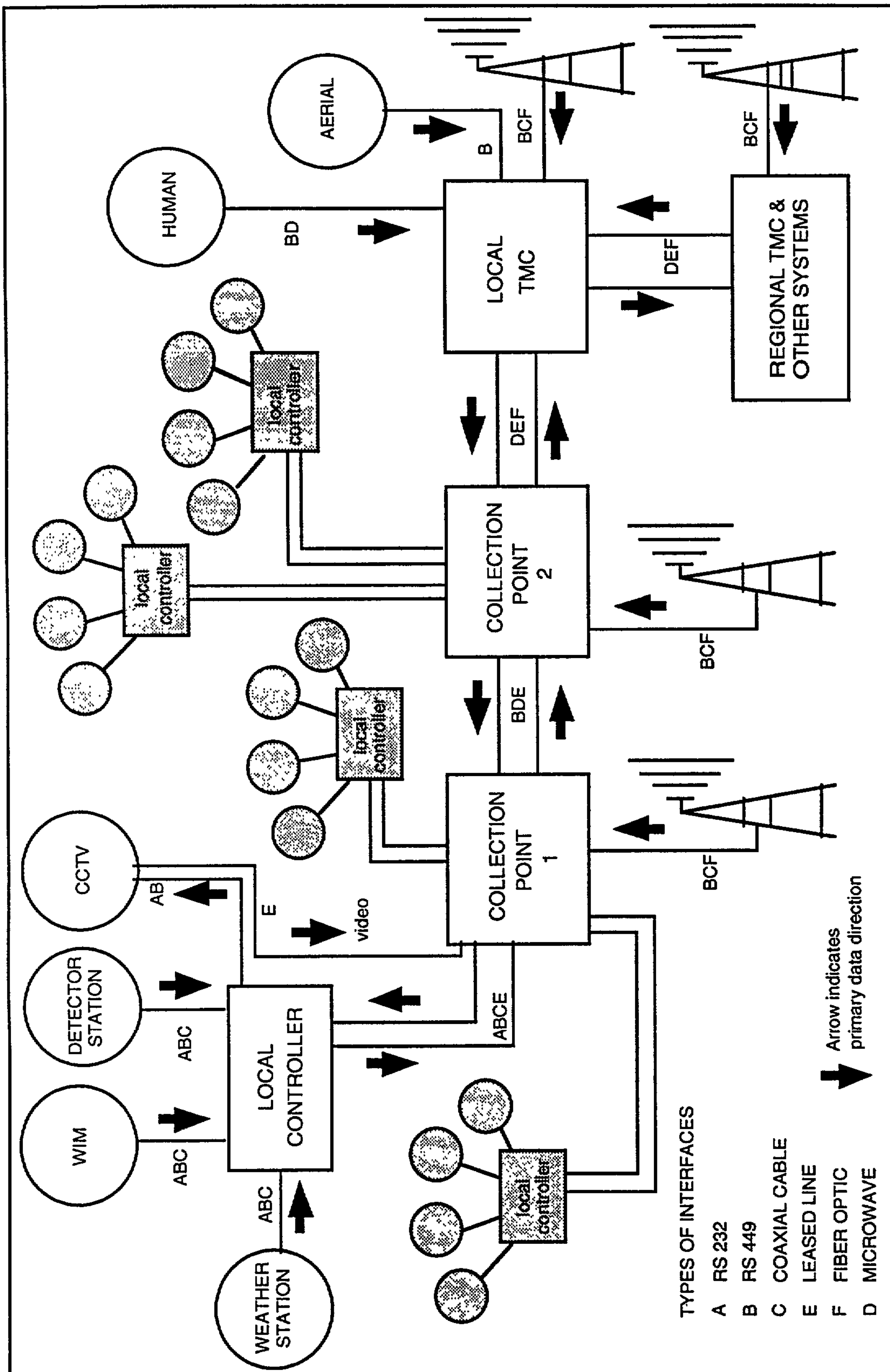

Figure 5-21. Surveillance System Communication Links, Nodes, and Interfaces

40 feet, and 1.2 Kbps at distances of up to 4000 feet. The data stream is bi-directional, as is the RS232 interface, but not compatible with most computers without a special input/Output (I/O) port. Since most surveillance equipment is manufactured with the RS232 as a standard interface, the installation of an RS449 interface is usually an additional cost. The RS449 interface is generally used for the transmission of field data to a destination within half a mile, and the data rate is low enough not to warrant a more expensive communication system.

Coaxial Cable

Coaxial cable can accept data, both digital and analog, at speeds of up to 10 Mbps, which are sufficient to serve up to 20 CCTVs at one location. The high data and video transmission rates are achieved by frequency division multiplexing and time division multiplexing of the signals on coaxial cable. The transmission of video signals requires a far larger bandwidth than traffic flow data. The consideration of transmission needs for CCTV surveillance systems effectively precludes all options except coaxial cable, fiber optic, and microwave.

Fiber Optics

Coaxial cable systems have been effectively supplanted by fiber optics for long-haul operations. Fiber-optic systems are more reliable and have a higher capacity. Since the general rule is that a clean signal can be transmitted through a fiber-optic cable over a distance of approximately 20 to 30 miles without regeneration, a digital signal can be regenerated almost indefinitely. A fiber-optic system can transmit both digital data and, either compressed or full motion, video signals.

The standards used in a fiber-optic communications system have been consolidated under the name Synchronous Optical Network (SONET). SONET standards include high-speed optical bit rates from approximately 50 Mbps (Optical Carrier Level One) to approximately 2.4 Gbps (OC48). OC1 means the ability to provide an equivalent data rate of one DS3 bit rate of 45 Mbps. DS3 is one of the many levels of bit rates in Bell System Standard digital transmission hierarchy explained as follows.

The fundamental rate of Bell System Standard digital transmission hierarchy is named Digital Signal Zero (DSO) which functions at a rate of 64 kilobits per second (Kbps). A DSO channel can support one voice communication path, a data communication path of 56 kbps, or, in the instance of data communications, can be subdivided into multiple lower-speed signals. A DSO rate is multiplexed into a signal containing 24 DS0 signals and is referred to as Digital Signal One (DS1). From the DS1 level, the Bell System Standard provides for additional multiplexing of signals such that the DS2 rate becomes 6.312 Mbps, and the DS3 rate becomes 45 Mbps.

A DS2 signal is capable of carrying the digital equivalent of 96 voice channels; and the DS3 rate contains 28 of the basic DS1 signals, or a digital equivalent of 672 voice channels. Hence, an OC48 can transport 48 DS3 signals, which is equivalent to more than 32,000 voice or data channels.

The digital signals sent by the optical transmitters of different equipment manufacturers are being standardized in their electrical and optical properties as well as in format. This makes it possible to install equipment from different vendors at opposite ends of a fiber-optic cable.

Besides the long-haul data transmission advantage of a fiber-optic system, a multi-mode fiber-optic system offfers cost advantages for short distance communication of up to 2000 feet. This is because the cost of the multi-mode cable and the electronics is less. The common use of this system is to bring CCTV signals to a controller cabinet in the field.

Microwave

Microwave radio systems have a sufficient bandwidth to transmit data and video at speeds of up to 40 Mbps for distances of up to 50 miles. Although a microwave system can transmit data over long distances, its main disadvantage is the line-of-sight requirement, which restricts the ability to install surveillance equipment at desired locations. Microwave radio is also not economically feasible for short distance operations, except to connect a few remote locations, because antennas would be required at each sensor site.

Spread Spectrum Radio

Spread spectrum radio is useful for relatively short distances and for remote sites, but it has serious limitations. The data speed of approximately 256 Kbps is sufficient for transmission of data, both digital and analog, and for transmission of compressed video. A limitation of the system is that the transmission distance is only 1 to 2 miles and is strictly line of sight. More powerful radio systems are available with transmission ranges of up to 20 miles, but these systems require FCC licenses and specific transmission frequencies, which may not be available in many urban areas.

Cellular Telephone

Cellular telephone communication is midway between radio and telephone communication systems. The cellular telephone interfaces with the land line services of the telephone network and can provide all of the functions available through a telephone system. A major disadvantage of the cellular telephone is that a momentary break in communication as the cellular telephone moves from one cell to another could cause a data communication failure. Thus, the use of cellular telephone communication for surveillance may only be suitable to fixed or relocatable installations (such as temporary traffic detection sites).

Leased Line

Leased telephone lines have a data capacity of 1.544 Mbps or a T-l line. This capacity is sufficient for most data transmissions but can only accommodate compressed video. Disadvantages of using leased lines include access and cost. The surveillance system proposed for the l-95 Corridor is centered on freeway/highway operation. Most of these roadways do not have easy access to telephone lines. The cost factor can be of considerable concern, because a T-l line could cost in the vicinity of $2,000 to $3,000 per month in rental or lease fees.

5.6.2 Field Communications Requirements

The field communications network provides the means to bring the surveillance data from the various sensors to a central location such as a TMC for processing or direct applications. Based on the system structure described earlier, the field communications requirements were defined for roadside sensors, controllers, collection points, and mobile assets.

Roadside Sensor Communications

The purpose of roadside sensor communications is to link any field sensor or control unit with the local controller cabinet where the data or video signal is processed and/or retransmitted onto the local collection network. Traffic flow and environmental data may be digital or analog, and the video signal will be analog. Some sensors will process the data in the sensor unit, while others will pass the raw data to a processor in either a controller cabinet or a central location. The control signals are transmitted to the sensor or camera, either by using the bi-directional communications system, or by using a communication system separate from the data flow.

An RS232 interface is generally provided with almost all types of field sensor equipment as a standard interface, permitting the attachment of almost any computer for field monitoring, adjustments, and repair. For most roadway traffic flow detection equipment, the sensor part of the system is located in the controller cabinet. For system components such as CCTV, the sensor and control hardware is located in the field equipment housing.

The RS232 and RS449 interfaces are generally used for the transmission of control signals to surveillance components. Most system designers prefer to segregate the control signals from the data or video signal, and use the RS232 interface for this purpose. Generally speaking, if the controller cabinet is within 50 feet of the surveillance, an RS232 interface will be used. If the unit is further than 50 feet from the controller cabinet, but within one half of a mile, the more expensive RS449 interface should used.

Because the distances between the roadside sensors and the field controllers are relatively short, coaxial cable is a viable alternative for CCTV video signal, and would be sufficient for the required data transmission. This interface will usually require a separate device at the equipment enclosure to encode the data and control signals onto and off of the coaxial cable.

Some pieces of field equipment are currently equipped with fiber-optic connections or can be attached to fiber-optic communications devices. This interface is the slower multi-mode fiber connection, using a multiplexer instead of a SONET-level system. Many of the lower speed devices are single channel units; therefore, a separate interface will be required for each piece of field equipment.

Fiber-optic cables can be used between high bandwidth components, such as CCTV cameras, and the local cabinet or CCTV processing equipment. CCTV processing equipment is generally not environmentally hardened and must be installed in an environmentally controlled enclosure. These enclosures are not installed at each camera. A minimal amount of processing is performed at the camera site, and the signal is transmitted to the equipment in the environmental enclosure using either a coaxial or a fiber-optic cable. The fiber-optic cable is the preferred medium. Since the distance between camera and cabinet is usually under 2000 feet, multi-mode fiber-optic cable can be used with a single channel modem. The CCTV analog signal can also be returned over a single multi-mode fiber-optic cable.

Controller Communications

The controller provides a means of transmitting the data between the sensor unit and the local collection network. The interface between the sensor and the processing unit in the controller cabinet must match the interface at the sensor unit, while the interface with the local collection network must match the network. The controller cabinet is also the site of some data processing in a distributed system. In most cases, the raw sensor data is processed and held in memory until the processing unit places the data on the local collection network. Data may be transmitted to the central location based on a specific command from the central unit, or on a timed basis. Generally, the central control will transmit a command to each local unit in sequence, and the local unit will respond with its accumulated data.

The type of interface is dictated by the distance between the controller cabinet and the local collection network access point, the type of transmission (data or video signal), and the amount of data. In some cases, when the distance between field equipment sites is sufficient to require a local collection node, or if the field equipment site coincides with a local collection node, the controller cabinet is also the access point for the local collection network. This type of system is usually a daisy chain system. In systems where the field equipment data and control signals are transmitted to the local collection network by a star pattern, multi-drop, or similar configuration, the controller cabinet and the local collection network cabinets are separate cabinets.

Both the RS232 and RS449 interfaces are used for the transmission of traffic flow data from roadside detector cabinets to local communication cabinets, local transmission systems, and internal cabinet connections between different pieces of equipment. If the local field equipment includes CCTV cameras, there may be several different types of interfaces present in the controller cabinet. For example, a coaxial cable may be carrying a video signal in from the roadside camera. If the cable is not being used for retransmission of the signal to a local collection node, the only coaxial interface will be that with the roadside field equipment. A coaxial cable or an RS449 interface may be used if the retransmitted signals, either data or video, will be sent via a radio or microwave transmitter located at the controller cabinet.

The transmission of data across fiber-optic lines is becoming increasingly advantageous. The great amount of data and the long life of the system is offsetting the slightly higher cost of installing fiber-optic cable and electronics. The transmission of data between a local controller cabinet and the collection point would probably use the slower multiplexed signal rather than the high-speed SONET-level system. The multiplexed signal should be sufficient for all data needs at the controller cabinet, except for the video signal, as discussed in the next paragraph. The slower fiber-optic system can only accommodate a compressed video signal.

The video signal from the CCTV camera installations will either be processed in the controller cabinet or retransmitted to the local collection network node. It is most likely, given the susceptibility of CCTV processing equipment to malfunction under adverse environmental conditions, that the video signal will be retransmitted onto the local collection network node for processing at a central location under controlled environmental conditions. Generally, this retransmission will use the same type of medium as was used to transmit the data to the controller cabinet, because the incoming signal will probably not be processed, only retransmitted. This medium will be either coaxial cable or fiber-optic cable. The retransmission or repeating of the signal can be separate on the fiber-optic or coaxial cable, or can be combined with other signals using frequency or time division multiplexing techniques. Coaxial video transmission systems usually use Frequency Modulation (FM) systems to combine the signal and place it on a cable with other signals.

Collection Point Communications

A collection point either channels the incoming data to the appropriate processing hardware, or combines and retransmits the data to the local TMC. Most of the incoming data will be processed before or at this location. The CCTV video signal may also be processed at this location, or it may be converted from an analog signal to a digital signal and placed on a high-speed data line. If the video signal is already a digital signal, it will be combined with other digital signals for retransmission.

The RS232 interface is generally used for internal cabinet connections between different pieces of equipment. The RS232, RS449, and coaxial interfaces can be used to connect the local collection point equipment to a radio transmission unit located at the collection point. The distance between the collection point cabinet and the radio transmitter, and the amount of data to be transmitted determine the actual type of interface required.

Fiber-optic communications of incoming signals may be either low- or high-speed. Signals going out over fiber-optic interface will all be high-speed signals, probably on a SONET-level communications system. Given the low ratio of unit cost to available bandwidth, it is reasonable to assume that most of the outgoing data will be on fiber-optic cable over a SONET-level system. This assumption may not be valid at locations where the cost of installing fiber-optic cable becomes a major factor.

All high-speed, SONET-level communications can, in most cases, be accommodated by a single high-speed SONET interface. Each high- or low-speed signal coming from the local controller cabinet can be handled in one of three ways:

+ The high-speed signal can be placed on the high-speed outgoing line as a separate information packet.
+ The incoming high-speed signal can be combined with other high-speed signals and retransmitted to the next collection point on the network or to the TMC.
+ The low-speed signals can be combined and placed on the high-speed system.

In the other direction, from the TMC, the high-speed interface will either pass the incoming signal through as a high-speed signal, or divide it into low-speed signals that will then be transmitted to the local controller cabinet over an assortment of possible interfaces as previously described .

Another viable interface for communications between the local collection point and the TMC is radio, including microwave. The incoming signals, regardless of communications type, can be processed through the appropriate incoming interface, and combined into information packets for transmission over a radio system. The interfaces used for sending data to or receiving data from a radio transmitter are usually RS232 or RS449. These interfaces limit the transmission capabilities of the radio. When large amounts of data must be transmitted, other interfaces (such as coaxial) are used.

The last choice for a communication system from the local collection point is leased telephone lines. This option has the ability to carry the data information, but has insufficient bandwidth for full-motion video. There are some video compression systems being developed that will place a near-full motion compressed video signal on telephone lines, but the number of such signals per line is limited. The interface with the leased telephone lines can be either analog or digital, and can be up to a T-l bandwidth.

Mobile Asset Communications

Wireless communications will be needed to provide a link with mobile surveillance assets, such as patrol vehicles and aerial surveillance platforms (if implemented). Data and voice communications with patrol vehicles may be accommodated via mobile radio (e.g., in the 450 MHz or 800 MHz bands). Since radio frequencies may be limited in many urban areas, the use of other means, such as Cellular Digital Packet Data (CDPD) may be viable for data transmission. The communications link between an aerial surveillance platform with a ground station, such as a TMC, should be able to accommodate the transmission of voice, data, and video signals.

5.6.3 TMC Communications Requirements

The TMC receives data and video signals from the local collection network and sends control signals back to the field devices across the local collection network. The TMC also processes all of its surveillance data and distributes it to internal monitors, other TMCs, and the public.

The local TMC will have both internal and external communications. Since the external communications functions to other TMCs are addressed by Project #1 (IEN), their requirements are not defined here, except for the interfaces. The requirements for the internal TMC communications are as follows:

+ The internal communications of the local **TMC** shall contain two separately redundant networks: analog and digital.

+ The analog network shall provide for the distribution and recording of analog voice, non-digitized CCTV, and other analog data types. It shall also have a capability to convert analog data to digital data upon demand.

+ The digital network shall provide for the distribution and recording of digital data and digitized analog data. It shall also have a capability to convert digital data to analog data upon demand.

The internal interfaces are between the I/O ports, generally called a Central Communications Interface (CCU), and the assorted computers, recording devices, and similar components in the TMC. The interconnect interface will probably be a Local Area Network (LAN) system commercially available from a number of vendors. The interfaces used by the different LAN systems slightly differ in detail, but all are basically alike in their passing of data from the CCU to the local computer equipment. RS232 interfaces are also used by many types of computers and computer-related components.

The external interfaces are of two types: those between the TMC and the local collection points, and those between the TMC and other TMCs or public/private users. The external communication media will include high-speed types, SONET-level fiber-optics, radio and microwave, with some leased telephone lines. The associated interfaces include: fiber optics, coaxial and leased telephone for high-speed land data across land lines, and RS449 connected to radio and microwave transmitters for high-speed to moderate-speed data by wireless.

5.7 SOFTWARE REQUIREMENTS

The software requirements consist of mostly commercial, some custom, and many hardware-related proprietary programs. Most of the field equipment, including vehicle detection units, CCTV surveillance units, and Video Imaging Detection (VID) units, include manufacturer developed proprietary software to permit user operation of that particular item. Some of the communication systems also include software, such as the fiber-optic SONET and Multiplexer systems, spread spectrum radio, microwave, cellular telephone, and leased telephone lines. The last item, leased telephone lines, is controlled either by the telephone service suppliers or by commercially available telephone interface equipment.

Proprietary software can be integrated into the system once the protocol interface has been established. Each piece of hardware controlled by proprietary software is meant to download and/or upload data from an external source. The external source, in this case it is the surveillance system, can be programmed to accept and understand the proprietary software data. The computer programmer must first retrieve the hardware's protocol, usually by requesting it from the manufacturer. The manufacturer will usually give the protocol to the programmer once a non-disclosure agreement has been signed. The programmer can then write for the controller a **program that will interface with the proprietary software in the detector or surveillance field** hardware to permit the central system to upload data and download commands.

5.7.1 Software at the Controller

The controller cabinet houses the roadside detectors and surveillance equipment, all of which are controlled or processed by proprietary software. The controller, housed in the controller cabinet, will require some programming for accumulation of the detector data and transmission of that data to the collection point upon demand. Many diagnostic software programs will be controlled and accessed by the TMC or the collection point equipment.

5.7.2 Software at the Collection Points

The collection point could have the same software requirements as the controller cabinet, with the additionof the high-speed communication systems. As stated previously, the SONET-level equipment is packaged with operating and diagnostic software. The user needs to provide overseer programs only if they are requested.

5.7.3 Software at the Local TMC

Additonally, the TMC will have a considerable number of prepackaged proprietary software programs, but a number of custom programs are required also. From the surveillance perspective, software applications provide a number of functions, such as:

+ Maintaining the surveillance asset configurations.
+ Ingesting the incoming data.

+ Processing the data further as necessary.

+ Providing the data storage capability and maintaining a database.

+ Disseminating information to the users.

+ Supporting operators.

A Network Management System (NMS), which is usually PC based, will provide software required to automatically administer and control the SONET transmission system. The NMS will interface with the SONET terminal equipment at both the collection point equipment enclosures and the TMC. It will support status and alarm data between each of the collection point equipment enclosures and the TMC. It will also send control data to the collection points to allow remote operation of the collection point communication equipment from the TMC. The flow of NMS data to and from the collection point equipment enclosures will use a data circuit embedded in the overhead bytes of the SONET transmission system payload.

Capabilities of the NMS include alarm status reporting, system control and testing, determining fault locations, and circuit provisioning (setting up channel time slot assignments at all sites). The remote provisioning function will allow the NMS to automatically reconfigure the communication system in the event of an optical equipment failure. Both ends of circuits which were assigned to the main route would be reassigned.

The NMS would also be capable of monitoring and controlling devices and functions external to the SONET equipment, such as Controlled Environment Vault (CEV) internal alarms (high/low temperature, door open, gas accumulation, and flooding), video transmission system protection switching, and others.

Many maintenance activities will be possible using the capabilities of the NMS. Properly programmed, the NMS will notify the maintenance supervisor of trouble, determine the trouble location, and specify the failed module, before a technician is sent to troubleshoot the equipment at the collection point enclosure. The NMS may also be used to keep records on logistics, such as the exact location of individual equipment modules, whether within the system or out for repair.

The data filing and retrieval systems are critical to the successful operation of the TMC. Considerable effort must be expended to provide software that can select information for any route, and display that information in a usable form. The system must provide an interface to automatic dial-in telephone services.

Typical software capabilities may include:

+ Traffic and Travel Information Access Management and Dissemination - provides the operator with controls to mange traffic and travel information collected and processed by the system. Features of this software may include:

  - Multiple-Source Information Correlation — provides the operator with the ability to correlate collected information packets or reports (i.e., text data) with identified events (e.g., incidents), Corridor segments, reports, databases, or other operator-defined information categories. Databases may include:

    - Traffic Operations.
    - Traffic Modeling.
    - Communications Link Management.
    - Incident Log.
    - Traffic Network Status.
    - Historical Data.
    - Roadway Conditions.
    - System Map Data.
    - System Status Data.

  - Information Dissemination/Distribution Lists — provides the operator with the ability to identify and assign those recipients to ‘receive online categorized information as released for dissemination by the operator. The lists may include logical dissemination addresses (e.g., system communications port), communications media, information category types, and telephone.

- Generate and Review Advisory Reports — provides the operator with the ability to generate travel advisories for dissemination in a defined area through user-configurable forms.

- Manage Information Database and Control Access — provides the operator with the ability to manage ATIS information databases containing traffic- and travel-related data.

+ System Operations Performance and Malfunction Management — provides operator control for managing system operations, performance, and subsystem/component malfunctions. It provides the operator with general operational status and statistics for all subsystems and allows the operator to perform diagnostic interrogations for the integrated subsystems to the component level (e.g., camera, ramp/detection station equipment, VMS, and HAR). Detailed status received from the interrogations are formatted into status summaries for recordkeeping or maintenance action.

+ Automated Incident Management Tasking — provides a function which will assist the operator with the management, notification, and response to incident events detected by the system. The following subsystems may be included:

  - Automated Incident Verification — provides system control for identifying incident locations and appropriate CCTV cameras on the system map display. It provides the operator with a verification checklist to confirm the incident occurrence and location, and to initiate recordkeeping through incident log entries.

  - Incident Recordkeeping — provides operator control for collecting details for the incident log. This function is automatically invoked when an incident detection alarm is issued.

  - Incident Notification and Response Formulation — provides controls for identifying the appropriate agency(s), depending on the incident location, and for developing appropriate response actions in accordance with approved Corridor incident management plans.

+ System Monitoring of Subsystems — provides a system which will provide general monitoring capabilities and operational status of all subsystems, including the

SONET backbone, and will generate appropriate operational performance statistics reports identifying each subsystem's functional status.

5.8 HARDWARE REQUIREMENTS

Support structures are defined as those outside plant components of the communications system that are required to facilitate installation and maintenance of the field portion of the traffic management system. Support structure requirements are derived from the physical topology of the communications system that may be employed. Therefore, while providing recognition for growth, the primary design requirement for support structures is to mechanically accommodate the field portion of the communications network. Support structures typically require a significantly large proportion of the capital investment. As such, they should be designed to satisfy the requirements of long-term system goals.

Support structures are also required for mounting the over-the-road and roadside detector hardware. The over-the-road detectors mount their respective sensor units either over individual lanes or at locations where one sensor can observe and record traffic in several lanes. The sensor units mounted over individual lanes can be microwave, radar, IR, or electronic tag reader (such as those used in ETTM) type sensors. Since these types of sensors are small, they can be mounted on existing sign structures or bridge structures. Their weight and size generally do not cause any loading problems for the existing structures. The electronic tag readers with covered antennas are probably the largest, at approximately 12 inches wide, 4 inches thick, and 18 inches long. The major concern in installing over-the-road sensors is the vertical clearance to the roadway. Roadside sensor mounting is considerably easier. The sensor should be mounted 20 to 35 feet above ground level. The sensors mounted at the high end of this range are better able to observe the entire traffic flow without interference from trucks; but some sensor manufacturers place upper limits on the mounting height due to range limitations of the sensors. The mounting pole usually used is a standard traffic signal pole with sufficient internal harmonic damping. The controller cabinet that houses the detector equipment is usually located close to the detector's sensor and is a ground-mounted cabinet.

Support structures will normally consist primarily of conduits, cable vaults, pull boxes, and CEVs. These facilities are the means by which the communication cables are routed for connection to field devices.Depending upon a specific design, CEVs may or may not be utilized as a hub point for housing field communication transmission equipment.

The sophisticated optical and electronic communication equipment at a large communication hub requires a controlled environment; therefore, only collection points and TMCs will be designated as large hubs. It is typical to install this type of equipment in shelters which provide a building type of environment. While above ground equipment shelter buildings have been used commonly in the communications industry, there has been an increasing trend toward the use of underground vaults for housing this equipment. A CEV provides security and aesthetic advantages over an above ground building. A CEV also provides excellent protection for costly equipment in a roadway environment, because most of the shelter is buried and not susceptible to damage by wayward vehicles.

A CEV is constructed of concrete or steel and can be buried in the ground with only an entrance hatch and air vent protruding above the finished grade. It is equipped with cooling and heating systems to maintain controlled temperature and humidity levels for the installed optical and electronic equipment. It is also equipped with gas detectors and alarms for personnel safety: and, if buried, it is equipped with an automatic sump pump to protect against flooding. Concrete and steel CEVs have similar characteristics with respect to electronic equipment accommodation.

Large communication hubs may contain equipment required for video transmission, video distribution, voice and data transmission, and voice and data distribution systems, and associated fiber-optic, coaxial, radio, and twisted wire pair (RS232 and RS449) interface hardware. Also, video processing equipment can be included at these sites. The equipment required in each large hub must be installed inside of a shelter which provides a suitable environment for the reliable operation of the system.

The local controller cabinets and some small collection points fall into the category of small communication hubs. These sites will contain sufficient equipment to support only video and data transmission systems. No video signals will be processed.

Some data processing can be accommodated in these cabinets. This will include any associated fiber-optic, coaxial, radio, or twisted wire pair (RS232 and RS449) interface hardware. The equipment required in each small hub can be installed inside of a standard cabinet which provides a suitable environment for the reliable operation of the system. Most notably, a small communication hub design will not likely require a controlled environment vault.

5.8.1 Hardware at the Controller

The roadside sensor units will probably be installed in the controller cabinet. These units manage the detector operations. They control the detector operation and process and store data until commanded to send the data to the collection point. The hardware in the controller cabinet will be as varied as the number of types of detector and traffic surveillance and control systems employed along the roadway. Several pieces of roadside equipment may be located in any one controller cabinet.

Traffic flow detectors each have their own type of sensor device, but all are interfaced with the communication system. The interface can be individual modems, each occupying a separate output communicationline, or a multiplexer that combines each outgoing data packet and places the resultant data onto a single outgoing communication line.

Most detectors send their information into a controller for processing (if required at the controller cabinet level), accumulation of the data, and transmission of the data to a central point upon command. The controller most often used for these tasks is the type 170 traffic signal controller, reprogrammed to accept and process data. The type 170 controller, and the newer type 179 controller were developed by the California Department of Transportation (CalTrans), for use as a versatile traffic signal controller. The unit is actually a field hardened computer with full I/O functions. The computing power of the unit can be increased by the installation of a VME bus backboard. The type 170/VME controller unit has the I/O of the type 170 and the computing power of a desktop computer for data analysis. The equipment proposed for installation along the I-95 Corridor will probably require a type 170 controller for data processing.

Of the many types of available traffic detector systems, the following will probably be installed in the controller cabinets:

+ Inductive loops or magnetic probes imbedded in the pavement require a sensor unit within 800 feet of the side of the roadway. The sensor unit can be a dumb unit that only detects vehicles, or the sensor can have processing capabilities. If the unit is a dumb unit, a controller must be supplied and located in a cabinet within 2000 to 3000 feet for the processing of the data.

+ Overhead and side-fire vehicle and speed detectors also require a sensor located in close proximity to the detector unit. The distance between detector and sensor unit is usually only 100 to 200 feet. These detectors may include both Doppler effect and ranging sensors. The detectors generate more information, including vehicle speed. Only the Doppler sensor can measure the actual vehicle speed. The ranging sensor computes speed. These detectors require a more sophisticated processor to compute and accumulate the data, since most commercially available units compute average values.

+ VID units are CCTV cameras placed in a fixed location, usually over the roadway. Since one camera can observe and differentiate approximately 20 to 30 distinct fields, the camera should be mounted high enough to provide it with a wide viewing area. Most camera installations are on high poles, up to 50 or 60 feet, or on overpasses. Installation includes a small field unit that places the video signal on a transmissionline, usually fiber-optic. This field unit is in a box and is mounted as close to the camera as possible, usually on the top of the pole next to the camera. Typically, to avoid multiplexing, a separate fiber must be dedicated to each camera. Given that multiple-fiber cables are small and economical, and that single-mode fiber can be run up to 30 miles without repeating, this solution is very attractive for video communication between the cameras and local collection point. No video processing is required in the local controller cabinet. The only hardware required in the cabinet is a transmission system, either coaxial or fiber-optic, to retransmit the signal to the collection point. The fiber-optic system will be a low-speed system rather than a SONET-level system. Neither of these communication systems, coaxial or low-speed fiber-optic, requires an environmentally controlled enclosure.

Traffic surveillance equipment includes CCTV cameras with fully mobile mounting; that is, the mount is equipped with pan tilt and zoom at a minimum. These units need control data for operation of the camera and the mount, and they generate an analog video signal. The control data will come through the controller cabinet as data on a low-speed communication system. The data is split from the data stream and. directed to the specific camera by the communications interface, which is an intelligent modem located in the controller cabinet. The video signal is not processed in the controller cabinet, but is retransmitted to the collection point.

Devices may be present in the controller cabinet to interface the data stream with radio or microwave transmission equipment. The radio interface is either a smart modem or a dumb modem with the processing capabilities placed in the controller. The modem converts the data flow into the required format for transmission and places it in a carrier wave. Conversely, the incoming data is removed from the carrier wave and translated back to usable data.

5.8.2 Hardware at the Collection Points

A collection point can also act as a local controller cabinet and can include most of the same equipment. This will occur when the distances between controller cabinets are equal to the distances between collection points on lightly instrumented roadways.

The collection point is responsible for placing the low-speed fiber-optic communications onto a high-speed system for transmission to the TMC. This equipment currently requires a controlled environmental enclosure. As previously described, the collection points will probably be constructed as CEVs. The SONET equipment is rack mounted and will require approximately 100 square feet for a two rack installation. The installation will also include a monitoring system and backup batteries to maintain the SONET system until repair crews can access the site. The batteries need to be sufficient to keep the site operational until the repair crew arrives. The repair crew must be equipped with a portable power source.

The type 170 controller with VME bus computer should be sufficient for all data-related computing tasks at the collection point. The data that was not processed at the controller cabinets will be processed at this location. Since most of the data will already be fully processed, or will be processed in the TMC, the computing requirements at the collection point are minimal. Therefore, the computing requirements of the collection point are similar to or fewer than the requirements of the controller cabinet. The collection point is generally a communication transmission point where data from one or several controller cabinets is processed and placed onto a fiber-optic cable for transmission back to the TMC. Generally, the data from one collection point will pass through other collection points before reaching the TMC. At these other collection points, the incoming data may pass through or will be combined with additional data from the collection point, and will be retransmitted to the next point.

Depending on the selected video transmission system, either analog or digital, the collection point must process the signal and retransmit to the TMC. Essentially, there are two options in network design for video. The first option is to use AM and FM multiplexing techniques to transmit multiple video images over a dedicated optical fiber from a collection point. The second option is to digitize the analog video signal and send it to a broadband digital system, such as a SONET fiber-optic system. To convert an analog signal to a digital signal, a coder is used; to restore the digital signal to a usable analog signal it passes through a second device, referred to as a decoder. A coder and decoder can be manufactured as an integrated unit and are generally referred to as a CODEC (coder/decoder). These units are generally environmentally hardened.

There is a multiplex system that will support video channels simultaneously over a single fiber for distances of up to 30 miles. However, the multiplexing techniques are not compatible with the digital data transmission of a SONET system, thereby necessitating separation of the functions onto different fibers. It is, however, practical to use a common bundle of fibers, and to dedicate one or more fibers per hub exclusively for video transmission, and the other fibers for data.

5.8.3 Hardware at the Local TMC

A collection point can be located next to a TMC, but the TMC will not include any of the data gathering functions of either a controller cabinet or a collection point. The TMC is responsible for both retrieving data and video from the high-speed communication systems and placing data and video onto the high-speed communication systems for transmission to the local collection points and to other TMCs. In order to perform all of these communications functions, the TMC must include all of the interfaces for all of the high-speed communication systems including fiber-optic, coaxial, radio, microwave, and leased telephone lines. Besides this equipment, the TMC must be equipped with a CCU and a Digital Access and Crossconnect System (DACS), to support ease of circuit rearrangement between field sites as well as to aid in rapid restoration of service in the event of an outage. Also, a DACS allows DS1 lines to be remapped electronically at the DSO level. It will allow the assignment and redistribution of 64 kbps data communication and voice channels among various T1/DS1 systems connected from the field sites to the DACS, at the digital level, and can therefore be considered a DS1 switch. The DACS will also provide per-channel DSO test access in digital form. DACS is not a direct replacement for, nor an alternative to, any single previously existing network equipment. It is, however, a versatile piece of equipment, which has several roles in a large telecommunication network. Dedicated lines, which are the workhorse of traffic management systems, can be rapidly reconfigured and reengineered. If the dedicated lines were implemented simply as pairs of wires (or the equivalent), modification of the circuit would be difficult, whether for maintenance purposes or redesign purposes: the DACS facilitates this process.

A DACS allows DSO channels to be routed without having to be demultiplexed. Hence, circuits from the various field sites can be concentrated at the TMC. The equipment allows rapid and inexpensive cross-connection of DS1 channels: the connections can be monitored, tested, disconnected, and reconfigured easily from local or remote terminals. A DACS serves the same function in the digital environment that a distributing frame served in an analog environment.

The VID processing equipment will be located in the TMC. This equipment includes the processing computers and monitors, both of which are manufacturer specific.

The TMC will be the interface with the public. It will be equipped with full telephone service including automatic dial-in service. The system computers must be capable of selecting, upon request, video pictures and specific route data for transmission to public and private users. This also includes storing and filing all pertinent information, and the retrieval system to access that information and deliver it by both paper and electronic services.

The TMC will also be equipped to control and monitor the entire system, including computers, monitors, and recording devices, such as VCRs for the video signals. The computers must be the highest level of PC type computer. "Main frame" computers are no longer needed, because all of the functions of the large older computers can now be done by table top units. Display devices should include regular and high-resolution monitors for use by the individual operators. Large high-resolution monitors should also be used by the supervisor and for general displays.

5.9 OPERATIONAL RESPONSIBILITIES ANALYSIS

The purpose of this section is to define and develop an operational responsibilities framework for use in the design and implementation of a Corridor-wide surveillance system. The following paragraphs discuss the assumptions used for developing the operational responsibilities, define the operational responsibilities required to effectively implement an integrated surveillance system, and describe the primary issues involved in the implementation of such a system.

5.9.1 Operational Responsibilities Assumptions

In order to develop the operational responsibilities for the I-95 Corridor Coalition, initial assumptions were made regarding surveillance data collection, processing, and dissemination. These assumptions are as follows:

+ Specific technologies are not defined; only the data which the Coalition will require is defined.

+ Operational responsibilities definition does not address the existing surveillance technologies and communication systems currently deployed in each member's jurisdiction; only the data which that agency is responsible to provide to the Coalition are defined.

+ Each individual Coalition member is responsible for the maintenance and operation of surveillance equipment within their respective jurisdictions.

+ It is the Coalition's responsibility to establish and coordinate operational protocols and policies for Corridor-wide operations.

+ Specific data processing methods or algorithms are not defined; it is the responsibility of each member agency to determine its own data processing methodology. However, the Coalition must establish standard data dissemination formats and communication protocols for system compatibility.

+ Operational responsibilities are defined independent of hardware, software, and communication interface requirements.

These initial assumptions are derived from the concept of cooperation and coordination among the agencies responsible for specific transportation systems and equipment. This is the fundamental basis for developing the preliminary operational responsibilities framework. The system envisioned is not of one master system operated by a single entity, but rather a series of individual ITS systems, each planned, designed, implemented, and operated in close coordination with the others, and remaining under the jurisdiction of the individual states or operating authorities. Under this vision, the Coalition's primary activities include:

+ Coordinated collection, analysis, and dissemination of surveillance data, and traffic and travel conditions to all agencies requiring this data.

+ Maintaining a coordinated traffic database for operation, management, and strategic planning.

+ Coordinated planning, implementation, and operation of surveillance systems.

+ Ensuring compatibility of technology, communications protocols, and data format for all surveillance systems implemented within the Corridor.

+ Developing the necessary interagency cooperative agreements, and standardizing institutional arrangement and commitments required to operate and manage the Corridor-wide surveillance system effectively.

A central clearinghouse for traffic and incident data is the principal component which binds these activities together. In order to implement these activities, the central clearinghouse needs to:

+ Link to the individual traffic operations centers of all members.

+ Receive regular communication on the traffic conditions for major roadways from all jurisdictions.

+ Provide real-time information on traffic conditions and travel modes to other control centers and individual users, including the media, when queried or on a scheduled basis.

+ Serve as a coordinating facility for Corridor-wide incident conditions.

In turn, each individual ITS surveillance system will provide the necessary data to the clearinghouse for these activities to be integrated into a seamless, coordinated Corridor-wide surveillance system. As such, the I-95 Corridor Coalition is a partnership of the major public and private transportation agencies which serve the Northeast Corridor of the United States, including all major free and toll highways which parallel I-95, the major routes which feed these north-south highways, and the various modes and facilities serving passengers and freight.

In order to formulate an operational responsibilities framework, it is necessary to prioritize critical surveillance areas within the I-95 Corridor so that a coordinated traffic control network can be implemented in those areas most affected by traffic congestion. As identified in the Information Exchange Network (Project #1) Requirements Report dated January 27, 1995, various data elements that will comprise the IEN may be classified as follows:

+ Corridor — information that is important to the majority, if not all, of the Coalition members.

+ Regional — data provided among agencies located within a "metropolitan sphere". Suggested regional groupings are:

  - Boston Region (Maine, Vermont, New Hampshire, Massachusetts, Connecticut, and Rhode Island).

  - TRANSCOM Region (TRANSCOM member agencies within New York, New Jersey, and Connecticut).

  - Philadelphia Region (New Jersey, Delaware, Pennsylvania, and Maryland).

  - Baltimore-Washington Region (Maryland, District of Columbia, and Virginia).

+ Local — detailed data, including incident details and response plans, provided by two or three adjacent agencies.

It is each local agency's responsibility to supply the corresponding regional area with the required data necessary for effective regional coordination, and to provide the required data to the Corridor for Corridor-wide application.

5.9.2 Operational Responsibilities Framework

The intent of the operational responsibilities framework is not to define the administrative structure of the surveillance system's operations. The intent is to analyze the appropriate functional responsibilities of each of the member agencies relative to the surveillance data that is required to enhance their operation, and the information they need to provide to the Coalition for coordination and database support.

Coalition members state that their operating mission is to provide safe, efficient, effective, and environmentally sound highways and other surface transportation systems. The overall mission of the Coalition is to work cooperatively to improve mobility, safety, environmental quality, and efficiency of interregional travel in the Northeast Corridor through real-time communication and operational management of the transportation system. Therefore, the basis of the Coalition's operational responsibility is to provide an environment for government officials and private transportation providers to organize and expedite critically needed policies which will shape the future of ITS investments along the I-95 Corridor.

The transportation system in the Corridor is truly multimodal and intermodal. The Corridor is served by 13 major commercial airports, dozens of regional airports, over two dozen major rail stations which provide AMTRAK service, and 11 major ports. The Corridor states contain a total of 6,990 miles of Interstate and 22,450 miles of principal arterials and expressways/freeways. Therefore, in order to implement an integrated Corridor-wide surveillance network, it is necessary to define and develop an operational responsibilities framework.

The operational responsibilities framework has been developed based on each member's role within the Corridor and the core functional requirements identified in the Functional Requirements Section. The complex organizational structure of the Coalition was analyzed to determine the functional operating responsibilities of each member. These various operating agencies, authorities, or organizations include:

+ Local Traffic Operations Agencies.
+ Freeway Traffic Operations Agencies.
+ Toll Authorities.
+ Transit Authorities.
+ Commercial Vehicle Fleet Operators (CVFO).
+ Maintenance and Construction Agencies.
+ Public Safety Organizations (e.g., police, medical, and fire).

This section will define the functions of these agencies and describe the information requirements each agency is responsible to provide to the Coalition. The collective information at the Corridor level will be shared among the various Coalition members for strategic planning and policy building, as well as direct coordination.

Local Traffic Operations Agencies

Typically, local traffic operations agencies perform local traffic control duties and participate in incident management functions, such as traffic signal control on metropolitan arterials and local streets. These agencies monitor and control traffic conditions by collecting traffic data, assessing traffic performance, detecting traffic incidents and congestion, and assessing incident severity for incident management. For example, coordinated signalized arterials or traffic-adaptive signal systems require a local operations center to function effectively. Local traffic operations agencies also monitor roadway hazard conditions to detect debris on the road, detect pavement and bridge damage, and detect slippery road conditions. The efforts of Local Traffic Control Operations Agencies generally exclude freeway operations which cross through their jurisdictional area, however close coordination with freeway operations is necessary for seamless traffic control, especially during incident situations.

The data obtained from surveillance technologies deployed in these areas must be provided to other operating agencies for coordinated response and support. Operational policies, response plans, communication protocols and surveillance data collected must be disseminated to the various municipalities and regions for effective and efficient operations.

It will be the responsibility of the Local Traffic Operations Agencies to provide processed surveillance data, including traffic incident data, travel time data, traffic count data, traffic signal data, traffic demand levels and locations to the Coalition. This information will be shared with the various Coalition members for strategic planning and policy building, and with adjacent regional and local jurisdictions who require direct coordination.

Typical users of this data include the Freeway Traffic Operations Agencies for integrated traffic control, Police and Emergency Organizations (e.g., medical teams or HAZMAT clean-up crews) for incident management, Transit Authorities for scheduling purposes, CVFOs for route planning, and the Coalition for database support.

Freeway Traffic Operations Agencies

Freeway Traffic Operations Agencies include freeway systems within the I-95 Corridor operating within specific jurisdictional boundaries. Typically, these agencies perform traffic operations throughout the freeway system by monitoring traffic conditions, acquiring individual vehicle information, monitoring environmental conditions, monitoring roadway hazard conditions, monitoring commercial vehicle regulations adherence, monitoring air quality conditions, and providing surveillance data to the Coalition database.

It will be the responsibility of the Freeway Traffic Operations Agencies to provide operational policies, response plans, and processed surveillance data to the Coalition. Examples of the required data include traffic incident data, travel time data, traffic count data, traffic composition data, ramp metering data, traffic demand levels and locations, roadway hazard data, vehicle emissions data, and environmental conditions data. This information will be shared by the various Coalition members for strategic planning and policy building. Adjacent regional and local jurisdictions who require direct coordination will also be provided with this data.

The data obtained from surveillance technologies deployed in these areas must be provided to other operating agencies for coordinated response and support. Typical users of this data include the Local Traffic Operations Agencies for seamless traffic control, Police and Emergency Organizations (e.g., medical teams or HAZMAT clean-up crews) for incident management, CVFO Organizations for fleet support, Maintenance and Construction Agencies for schedule and planning coordination, and the Coalition for database support.

Toll Authorities

In the context of this responsibility analysis, the operations of a Toll Authority encompass those of a Freeway Operations Agency, a Maintenance and Construction Agency, and a Public Safety Agency. Toll authorities function similarly to Freeway Operations Agencies for traffic control and incident management, Maintenance and Construction Agencies for the upkeep of the transportation facilities, and Public Safety Agencies for incident response, incident clearance, and the enforcement of transportation laws and regulations. In general, Toll Collection Agencies need to collect traffic surveillance **data for congestion and incident management, identifying high travel** demand areas, toll facility planning, operartions and safety improvement, TDM, and facility maintenance.

Toll financing has enabled Toll Authorities to be the front runners in providing state-of-the-art services to their users. Toll Authorities serve as useful operational test beds for innovative technical and policy concepts. Presently, several of the I-95 member transportation authorities are pioneering the use of ETTM technology. The use of ETTM provides many opportunities for the management of transportation beyond a toll collection system. Work is underway by TRANSCOM to utilize the ETTM-equipped vehicles as probes to generate information on highway conditions and to aid in incident detection. The widespread use of ETTM equipment should substantially reduce queues at toll booths and result in a significant reduction in accidents and air pollution at these locations. The use of this technology also provides opportunities to facilitate congestion pricing. The experience of the Toll Authorities in the use of ETTM will provide valuable information to public policy makers in that regard.

It will be the responsibly of the Toll Authorities to provide surveillance data, response plans, and operational policies to the Corridor for coordination with adjacent agencies for regional traffic management. Surveillance data includes traffic flow data, incident data, travel time estimates, traffic count data, traffic composition data, link travel time data, and air quality data. This information will also be shared with the entire Coalition for TDM strategic planning and air quality compliance strategies.

The data obtained from surveillance technologies deployed in these areas must be provided to other operating agencies for coordinated response and support. Typical users of this data include the Freeway Traffic Operations Agencies for integrated traffic control, Police and Emergency Organizations (e.g., medical teams or HAZMAT clean-up crews) for incident management, CVFOs for fleet support, Maintenance and Construction Agencies for schedule and planning coordination, and the Coalition for database support.

Transit Authorities

Transit Authorities include public and private transportation services which provide alternative SOV transportation modes to the public, including Park-and-Ride lots to encourage carpooling and public transportation use. Typical operational responsibilities for the Transit Authorities include the acquisition of individual transit vehicle status (e.g., schedule adherence), monitoring traveler security, and monitoring parking facilities.

It will be the operational responsibility of the Transit Authorities to provide the Coalition with route and schedule data, schedule adherence data, probe travel times, and parking lot availability and capacity data. This information will be provided to the Coalition to support TIS and TDM strategies.

The data obtained from surveillance technologies deployed in these areas must be provided to other operating agencies for coordinated response and support. Typical users of this data include the Local and Freeway Traffic Operations Agencies for inter-jurisdictional transportation coordination; Police Organizations, either transit or local police, for traveler security; Maintenance and Construction Agencies for schedule and planning coordination; and the Coalition for database support. Schedule coordination among interlinking Transit Authorities is critical for supporting commuter and interjurisdictional travel.

<u>Commercial Vehicle Fleet Ooerators</u>

In order for electronic clearance and automated roadside safety inspections to be implemented successfully, it will be the CVFOs' responsibility to install the proper AVI equipment and to provide the required data to the Coalition. A joint developmental effort between the Coalition and CVFOs must be established for implementation, planning, and funding purposes.

CVFOs are the main beneficiaries of the implementation of advanced transportation management concepts, such as electronic clearance and automated roadside safety inspections. However, certain transportation agencies will also benefit from the implementation of AVI technologies, such as Toll Authorities utilizing compatible ETTM systems. Additionally, coordinated commercial regulations will benefit the entire Corridor membership. It is also important to note that transportation law enforcement data, such as commercial truck weight information, is integral to the Maintenance and Construction Agencies for pavement maintenance planning.

Typical users of CVFO data will be Toll Authorities for toll collection, Local and Freeway Traffic Operations Agencies for traffic composition data and incident management, and Commercial Vehicle Operations (CVO) Regulatory Organizations to monitor violations.

Maintenance and Construction Agencies

Maintenance and Construction Agencies are responsible for roadway maintenance, such as snow or debris removal and roadway construction coordination. These agencies need to acquire maintenance and construction vehicle identification and location data, plan and schedule snow and ice removal, monitor debris, pavement, and roadway structural conditions, and coordinate with traffic operations agencies to function effectively.

Maintenance and Construction Agencies will be responsible for providing the Coalition with operational plans and schedules and surveillance data. Typical data includes vehicle identification and location data, roadway maintenance plans and schedules, roadway construction plans and schedules, roadway pavement conditions, and snow removal status in the Corridor road network.

The data obtained from surveillance technologies deployed in these areas must be provided to other operating agencies for coordinated response and support. Typical users of this data include both Traffic Operations Agencies and Toll Authorities for coordinated emergency weather conditions operations as well as traffic control during construction, Transit Authorities for scheduling purposes, and the Coalition for database support.

Public Safetv Oraanizations

Public Safety Organizations include agencies whose operations are vital and integral to the implementation of traffic incident management and control response plans. Included within these organizations are state, local, and transit police, fire and HAZMAT removal departments, and emergency medical teams.

For the successful implementation and coordination of traffic incident management and response plans, it is imperative that these organizations agree to operate cooperatively with the respective TOCs. Operational policies and plans must be coordinated among the relative municipalities and Coalition members. Public Safety Organizations will be responsible for providing the Coalition with vehicle identification and location data, incident verification data, and fire and hazardous removal details. The data collected from these organizations is critical to optimizing incident response plans and enhancing traffic safety (e.g., through road improvement and safety law enforcement).

5.9.3 Operational Responsibility Issues

While the operational responsibilities framework defines what information each member is required to provide to the Coalition, coordination of the data collection and subsequent response is a primary responsibility of the Coalition. In order to effectively implement and integrate a Corridor-wide surveillance network effectively, coordination and operational issues must be addressed on a Corridor-wide level. These issues are as follows:

+ Multi-jurisdictional coordination.
+ Regulations coordination.
+ Data and interface standardization.
+ Coverage.

Each of these issues is related to the operational efficiency of the Corridor-wide surveillance network, and should be addressed.

<u>Multijurisdictional Coordination</u>

Multijurisdictional coordination is a critical issue which must be addressed to ensure the successful operation of a Corridor-wide surveillance system. The coordination of network operations and event responses between multiple jurisdictions is vital to meeting the Coalition's mission of cooperative operational management. Certain operations may require resources from multiple jurisdictions and the coordination of surveillance information will assist in tracking these resources at the regional level. For example, incident events and responses in one jurisdiction may impact neighboring jurisdictions. Therefore, a coordinated response and resource allocation would benefit all affected jurisdictions. Coordination is the principal issue, because its ideal configuration and implementation generally ignore agency boundaries.

In order to provide a means to coordinate, sufficient and appropriate data sources throughout the Corridor will have to be established. The Coalition must address institutional management and information sharing in order to implement a fully integrated system. Resources such as the

Informational Exchange Network and a centralized database will provide member agencies access to the data, allowing both real-time and regional coordination.

Regulations Coordination

Since multiple states and transportation authorities are members of the Coalition, imposing and enforcing regulations globally will prove to be difficult. There is more than one set of regulations to consider. To address this issue, member agencies may generate a set of Corridor-wide regulations. Minimally, member agencies should coordinate which ITS technologies are to be utilized in the Corridor. For example, various fee structures charged for commercial vehicle use of roadways may be standardized, or fee collection may be integrated between Coalition members in order to both reduce delay experienced by commercial traffic and assist in assessing fees. In fact, efforts such as the E-Z Pass are being coordinated at the regional level for standardizing electronic toll collection technologies. This type of initiative should continue and expand to address other issues related to surveillance standards. In addition, member agencies can make the entire Coalition aware of regulatory restrictions that may be passed on to the Corridor traffic.

Privacy is a separate public concern with the general usage of ITS technology. Present and planned surveillance components are able to collect data which can be perceived as private (i.e., AVI and GPS technology identifies vehicles, speeds, and routes). This is a sensitive issue that must be addressed by Coalition members in order to gain and maintain public confidence. As stated in the National Program Plan for ITS, dated November 1994, utilizing surveillance devices for law enforcement of privately owned vehicles must be considered very carefully. In order to encourage public appreciation of ITS, it is critical that the general public be aware of the benefits that ITS can provide. Increased public confidence will allow the Corridor Coalition to provide more benefits because confidence will lead to the increased use of ITS services by the public.

Data and Interface Standardization

Data and interface standardization represents the physical side of the coordination introduced in the previous issues. As there are several sources of surveillance data available at present, there are also several methods of data collection and data formats. In addition, future technologies will introduce new data and formats required by the Coalition. Simply, standardization of methods for storing data in the central database will need to be coordinated by the member agencies.

Standardization will provide efficiency in terms of data storage and the development of communication and interface networks to the member agencies. Standardization of operations and maintenance of surveillance components within the Corridor will provide a baseline for agencies to utilize when establishing operations and maintenance criteria.

Coverage

The final major issue to consider is coverage. This includes both physical and functional coverage of the network. Member agencies have variable funding and local goals. Potentially, this will promote variable growth rates of the surveillance network from region to region, agency to agency. Coordination between the member agencies will be required to accommodate physical and functional gaps in the surveillance network. Coordination between the agencies will allow for identification of these existing gaps and planned coverage, allowing for proactive activities to respond to these gaps. For example, if airborne surveillance technologies are implemented, a clear arrangement for meeting surveillance coverage requirements will need to be coordinated between multiple jurisdictions.

5.9.4 Summary of Operational Responsibilities Framework

The surveillance system envisioned, is not that of a single system operated and maintained by a single agency, but rather that of a series of individual systems, each operated in close coordination with the others, and remaining under the jurisdiction of the individual states or authorities. A central clearinghouse for traffic and incident data is the principal component which binds the Coalition together. Under this vision, it is the responsibility of each of the individual agencies, authorities, or organizations to plan, design, implement and operate their individual surveillance system in close coordination with the others. All surveillance systems implemented under each of these agencies will remain under the jurisdiction of the individual operating agencies. Additionally, it is the responsibility of these agencies to provide their surveillance data to the Coalition.

It is the Coalition's responsibility to coordinate and provide access to'sutveillance data across the Corridor, initiate the necessary interagency cooperative agreements, develop and maintain a central clearinghouse database, establish compatibility of technology, standardize data formats, and define communication protocols.

5.10 SUMMARY

This Chapter began with the description of the operational concepts and operational scenarios for the I-95 Corridor-wide Surveillance System based on the functional needs identified in the goals and objectives survey. These concepts and scenarios form an initial basis for exploring the various functions that the system has to perform. A systems engineering methodology was applied to define the functional requirements for the surveillance system. These functional requirements are technology independent and serve as a foundation for defining the communication, interface, software, and hardware requirements, as well as for formulating the conceptual systems design. The functional requirements definition process has also helped to define the boundary of this Project as distinct from other Corridor Projects. A number of common were identified, leading to more well-defined inter-project coordination.

To facilitate the development of other communication, interface, software, and hardware system requirements, assumptions regarding the Corridor-wide surveillance system hierarchy were made. The hierarchy includes three levels (field, state and local operations center, and Corridor) that are consistent with the vision of the Coalition. Based on this hierarchy, detailed communications, interface, software, and hardware requirements were developed for the lowest two levels to avoid duplication of effort with the Information Exchange Network Project (Project # 1). Furthermore, interface requirements to allow the exchange of surveillance information from one level or entity to another were also provided.

The last part of this Chapter describes a framework for defining the surveillance operational responsibility of the Coalition member agencies. This framework follows the present functional and modal responsibilities of the participating agencies. The focus of the framework was to foster a cooperative relationship between the members while preserving their operational autonomy.