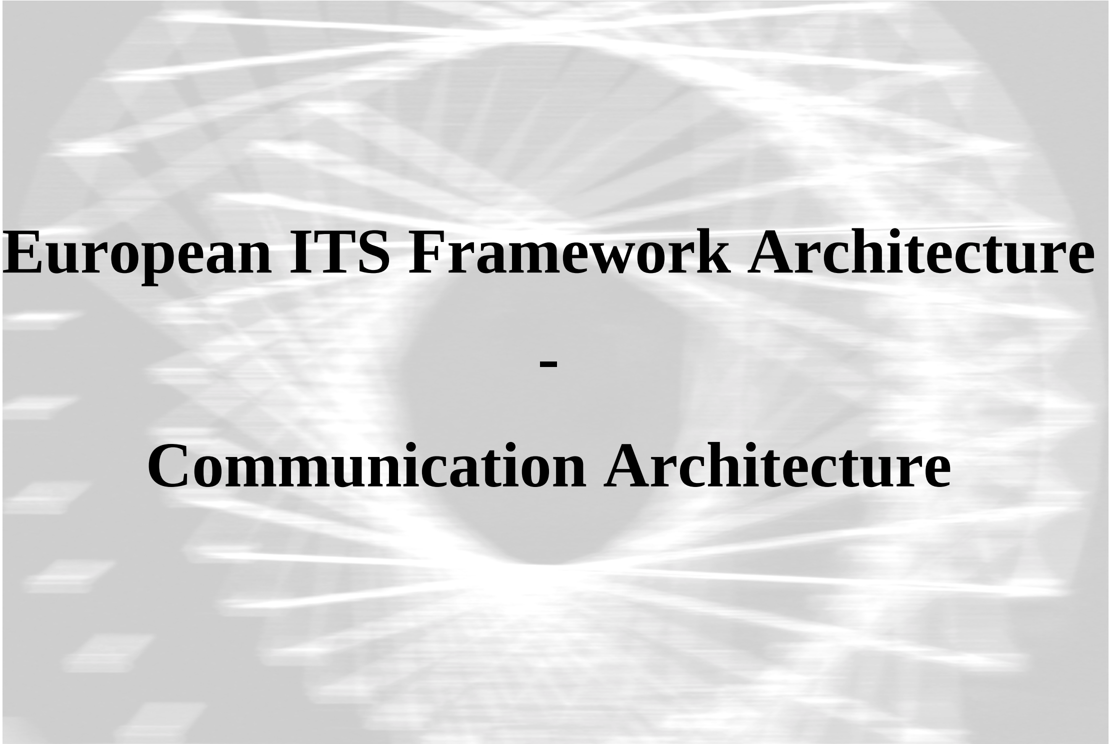


European ITS Framework Architecture

-

Communication Architecture

D3.3 - Issue 1

August 2000

This public report has been produced by the KAREN (Keystone Architecture Required for European Networks) project, as part of the 4th Framework Programme - Telematics Application Programme – road sector.

KAREN partners contributing to this report are:

EXPERTEL – GROUP FRANCE TELECOM
ERTICO
ISIS
SIEMENS TRAFFIC CONTROLS LIMITED
MANNESMANN PASSO
AEROSPATIALE MATRA
ALCATEL AUSTRIA

Neither the European Commission, nor any person acting on behalf of the Commission is responsible for the use which might be made of the information in this report. The views expressed are those of the authors and do not necessarily reflect Commission policy.

Document control sheet

Activity name: KAREN

Work area: Framework Architecture Development - WP3

Document title: Communication Architecture

Document number: D3.3

Electronic reference:

Editor: Richard Bossom

Main author(s): Michael Büter, Guillaume. Fraigneau, Jean-François Gaillet, Thierry Peson, Markus Szvetits, Jean-François Jouen

Dissemination level[1]: Public usage

Version history:

Version number	Date	Editor	Summary of changes
Issue 1	August 2000	R.A.P. Bossom	Final Public Issue

Approval:

	Name	Date
Prepared	*Richard Bossom*	*August 2000*
Reviewed	*Gino Franco*	*August 2000*
Authorised	*Jan Willem Tierolf*	*August 2000*

Circulation:

Recipient	Date of submission
CEC	August 2000

[1] This is either: Restricted (to the programme, to the activity partners) or for Public usage

Table of Contents

Figures

Tables

Executive Summary

This Document provides a description of the Communication Architecture which forms part of the European ITS Framework Architecture. A Communication Architecture defines and describes what kind of communication links needs to be used in a System in order to support its physical data flows. These physical data flows are presented in the European ITS Physical Architecture provided in a separate document produced by another part of the KAREN Project.

The Communication Architecture is described in some detail by this Document, which also covers the methodology used for its development. The basic concepts of communications are discussed, including general points about the characteristics of links within Systems between different physical locations, and between Systems and the parts of the outside World with which they interface.

The communications requirements of several of the "example Systems" in the European ITS Physical Architecture are described and analysed. Conclusions about the best type of communications to use are also provided.

A brief description of current communications technologies and an overview of the OSI model are included in Annex 1. This is provided as a separate Document for ease of use and reference. The actual data used for the analysis of the "example Systems" featured in the main part of the Document is included in Annex 2.

1 Introduction

1.1 Scope

This Document is part of the set of deliverables produced by the KAREN Project to describe the European ITS Framework Architecture. This particular document (D 3.3) provides a description of the Communication Architecture that has been developed by the Project Team. The background to the development of the Framework Architecture is provided in the European ITS Framework Architecture Overview document (D 3.6) – see reference 10(d).

1.2 Where the Document fits in the Architecture Documentation

The Document is one of a set of seven documents provided by the KAREN Project to describe the complete European ITS Framework Architecture. The other documents in the set are as follows:

D3.1	European ITS Functional Architecture
D3.2	European ITS Physical Architecture
D3.3	European ITS Communications Architecture - this document
D3.4	European ITS Cost Benefits Report
D3.5	European ITS Deployment Study Report (internal use only, but included in D4.2)
D3.6	European ITS Framework Architecture Overview
D3.7	European ITS Models for ITS deployment

The other Documents can be obtained from the reference shown in the last Chapter of this document. Note that throughout this Document, any references to the “KAREN Architecture”, refer to the “European ITS Architecture”.

1.3 Definition of a Communication Architecture

A Communication Architecture defines and describes the means which support the exchange of information between different parts of the System. This information exchange is carried out using Physical Data Flows that are described in a Physical Architecture. In the KAREN context, this Communication Architecture defines and describes the means to support physical data flows for some of the “example Systems” in the European ITS Physical Architecture. This is described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This in turn refers to the European ITS Functional Architecture (D 3.1) – see reference 10(b) for the definition of the data in each Physical Data Flow.

The description and definition of the means to support physical data flows concerns two complementary issues. The first issue is to provide the means that enable data to be transported from one point to another and that the way this data is transported is suitable for the System in terms of cost, alteration and delay. In other words, the issue is to describe and define the “pipelines” that are needed to transport the information. The second issue is to make sure that the information sent from one end of the “pipeline” is interpreted without deviation at the other receiving end of the “pipeline”.

These two issues are addressed by the European ITS Communication Architecture. The first one requires an analysis which leads to the definition and description of the communication links at the main interfaces of the System. The second one reflects the needs for private or standard protocols. As part of the European ITS Communication Architecture, this leads to the description of existing standards in this Document. However further analysis on these standards will be found in the European ITS Framework Architecture Deployment Approach and Scenarios Deliverable Document (D.4.1) – see reference 10(e).

The Communication Architecture forms part of the European ITS Framework Architecture and therefore shares its characteristics. These characteristics are described in the European ITS Overview Document - see Deliverable D 3.6 – see reference 10(d).

1.4 Document Structure

The documentation of the European ITS Communications Architecture has been divided into two parts. The first part is the Main Document (this document) and the second part is the Annex, which is in a separate Document. Each contains Chapters. The rest of this section describes those that are in this (the Main) Document, with each one being identified by its number in brackets (n).

This Document starts off with Chapters that describe the methodology for the communications architecture analysis work (2), the links with other parts of the European ITS Architecture (3), links with the outside World (4) and an introduction to some concepts used in the rest of the Document (5).

The discussion of the results of the analysis of the physical data flows in some of the “example Systems” from the Physical Architecture is provided in Chapter 6. This is followed by Chapters on the general characteristics of Links between different physical locations (7) and Links with the outside World (8). Finally in Chapter 9 there is some discussion of the impact of standards.

1.5 List of Abbreviations

DFD	Data Flow Diagram
EP	Electronic Payment
ITS	Intelligent Transport Systems
KAREN	Keystone Architecture Required for European Networks
LMDS	Local Multi-point Distribution Service
MMDS	Microwave Multi-point Distribution Service
PMR	Private Mobile Radio

PT	Public Transport
P+R	Park and Ride
SMS	Short Messaging Service
TCC	Traffic Control Centre
TIC	Traffic Information Centre
TICS	Transport Information and Control Systems

2 Methodology

2.1 Introduction

This Chapter of the Document describes the methodology that has been used to develop the European ITS Communication Architecture. It has been included to provide readers of this Document and users of the Framework Architecture with information that will help them to have a better understanding of how the conclusions and recommendations in later Chapters were produced.

2.2 Discussion on the Method

2.2.1 The pipeline and the language issues

As stated in section 1.3, a Communication Architecture defines and describes the means that support the exchange of information between different parts of the System. In the KAREN context, this Communication Architecture defines and describes the means to support physical data flows.

Again as noted in section 1.3, describing and defining the means to support physical data flows is concerned with two complementary issues. These two issues need to be addressed with two different methodologies.

Figure 1 The Pipeline/Telecommunication Issue

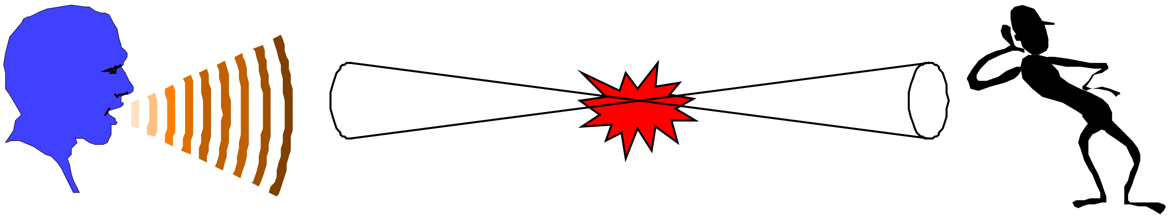
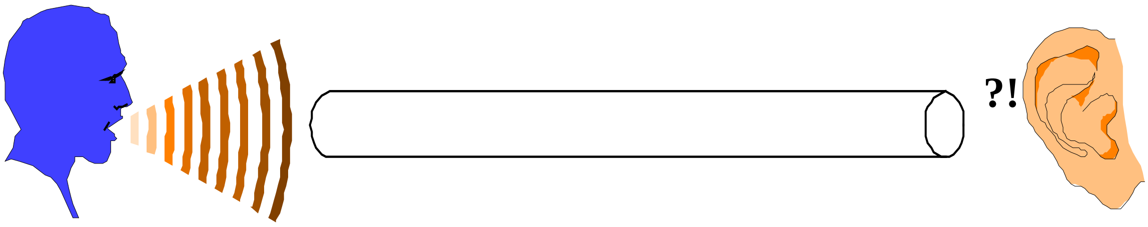


Figure 2 The Language/Standards Issue



The first issue is to provide the means that enables data to be transferred from one point to another, and that the way this data is transported is suitable for the System in terms of costs, alteration or delay. In other words, the issue is to describe and define the pipelines needed to transport the information. Technically speaking, the pipeline issue is dealing with the 4 lower layers of the OSI model: the physical, data link, network and transport layers - see Annex 1 for a short introduction to the OSI model.

Like the other components of the European ITS Architecture, the Communication Architecture must remain as much technologically independent as possible. Hence, the issue will be examined here from a generic point of view. To achieve this, the methodology proposed here is that the physical data flows from the most representative “example Systems” in the European ITS Physical Architecture are characterised and analysed to derive the most representative telecommunication needs at different interfaces of the System.

Describing these typical telecommunication needs is the first achievement of the Communications Architecture. Telecommunication technologies are changing so fast that it is not possible to provide a technology driven Architecture valid in the long-term. However the generic description of typical physical data flows, like the one proposed here, remain valid as long as the picture of the most representative “example Systems” does not change too much. Hence, this will provide solid ground for analysing issues related to telecommunication in ITS in general.

Together with the telecommunication issue, a second issue is also paramount as far as communication is concerned. This issue is to make sure that the information sent from one end of the pipeline is not only understood but also interpreted without deviation at the other, receiving end of the pipeline.

At first sight, it is just a matter of standards that must be agreed upon so that different parts of the System may exchange data in the most efficient way. But in fact, the ability of a System to provide services completely depends on the data it is processing. Hence, at stake is not only what kind of data is to be processed but also what level of detail is used to describe analysed objects. Other technical questions, such as where data is stored and which part of the System is processing which part of the data, must not be omitted. They often lead to very different kinds of exchanges and, thus, to very different kinds of message standards.

Moreover, it is clear that the way data is exchanged between different parts of the System is a crucial matter within a System, and that it triggers its capacity to provide one service or another. Since ITS has emerged from the development of many different manufacturers with different objectives, the emergence of common standards is a long and difficult process which will need strong support if interoperability is to be achieved.

As this standard issue is one of the paramount issues for the ITS world, a separate study has been planned in the European ITS Framework Architecture to examine it more thoroughly. The results are presented in Deliverable Document D 4.1 “Standardisation Framework”. Nevertheless, as it is also part of the Communication Architecture issue, an analysis of existing standards is provided in Chapter 9 of this Document.

2.2.2 The telecommunication issue

As discussed above, the Communication Architecture has to deal with two issues. This section describes KAREN Project approach towards the telecommunication issue.

Telecommunication choices are often made through complex processes and after different analysis stages. In fact, telecommunication choices have most of the time a large impact on a System and on its efficiency. The System studied here does not go against this rule: several important matters must be considered when designing a Communication Architecture. These are described below.

The first matter is to satisfy the System needs as well as possible. In fact, the telecommunication offer is not so wide that any need can be satisfied. Additionally, even if technical solutions are available, costs analysis may dictate not to take advantage of them. As consequence, most of the time, a System is designed in close relation with its Communication Architecture. Besides, when Communication Architecture evolutions are envisaged, it often implies an evolution of the System itself.

The actual design of the System (such as location of the data, location of the functions that process the data, level of detail of the data, etc.) is deeply correlated to its Communication Architecture. Hence, it is not feasible to derive a Communication Architecture directly and solely from a Functional Architecture. It is necessary to take into account technical choices made in actual implementations of the System. Hence, the first step of the approach will be based on the analysis of the most significant “example Systems” from the European ITS Physical Architecture, and the development of hypothesis on their implementations.

The second matter is to actually insert the telecommunication solution envisaged in the existing System. At stake are questions such as how to integrate the telecommunication solution into the existing telecommunication frame; how to make the latter evolve; or how to replace it. In the same manner it is important to make choices that will be valid in the long term. This means making sure that the solution will be able to evolve while the System is evolving, that it will support these changes, and that it may be replaced as easily as possible by another solution when it becomes obsolete.

This is a true organisational and technico-economic matter when implementing an actual solution, but it may also be tackled at a generic point of view.

In the frame of ITS, some parts of the System, such as the *vehicle*, for instance, may be related to other parts of the System for many different purposes. But, this does not mean that there must be as many telecommunication means as purposes. In order to simplify the implementation of ITS solutions and to lower costs, it is necessary that telecommunication means are shared for different purposes. To deal with this matter, a second step of the approach will lead to the identification of typical communication links that can be found at different interfaces of the System.

Last, but not least is the matter of costs. Costs are mainly linked with the acquisition of the solution, with the migration from the former solution to the new solution, with the running of the solution, and with the replacement of the solution. These costs must be considered not only in terms of material and services, but also in terms of personnel involved in all these phases. This matter is also very deeply linked with implementation choices and will not be addressed here. It has been actually covered by the KAREN Project in a separate costs and benefits study – see European ITS Costs and Benefits Study Deliverable Document (D 3.4) – see reference 10(f).

For the definition and description of a Communication Architecture, all these matters must be taken into account. Of course, the KAREN Project does not intend to deliver the technical solutions that perfectly suit the System, since such solutions do not exist. The Communication Architecture is based on generic approach that gives a frame where most important matters are tackled. This frame gives a global vision of the telecommunication issue that enables economical and technical issue linked with designing ITS solutions to be addressed more efficiently.

2.2.3 The standards issue

Standards for the telecommunications that are used by ITS have been in existence for some time. They have evolved over time following developments in communications technology and the data requirements of ITS. In recent times there has been an explosive growth in the use of telecommunications in many other sectors, e.g. e-commerce. The net result is that ITS can no longer expect to develop its own standards, except where it can be sure that it will use its own (private) infrastructure. If it wishes to make use of communications networks that already exist (e.g. line sharing) then it must use standards that are set by others.

Using existing communications networks is now seen to make economic sense, since it relieves the ITS owner and/or operator of the need to provide and maintain their own networks. Sometimes the cost savings can be significant because the communications load (band width) imposed by ITS data traffic is small in comparison with that imposed by other users. However as noted above, the penalty is that ITS must use standards that are set by those using the greatest bandwidth. If dedicated standards are to be used for ITS communications over shared networks, then they must be based on those supported by the users of the greatest bandwidth.

3 Relationship with the European ITS Physical Architecture

3.1 Introduction

This Chapter is intended to “set the scene” for the subsequent analysis of the communications needs of several of the “example Systems” that make up the European ITS Physical Architecture. It provides an introduction into the “Systems” themselves, to make the analysis in Chapter 6 more easily understood.

3.2 Relationship with European ITS Physical Architecture

3.2.1 Principles

In the European ITS Framework Architecture, the Physical Architecture has been defined in a separate Deliverable Document (D 3.2) – see reference 10(c). This Deliverable, provides descriptions of several “example Systems”. These show some of the ways in which the European ITS Functional Architecture can be used to produce Intelligent Transportation Systems (ITS), and/or Architectures that will support them. Therefore there is no “standard” or all encompassing European ITS Physical Architecture, or physical implementation of the Functional Architecture.

In view of this the purpose of the European ITS Communications Architecture is to show how the communications needs of Physical Systems and Architectures can be analysed so that the requirements can be determined. This has been done by studying the communications needs of several “example Systems” from the European ITS Physical Architecture. The results of the studies are recommendations on the types of communications that could and should be used by each of the “example Systems”.

3.2.2 Studied systems

Some of the “example Systems” from the European ITS Physical Architecture (D 3.2) – see reference 10(c), have been analysed for the Communication Architecture. A brief overview description of those involved is given on this and the next page.

- Integrated Traffic Management Systems (Area Integrated Traffic Management): Three of the systems in this area have been analysed. They are as follows.

  P1 - Integrated Urban Traffic and Public Transport Management System. This “example System” offers comprehensive traffic and travel real-time data at different levels of detail and complexity. It also provides communication channels to deliver services to the travellers and interfaces to outstanding ITS application protocols. It is based on an open environment, called TITOS (Torino ITS 2000 Open Showcase), which will be tested at the 7th ITS World Congress in Turin, Italy. TITOS will include state-of-the-art ITS components and infrastructures forming a “real-life” open platform implementing the most recent results in the field of system architecture, communication standards, service specifications and data exchange open specifications.

P2 – RDS-TMC Italian System. This “example System” is based on the RDS-TMC (Radio Data System – Traffic Message Channel) Italian service. It broadcasts comprehensive localised traffic and travel real-time data at the national level (highways and motorways). The RDS-TMC Italian service allows delivery of high quality, timely and relevant information during radio normal services and in the language chosen by the user. The system represents the RDS-TMC traffic information centre, at which, data and traffic events are collected, validated and properly coded to be passed to the RDS-TMC service provider and then to the public broadcaster.

P3 – Urban Traffic Control and Public Transport Priority System. This “example System” is based on the SPOT/UTOPIA (Urban Traffic Optimisation by Integrated Automation) system. It has been specifically chosen to represent the architectural solutions adopted by a decentralised system. The system aims at improving urban travel conditions by the application of fully automated hierarchic control principles which optimise dynamically operation of traffic lights in urban areas. Optimisation is based on real time data continuously measured plus historical data and knowledge of special events. The system also interacts with the AVM (Automated Vehicle Monitoring) system, which has the task of monitoring and forecasting the movement of the urban public transport fleet. The provision of this information is necessary for the System to give priority to public transport vehicles. It also includes the so called Multifunctional Outstation (MFO) which can interface to traffic signal controllers and other roadside equipment. This enables the delivery of other services such as public transport information.

- Electronic Cash Transaction System (P10, Area Electronic Fee Collection): This “example System” provides the facilities for handling the basic electronic cash transactions associated with the use of Automatic Fee Collection for the payment of transport telematic services. The system uses an electronic travel pass to pay for a number of different services. It is based on the Conceptual Model described in ISO standards and supports different payment modes, a wide variety of transport and transport related services, security and privacy and co-ordination between the collectors of money, charging points etc.

- Hazardous Goods Management System (P22, Area Safety and Emergency): This System deals with critical situations relating to the transport of hazardous goods. It provides options to monitor the route of hazardous goods and minimises the risk and the reaction time in the case of an accident. It makes use of in-vehicle sensors and on-board processors to monitor the goods in order to avoid critical situations caused by improper storage. This equipment also receives information from roadside systems or via broadcast. In case of an emergency either a manual (driver-operated) or an automatically released emergency signal will be generated. The system also involves a control centre, which fulfils a supervisory role.

- Urban Traffic Management System (P30, Area Traffic management): This System provides facilities that enable the management of road traffic that is using an urban road network. In addition to the actual traffic management facilities, the System includes additional facilities for the maintenance of the physical road network and the equipment used by the System for the management of traffic. Emergency Vehicle priority is provided using equipment on-board the Vehicle that links to local System equipment at the roadside. Links from this System to other Systems are also provided to enable co-ordination of traffic management across organisational boundaries.

- Inter-Urban Traffic Management System (P31, Area Traffic management): This System provides facilities that enable the management of road traffic that is using an urban road network. In addition to the actual traffic management facilities, the System includes additional facilities for the maintenance of the physical road network and the equipment used by the System for the management of traffic. Emergency Vehicle priority is provided using equipment on-board the Vehicle that links to local System equipment at the roadside. Links from this System to other Systems are also provided to enable co-ordination of traffic management across organisational boundaries.

- Traveller Assistance and Route Guidance System (P60, Area Traveller Assistance): This System provides facilities that enable a traveller to plan journeys in advance and then execute them. Additional facilities are provided that enable the traveller to take account of changes in relevant conditions for the journey and thus update the journey plan. Means to provide the user with on-line guidance while the journey is in progress, even if the user is located inside the vehicle and on the move, are added to the system.

A full detailed description of each of these “example Systems” can be found in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c).

4 Communication Architecture links to the outside World

4.1 Introduction

This Chapter provides the definition and description of the terminators for the European ITS Functional, Physical and Communication Architectures. A table of acronyms is provided that will be used throughout the rest of this document.

4.2 Definition of Terminator

A terminator is the representation of the outside World to the Framework Architecture. It provides a definition of what the Architecture expects the outside World to do, the data the outside World is expected to provide, and the data to be provided to the outside World by the Architecture. A terminator may be a human entity, a System, or a physical entity from which data can be obtained such as the atmosphere, or road surface. Both human entities and Systems may be part of Organisations or Public Authorities that contribute in some way to the provision of ITS services. A rigorous definition is provided for each Terminator and will be found in the European ITS Functional and Physical Architecture Documents (D 3.1 and D 3.2) – see references 10(b) and 10(c).

4.3 Physical Terminator Links analysed in the Communications Architecture

Only physical terminator links to non-human entities are analysed in the Communications Architecture. This is because the links to human entities are concerned with non-electronic communications issues such as ease of access, presentation etc. However a discussion of some of the issues that are part of the links to human entities will be found in Chapter 8 of this Document.

5 Communication links, communication ends and Physical Interfaces

5.1 Introduction

This Chapter introduces the concepts of communication link, location and physical interface that will be used throughout this Document.

5.2 Definitions

5.2.1 Communication Link

A communication link is the communication means that support Physical Data Flows. In "example Systems" from the European ITS Physical Architecture that are analysed in this Document, they can be found transferring data between two Sub-systems or between a Sub-system and a terminator.

5.2.2 Location, source and sink

Situated at each end of a communication link, locations are the places where Physical Data Flows originate (sources) or are received (sinks). Communication ends are the entity that can be found at the each end of communication links. A communication link may link one or several instances of a sink to one or several instances of sources. Locations are defined in the Chapter 2 of the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c).

5.2.3 Physical Interfaces

Physical interfaces are the part of the System through which communication links must be established. They can be found between two Sub-systems or between a Sub-system and a Terminator. Physical interfaces are defined by the location of their communication ends.

6 Analysis of example ITS systems

6.1 Introduction

This Chapter analyses Physical Data Flows from different “example Systems” as they are described in the European ITS Physical Architecture - see the brief overviews given in Chapter 3 of this document and the Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). These Systems need telecommunication links to support their Data Flows. In particular this Chapter studies the support of Data Flows between different sub parts of the Systems (internal communication) and support of Data Flows between the Systems and external entities (terminator communication).

For all the Systems, requirements concerning telecommunication links to be implemented have been characterised. From these requirements, diverse recommendations have been derived, including recommendations concerning the type of technologies that should be considered to implement a solution. The requirements for each Physical Data Flow can be found in the tables included in Annex 1.

6.2 Integrated Traffic Management: System P1

6.2.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P1 (Integrated Open System for Traffic and Travel Information Services) described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two sub-sections:

- Internal communications which deal with the communication flows between different locations of the system
- Terminator communications which deals with communication between the system and the terminators

In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The P1 System offers comprehensive traffic and travel real-time data at different level of detail and complexity. Moreover it provides available communication channels to deliver services to the travellers and interfaces to outstanding ITS application protocols.

It is based on an open environment, called TITOS (Torino ITS 2000 Open Showcase), which will be tested at the 7th ITS World Congress in Turin, Italy. TITOS will include state-of-the-art ITS components and infrastructures forming a “real-life” open platform implementing the most recent results in the field of system architecture, communication standards, service specifications and data exchange open specifications. By simply plugging-in the TITOS platform, participants will show their services or products through three different levels of interactions:

- Participants will have free access to real data from the Turin city, national and international traffic data, tourist and congress information. Examples of information provided by the 5T system (the system for the traffic and travel control and information in Torino) include vehicle flows and speeds, travel times, queues, pollution predictions and measurements, public transport travel times and timetables and car park availability.
- Subject to special agreements with 5T, it will be possible for interested service providers to benefit from processing engines that are made available by 5T and are capable of providing processed data on demand, to be used as a basis for value added services. Processing engines include information on incidents, congestion and anomalies detected on specified routes (both private vehicles and public transport network), the quickest route to reach a destination and collective re-routing information calculated according to the global dynamic control strategies.
- Finally, there will be free access to different communication channels to deliver services to final users. The communication media available as a minimum will be RDS-TMC, DAB/DMB, GSM, Televideo/Teletext and Internet.

The System aims at describing a complete ITS application where TITOS represents the core component, as the principal issue of this example is to show the inter-operability of the various actors involved in a “plug and play” working environment. Obviously, other components (e.g. traffic and travel information sub-systems) and infrastructures are needed to provide a basic operative system. These components complete the ITS application considered here.

The figure on the next page describes the overall communication links of the P1 system. To generalise the communications requirements, we have enlarged the scope of the system, and especially its cover. We consider here a network linking 10 metropolitan areas, each one including 10 cities having their own local sub-system.

The systems exchange data with 9 Terminators. Only 6 out of these 9 Terminators are considered in this section, others are human-machine interfaces or "physical interface" which do not require telecommunication support. These six Terminators are

(1) Related road System,

(2) Emergency Systems,

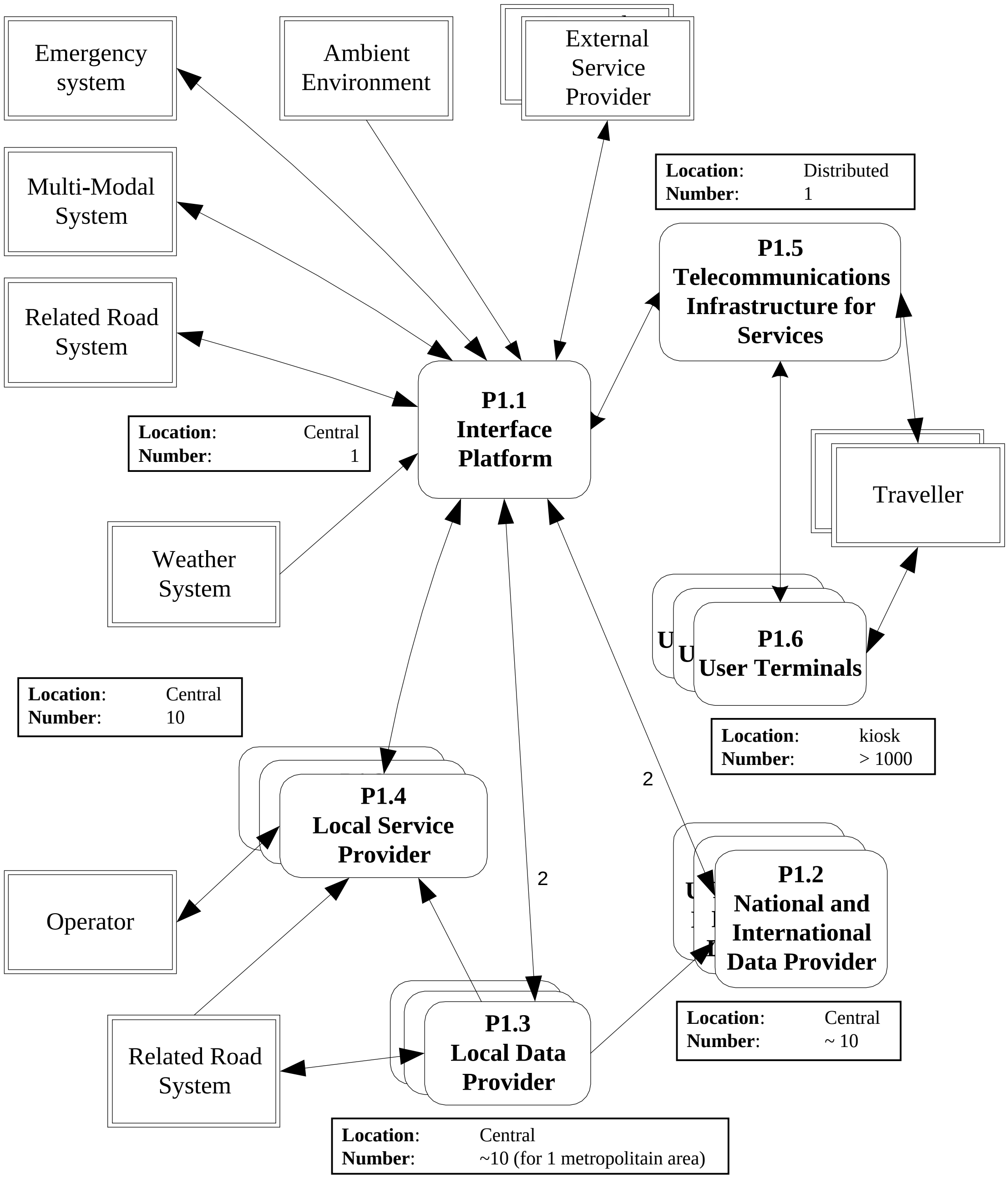
(3) External Service Provider,

(4) Weather systems,

(5) Multi-modal Systems.,

(6) Traveller (when entering the system via personal computer).

Figure 3 P1 System Diagram



6.2.2 Internal Communications

The P1system is mainly centralised. Four of its six sub-systems are thus centrally localised. The sub-system P1.6 (User Terminals) is distributed in many kiosks, while P1.5 (Telecommunications Infrastructures for Services) is in fact spread over several places, as it encompasses most of the telecommunication means required for the links with the travellers. The internal communications between the different sub-systems are therefore limited to :

- Central ↔ Central

- Central ↔ Kiosk

The central sub-systems are nonetheless not automatically located in the same place, but can be scattered in different premises all around the country. This is a question of organisation, and even if grouping all the sub-system in the same building makes things easier for communication links, other considerations can lead to different solutions. Furthermore, the idea of linking local sub-systems situated in distant cities lead to long distance or at least regional communications links, even between central systems.

The kiosks supporting P1.6 are distributed throughout the cities (and at the main transportation terminals : airport, railway stations, ...) to allow travellers easy access to the different services provided.

6.2.2.1 Central ↔ Central Requirements

As mentioned above, this link can be between two distant sub-systems, or between two entities both located in the same building.

The data transported by the internal networks concern three kinds of message.

1 Information or service requests from Travellers, that are routed first by P1.6 to P1.1. They distribute them to the appropriate entity, being either P1.4 (Local Service Provider.) or a terminator (cf. later on Terminator connections or directly processes them if it possesses the information required (information on traffic conditions or weather for example). These messages are very frequent (several thousands per day), can be emitted by thousands of customers, require short transmission time (up to a few seconds), and should be small (less than 1 kB). They may be local, regional or long distance. The integrity requirements are not severe;

2 Corresponding answers which follow the same path on the other directions. The frequency and response times are similar, but the size could be bigger, as some answers could for example consist in entire schedules chart, traffic condition maps, ...So messages up to 100 kB can be envisaged, requiring large bandwidth (around 100 kB/s) if the system is to be accepted by users;

3 Traffic information, either local, national or international, provided by P1.2 (National and International Data Provider) or P1.3 (Local Data Provider), or supplied to them by P1.1. These messages size should be of a few kB each, sent every few minutes, with up to several tens of them transmitted at the same time. Maximum transmission delay is also less than 10 seconds. As mentioned above, the analysis of this system should not be limited to one metropolitan area, as the concept allows connections between several areas, each regrouping different local systems.

Generally speaking, the P1 “example System” does not require any specific confidentiality or identification procedure.

The transmission distance to be covered by P1 depends on the size of the geographic area that it serves. If we consider a national geographic area, it requires long distance transmission between P1.1 and different instances of P1.2 or P1.3.

6.2.2.2 Central ↔ Central Technical Recommendations

As all the sub-systems are fixed, it seems logical to choose a wired communications system.

6.2.2.3 Central ↔ Kiosk Requirements

The messages transmitted through this channel consist in information request and corresponding answers, as described in the previous paragraph, except that the number of potential emitters is much reduced. This is because there may be one kiosk for one or several potential users (Travellers). The other requirements are similar.

6.2.3 Terminator Communications

As described above, the system exchanges data with 9 Terminators. Only six out of these 9 Terminators are considered in this section:

0 Related road System,

1 Emergency Systems,

2 External Service Provider,

3 Weather systems,

4 Multi-modal Systems,

5 Traveller (when entering the system via personal computer).

Others are human-machine interfaces or physical interfaces that do not require telecommunication.

6.2.4 Related Road Systems ↔ Central

This connection can be considered as a long distance one, and several RRS could be connected at the same time. It concerns the following types of messages:

1. Traffic Information. exchanged between the different systems. Those messages could be sent regularly, or event-triggered. But for the dimensioning, the frequency could be considered to be of a few minutes. Messages size should be of a few kBs, with maximum transmission delay of a few seconds, hence a required bandwidth of a few kB/s.;

2. Service Requests. These messages should be of small size (a few tens of Bytes), with a transmission delay inferior to one second. On another hand, many simultaneous messages could be sent at the same time;

3. Corresponding Answers. The size is much larger (up to a few kB), with the same acceptable transmission delay. As several answers could be transmitted at the same time, the throughput should be greater than 100 kB/s.

No particular integrity or confidentiality is required for these messages, if we suppose here that the information is exchanged free of charge between the different systems, which seems logical.

6.2.5 Traveller ↔ Central

This connection can be considered as a long distance one. Up to several thousands connections could co-exist at the same time. The messages are similar to the service request and corresponding answers described for related Road Systems, and so lead to similar requirements, except that here the services should be paid for, so here authentication procedures should be included.

6.3 Integrated Traffic Management: System P2

6.3.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P2 described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two subsections:

- Internal communications which deal with the communication flows between different locations of the system
- Terminator communications which deals with communication between the system and the terminators

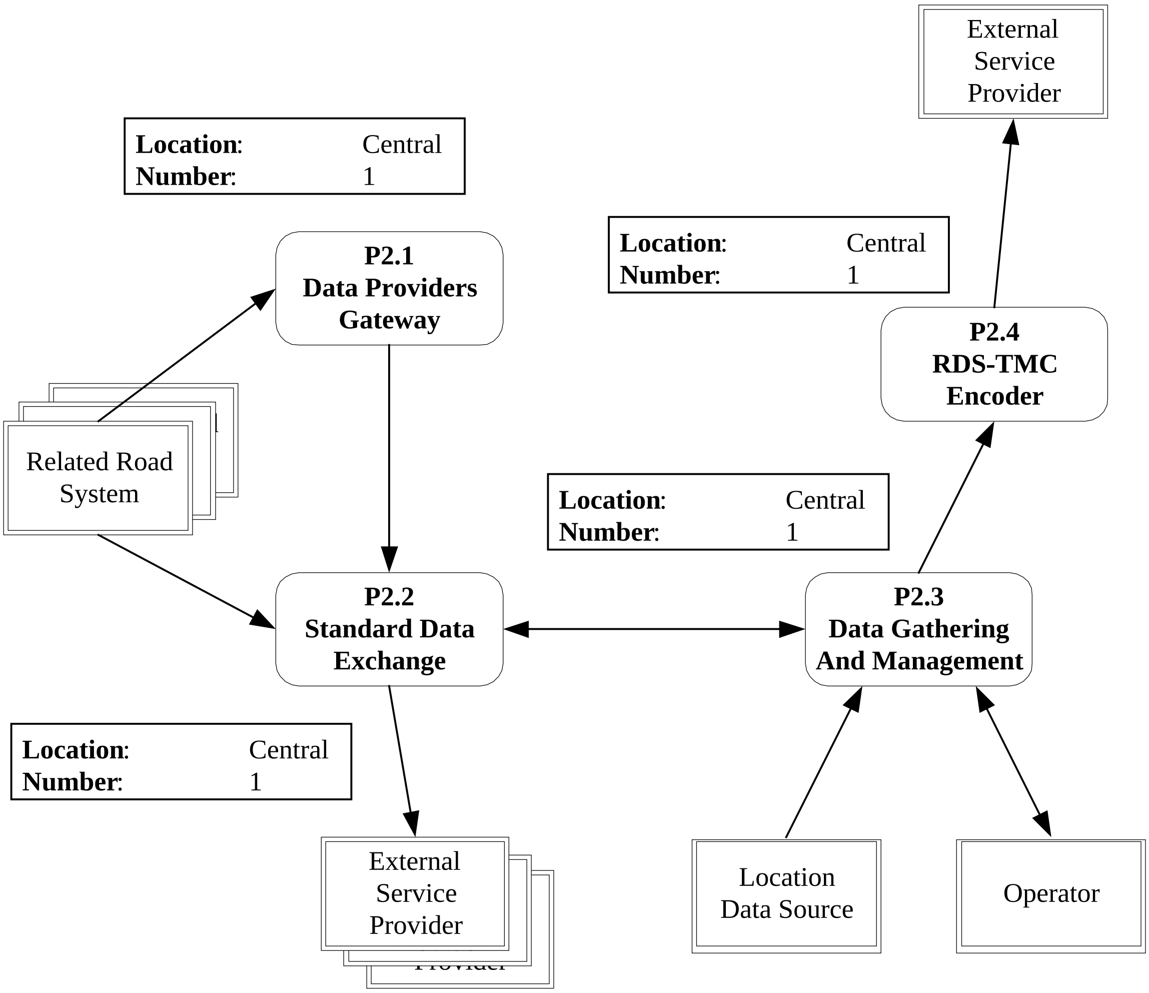
In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The example is based on the RDS-TMC (Radio Data System – Traffic Message Channel) Italian service. It broadcasts comprehensive localised traffic and travel real-time data at the national level (highways and motorways). The RDS-TMC Italian service allows delivery of high quality, timely and relevant information during radio normal services and in the language chosen by the user.

The described System represents the RDS-TMC traffic information centre, on the base of which the RDS-TMC service can exist. Here, data and traffic events are collected, validated and properly coded to be passed to the RDS-TMC service provider and then to the public broadcaster. Moreover, the described System is capable of providing the collected and validated traffic information to any external service provider requiring it i.e. for value added applications.

The figure on the next page shows the overall communication links within the P2 system.

Figure 4 P2 System Diagram



The system exchanges data with 4 Terminators. Only 2 out of these 4 Terminators are considered in this section, others are human-machine interfaces or "physical interfaces" which do not require telecommunication support. These two Terminators that are considered comprise:

(1) Related Road System,

(2) External Service Provider,

6.3.2 Internal Communications

The P2 system is centralised. Its four sub-systems do not have to be located in the same building, but we suppose here that they are situated in relatively close premises. The internal communications between the different sub-systems are therefore limited to Central ↔ Central local communications.

6.3.2.1 Central ↔ Central Requirements

As mentioned above, this link can be between two distant (within local range) sub-systems, or between two entities located in the same building.

The data transported by the internal networks concern two kinds of message, corresponding to different communication ends.

1 The traffic data messages issued by the related road systems, which have been reformatted if necessary by P2.1. These messages, exchanged between P2.1, P2.2 and P2.3 can present sizes up to one hundred Bytes, are transmitted every minute or so (several external sub-systems can be connected to the system, each of them sending its own data to P2.1 or P2.2). Transmission delay must be less than one second, which leads to a required throughput of around 1kB/s and no particular confidentiality or authentication procedure is required. The distance between the communication ends depends on the solution chosen for the location of the three sub-systems.

2 The message to be transmitted via RDS-TMC. These messages, sent by P2.3 to P2.4, are of similar size (some kB), leading to a throughput need of a kB/s or so. The other parameters are similar to those of the first category, and here again the transmission distance depends on the solution adopted for the location of the sub-systems.

As with all Central/Central communication links, wired solutions appear as the most appropriate.

6.3.3. Terminator Communications

As described above, the system exchanges data with 4 Terminators. Only three of them are of interest for telecommunications links: External Service Provider, Location Data Source and Related Road Systems.

6.3.2.2 Central → External Service Provider

This interface is composed of two kinds of messages:

- tesp_traffic_info, which corresponds to the traffic information to be broadcast by the Service Provider. The frequency is about once every few minutes, with message size of a few kB of raw data (once encoded). This message could be sent simultaneously to several Service Providers allowing a better coverage. The communication is of Central / Central nature, and it can be either local, regional or long distance depending on the location of the systems.

- tesp_traffic_data, which corresponds to traffic information validated by the system, and sent to a service provider for use in value added services. The frequency of the messages could vary, the size of the message could be up to hundreds of Bytes. The communication is of Central / Central nature, and it can be either local, regional or long distance depending on the location of the systems.

6.3.2.3 Location data source → Central

This interface is composed maps and location referencing data. As this kind of information presents a long validity period, this connection will be very seldom used. Also because the data is characterised by its huge size, it could be more appropriate to use physical means of transport, such as CD-ROMs for example. Therefore there is no need for real telecommunication link to be used, although this may change in the future with the development of alternative communications technologies.

6.3.2.4 Related Road System → Central

These external systems can send messages to P2 using two different channels:

- if they can use standardised protocols for communications between TICs (as defined in DATEX-Net specifications), they send their messages to P2.2. In this case, messages could be expected with a frequency of one every minute or so, with several RRS connected at the same time. The size could be of a few kB, with transmission delays of a few seconds. The communication is of Central / Central nature, and it can be either local, regional or long distance depending on the location of the systems.

- if they can't, P2.1 allows them to reach the system using other means of communication (even Fax, telephone, ...). In this case messages could be of any size, and the frequency will depend on the ergonomics and performance of the communication links.

6.4 Integrated Traffic Management: System P3

6.4.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P3 (Urban Traffic control and Public Transport Priority System) described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two subsections:

- Internal communications which deal with the communication flows between different locations of the system

- Terminator communications which deals with communication between the system and the terminators

In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The example is based on the SPOT/UTOPIA (Urban Traffic Optimisation by Integrated Automation) system.

This System is specifically chosen to represent the architectural solutions adopted by a decentralised system. It aims at improving urban travel conditions by the application of fully automated hierarchic control principles which optimise dynamically the stages of traffic lights sets in urban areas. Optimisation is based on real time data continuously measured plus historical data and knowledge of special events.

In addition to describing how the System controls highly complex urban road networks, it will be considered how its open architecture grants the integration with other different external systems. From this point of view, in this example it is shown the interaction with the AVM (Automated Vehicle Monitoring) system, which has the task of monitoring and forecasting the movement of the urban public transport fleet. The provision of this information is necessary for the System to give priority to public transport vehicles.

Finally, it is put the attention on the so called Multifunctional Outstation (MFO). Not only does its presence assure the actuation of the urban traffic control, but it also acts as data pusher of the information provided by external systems interfacing with the System here considered.

The figure below shows the overall communication links within the P3 system.

The system exchanges data with 5 Terminators. Only one of them (related road systems) needs to communicate via communication infrastructures, the other interfaces being of MMI or physical nature.

6.4.2 Internal Communications

6.4.2.1 Introduction

The P3 system is a hierarchical system. It is based on:

- A central traffic control sub-system (P3.1) gathering traffic and system status information from the different roadside sub-system, and managing the interface with the operators and Related Road systems.

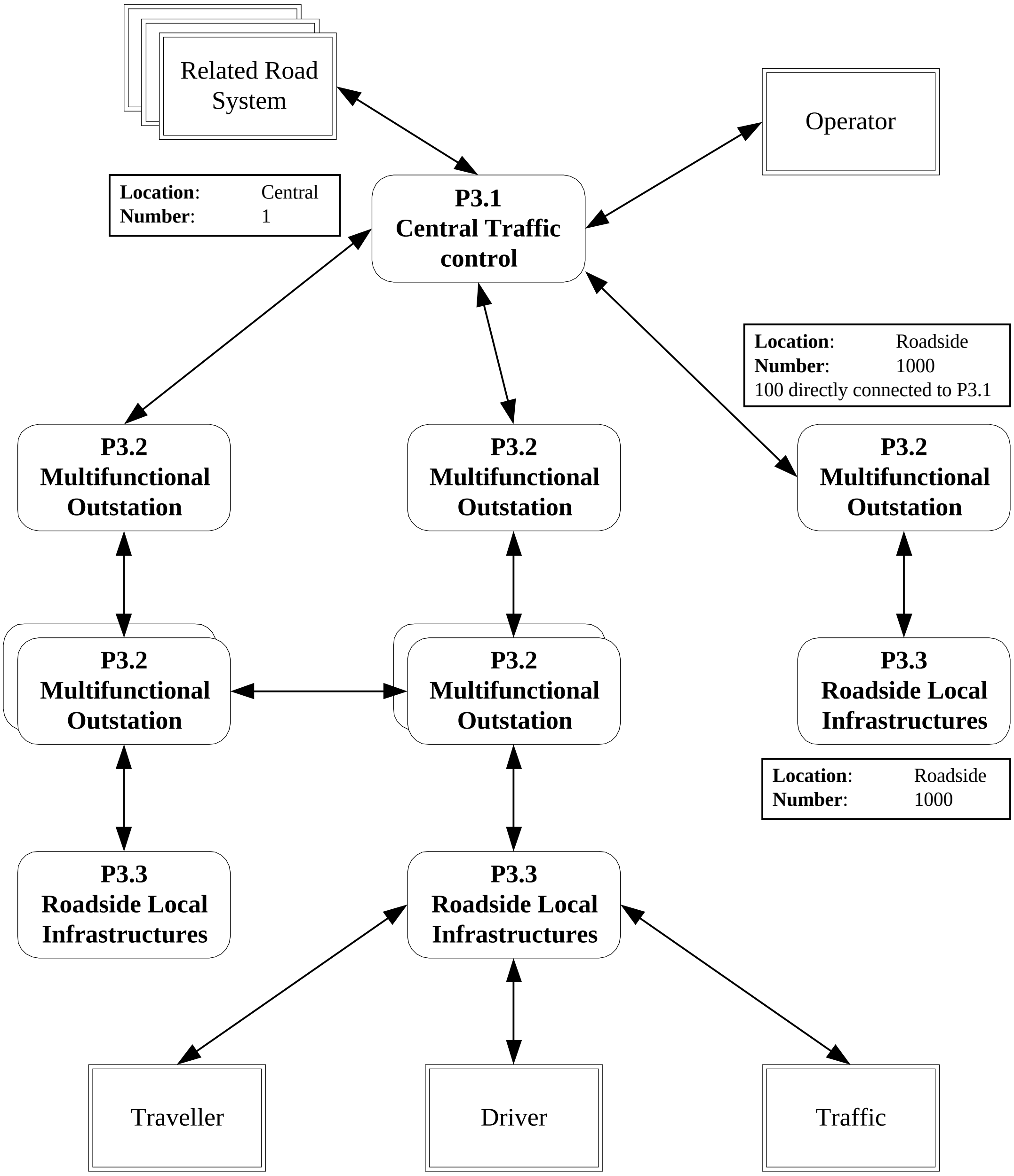
- Many roadside located Multifunctional Outstation Sub-Systems (P3.2, also called MFOs) which are either directly linked with the central systems, or connected to other MFOs, creating a network. We consider here a system including 1000 MFOs, 100 of which being directly connected with the Central sub-System. These MFOs gather traffic information at the intersection level, and establish the intersection control strategies according to this information, and from the one they get from their connected fellow sub-systems.

- Roadside Local Infrastructures (P3.3), each of them connected to an MFO, providing the roadside functionality for traffic management, namely management of traffic lights, various displays, sensors, etc.

The internal communications between the different sub-systems are therefore limited to :

- Central ↔ Roadside communications,
- Roadside ↔ Roadside communications, either between MFOs or between an MFO and its Roadside Local Infrastructure.

Figure 5 P3 System Diagram


Related Road System
Operator
Location: Central
Number: 1
P3.1 Central Traffic control
Location: Roadside
Number: 1000
100 directly connected to P3.1
P3.2 Multifunctional Outstation
P3.2 Multifunctional Outstation
P3.2 Multifunctional Outstation
P3.2 Multifunctional Outstation
P3.2 Multifunctional Outstation
P3.3 Roadside Local Infrastructures
Location: Roadside
Number: 1000
P3.3 Roadside Local Infrastructures
P3.3 Roadside Local Infrastructures
Traveller
Driver
Traffic

6.4.2.2 Central ↔ Roadside Requirements

As mentioned before, the central sub-system can be directly connected to 100 MFOs. The messages exchanged between these two kinds of sub-systems are of three types :

- from MFOs to P3.1 :
  - local traffic information, each MFO sends information at least once per minute, but additional messages are necessary because the MFO also transmits messages originating from MFO which are not directly linked with P3.1. So the link between the MFO and P3.1 sends one message every second or every few seconds. Message size should be around 100 B for one MFO (but remember

that each MFO directly connected with P3.1 must transmit it the messages sent by the 10 MFOs connected to it but not to P3.1), with a transmission delay inferior to the frequency, and therefore in the range of 1s,

  - application output. These messages correspond to data sent by devices belonging to other systems (VMS system, car park system, ...). The frequency should be similar to the previous category, with a lower size (a few tens of Bytes).

  - fault diagnosis, sent only in cases of failure, once every few minutes or so, with a small size (a few Bytes),

- from P3.1 to MFOs:

  - priority requests. for one MFO, this message should have a frequency of a few seconds. Each message is only sent to the intersections concerned by the public transport journey, and its size should be around 50 Bytes. This message may require source authentication.

  - control criteria, sent every few minutes to each MFO (a different message for each MFO), with a size inferior to 50 - 100 Bytes.

  - application input : frequency around one minute, size around 50 - 100 Bytes, sent to all MFOs

To sum up the needs, the link between the central system and one MFO must provide throughput around 400Bytes/s in each direction. There will also be transmission delays of around 1s, but no authentication or security is required, and integrity must be high. The system uses 9600 Baud lines, that means ~960Bytes/s at most, but the half duplex mode + protocol overhead are responsible for the 400Bytes/s considered. The transmission medium must be able to transport the messages on local distances (less than 20 km), in urban landscapes, and to join 100 subscribers.

6.4.2.3 Roadside ↔ Roadside Requirements

Here we have to distinguish two types of links:

- those between two MFOs, which are separated by some building blocks;

- those between an MFO and its associated Roadside Local Infrastructure, which are very close one from another.

For communications requirement between MFOs, the physical data flows include on one hand those exchanged with P3.1, as an MFO can serve as a relay between the central sub-system and other MFOs, and specific messages exchanged between MFOs, and corresponding to anticipated traffic light cycles. These messages are exchanged at a very fast rate (one every 3 seconds), but the size of the message should be less than100 Byte. The required throughput is therefore in the order of hundreds of Bytes per second. on each direction. The distance between the communications end located in urban landscape is 1 km or less, and each MFO must be able to exchange data with a maximum of 10 other MFOs.

For communications between an MFO and its Roadside Local Infrastructure, the exchanges include:

- actuation commands, sent every few seconds, with short duration needs, but a small size (a few bits),
- data sent by other applications devices, or to them. These messages have been described previously,
- priority requests originating from pedestrians for example, and sent by the RLI. The size is very small (a few bits), and the frequency of a few seconds,
- fault detection messages, sent very rarely, and of a few Bytes, with transmission delay smaller than 1 s.

The distance between the sub-systems is quite small (inferior to a few tens of metres), and the link is one-to-one: each MFO is connected to one RLI, and vice-versa. Therefore, the best solution is a dedicated cable linking the two sub-systems. If application devices needs in terms of bandwidth are small, other solutions could be contemplated, such as infrared or radio transmission.

6.4.3 Terminator Communications

As described above, the only terminator requiring communication links is Related Roadside Systems.

The exchange of message with this system concern :

- messages concerning other applications: similar to those exchanged between the central sub-systems and the MFOs,
- diagnosis for the status of the entire application devices network: this message could be sent a few times per hour, and is of important size (up to 100 Bytes), with transmission delays or about one minute,
- control strategies: the frequency should be every few minutes. Two solutions can be envisaged here. Either the message contains only the identification of the strategy to be implemented for the day, and in this case is of very small size, or the message includes the definition of all the parameters, plus charts, and in this case its size could be a few kB. In any case the acceptable transmission delay can be quite large (order of seconds), which allows not to require high integrity,
- special priority request messages, which require source authentication, and could be sent with a frequency of some seconds, and a size of 100 Bytes approximately. This message necessitates low transmission delays (a few seconds), and a high integrity, as emergency vehicles for example could be concerned).

The total requirement is therefore for a link providing a throughput of about 10 kBytes/s. Security or integrity needs are not severe, except for special priority request which could be transmitted on a specific means.

6.5 Electronic fee collection

6.5.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P10 (Electronic Cash Transaction System) described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two subsections:

- Internal communications which deal with the communication flows between different locations of the system
- Terminator communications which deals with communication between the system and the terminators

In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The P10 System provides the facilities for handling the basic electronic cash transactions associated with the use of Automatic Fee Collection for the payment of transport telematic services. The system describes the process of using an electronic travel pass to pay for a number of different services. This description has been deliberately simplified in the physical architecture document to keep the overall description as clear as possible. Thus, the links with other functional areas have been omitted from the diagrams, as was the description of the potential consequences of no payment detection (but those topics were nonetheless mentioned in the presentation of modules).

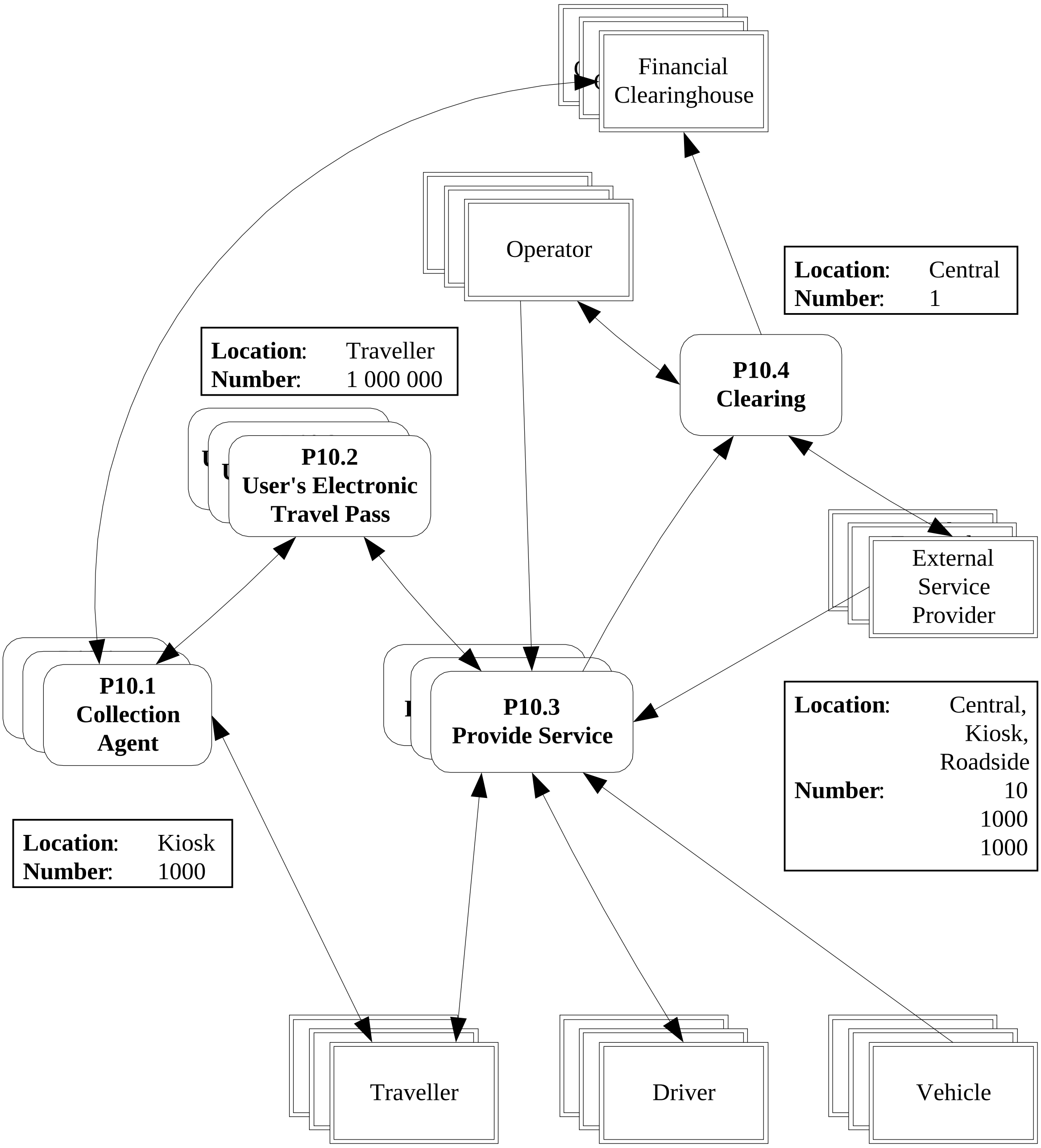
The system is based on the Conceptual Model described in DD ENV ISO 14904 “Road Transport and Traffic Telematics - Automatic Fee Collection - Interface Specification for Clearing between Operators”, which supports:

- different payment modes
- a wide variety of transport and transport related services
- co-ordination between the collectors of money, charging points etc
- security and privacy.

The figure on the next page shows the overall communication links within the P10 system.

The system exchanges data with 6 Terminators. Only 3 of them (External Service Provider, Financial Clearinghouse and Traveller) need to communicate with P10 via communication infrastructures, the other interfaces being of MMI nature. The interface with the traveller may also be partially or totally of MMI nature (in the case of P10.3 and P10.1 both being located in kiosks or on the roadside), but could also involve transmission of messages between traveller's home computers and the system.

Figure 6 P10 SYstem Diagram



6.5.2 Internal Communications

6.5.2.1 Introduction

The P10 system represents in fact not one system, but a whole family of systems, differing by their architecture concerning among other things the location of the P10.3 sub-systems. These Provide Service sub-system may be located centrally (in the case of a data server or booking system for example), on the roadside (for parking lots), or in kiosks (transport tickets vending machines for example). So the requirements for communication means will vary depending on the exact configuration of the system. On any case, the system is based on :

- a centrally located Clearing sub-system (P10.4), informing the financial clearing house of the operation performed, and asking it to update the user's and operator's account consequently, and providing services to the operators,

- a certain amount of Collection Agent sub-systems (P10.1), which here have been depicted as kiosk located but which could also be centrally located, in which case the traveller would have access via a home computer for example. These sub-systems present information to the travellers, and propose them contracts allowing them for access to services,

- user's electronic travel passes, carried by the travellers, which are used to allow their owners access to the contracted services, and to store funds loaded from P10.1, and debited by P10.3.

- a whole range of Provide Service sub-systems (P10.3), which control user's access to a service, and charge them according to their contract and service usage. These sub-systems, as mentioned above, can be located either centrally, on the roadside or in Kiosks. However, the physical architecture describes a link between P10.2 and P10.3, which would limit the choice of location between roadside or Kiosk, which in fact does not change a lot in terms of communications constraints. So in the rest of this document this sub-system will be considered as being located on the roadside.

In this case, the internal communications between the different sub-systems are limited to :

- Kiosk ↔ Traveller communications,
- Roadside ↔ Traveller communications,
- Roadside ↔ Central communications.

6.5.2.2 Kiosk ↔ Traveller requirements and recommendations

This link concerns P10.1 and P10.2. On one direction (Kiosk ↔ Traveller), it corresponds to the loading of the Travel pass, either with contract information, or with credit. On the other direction, it corresponds to the extraction of contract details. In any case, the transfer of data should be physical (reading of data included in a magnetic card or a memory chip). So this communication link has more to do with physical interface than with communications.

6.5.2.3 Roadside ↔ Traveller requirements and recommendations

This link is related to the data exchange between P10.2 and P10.3. The messages exchanged between the two sub-system are similar to those exchanged between P10.1 and P10.2, and the technological solution should be identical, since the support of information in P10.2 is the same.

6.5.2.4 Roadside ↔ Central requirements and recommendations

This link corresponds to the one way information from the Provide Service Sub-systems to the central clearing sub-system. Here the information exchanged is the details of the transaction performed between P10.3 and the traveller (or driver). The size of this kind of message should be rather small (less than 1 kB). If a network including 1000 roadside devices is considered, with one customer every minute, it leads to a required throughput of less than 17 kB/s. The transfer needs strong integrity requirements, and authentication of source and sink to avoid confidential information being read by non authorised persons, and fraud.

The maximum transmission delay is not the main requirement (one minute or more is perfectly acceptable), but the communications network has to be able to handle the numerous messages sent at the same time. The distance between the two communicating systems could be anywhere from a few meters (site) to hundreds of kilometres (long distance), depending among other things on the organisation adopted.

6.5.3 Terminator Communications

As described above, the system has real communication with three external systems: Traveller, External Service Provider and Financial Clearinghouse.

6.5.3.1 Central ↔ Traveller requirements and recommendations

This link only exists in the case that the Collection Agent or Provide Service sub-systems are centrally located. The communication requirements are then as follows:

- delay transmission : one second one way,
- throughput: up to several hundreds of connections at the same time, the Central ↔ Traveller direction carrying messages of up to 100 kB, leading to a total throughput of several tens of MB/s, the other direction requiring much less bandwidth,
- integrity: high level required,
- authentication: required for financial information.

6.5.3.2 Central ↔ Financial Clearinghouse requirements

This link corresponds to the P10.4 sub-system, which sends requests for financial transfer. These messages are of small size (less than 1kB), are transmitted every minute or so, which translates into a rather small bandwidth need. T he transmission delay requirement is also loose (several minutes is acceptable). Conversely, the most important needs relate to integrity, authentication (by the two ends) and possibly confidentiality. The two former characteristics must be of high level to prevent piracy, and to avoid problems for customers, operators and financial clearinghouses. The communication may be local, metropolitan or long distance according to the location of the system and of the terminator.

6.5.3.3 Kiosk ↔ Financial Clearinghouse requirements

This link corresponds to the P10.1 sub-system, which exchanges with the terminator information related to the status of the customer's account. These messages are small in size (around 100 bits), but are transmitted quite frequently (one every minute) by a large number (1000 in our example) systems. The resulting in a total bandwidth that is required is less than

2 kB/s. Transmission delay must be less than 1s, with a high level of integrity, and authentication.

6.5.3.4 Central ↔ External Service Provider requirements

This link corresponds to two kinds of messages :

- Database Loading. These messages are used to send to P10 the different data that will be presented to the user, or needed to determine access rights or tariffs. They are sent with a very long frequency (once a week or less). Their size can vary according to the way data is updated. The update message can contain the whole set of data, or just the data which have changed. In the first case, the size can reach several MB. The transmission delay is of limited importance (one hour is acceptable), but high integrity and source/sink authentication is required. The range of the communication can be anything from local to long distance.

- Statistics requests and results. These messages are also sent on a weekly basis, but are two-directional: the message from P10 is of small size (less than 100 bits), while the message to P10 could reach several kB. The transmission delay requirement depends on the way these messages are exchanged. If the process is automated (with no human involvement), transmission delay can be up to one hour. If it is initiated by a human intervention, the transmission delay must be on a few seconds for each direction. The statistics message requires source and sink authentication, and a high level of integrity. Range is the same as in the previous category.

6.6 Safety and Emergency Systems

This section deals with the analysis of telecommunication requirements of the system P22 (Hazardous Goods Management System) described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c).

This section comprises two subsections:

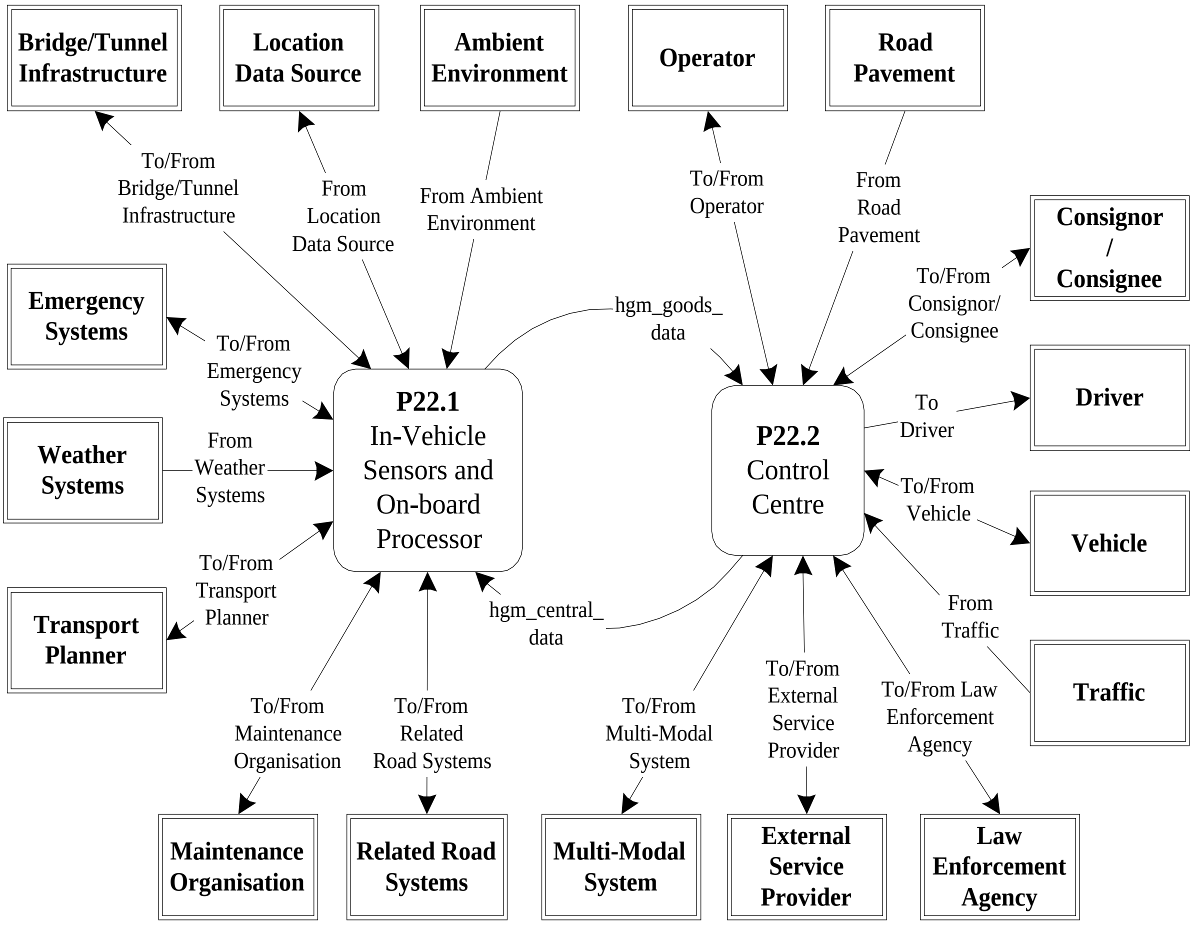
- Internal communications, which deals with the communication flows between different locations of the system
- Terminator communications, which deals with communication between the system and the terminators

The two subsections take into account the in-vehicle sensors and on-board processors (P22.1) and the control centre (P22.2)

In each of these sections, requirements for communications links are highlighted, and then technical recommendations are derived from these requirements.

The following figure shows the overall communication links within the P22 system.

Figure 7 Hazardous Goods Management System - Sub-system Diagram



The following table provides detailed information about the sub-systems and functions involved in the system.

Table 1 Hazardous Goods Management System - Sub-systems and Functions

Sub-system			Function		
No.	**Name**	**Location**	**No**	**Name**	**User Needs**
P 22.1	In-vehicle Sensors and On-board Processor	Vehicle	F 5.5.2	Enhance Driver Alertness	8.5.0.3
			F 5.5.3	Monitor Vehicle Status	
			F 5.5.4	Recover Operational Data	
			F 5.5.7	Provide Mayday Call	8.5.1;8.5.11
			F 5.7.3	Provide vehicle Position Determination	8.5.1;8.5.11
P 22.2	Control Centre	Central	F 8.1.1.2.2	Handle Hazardous Goods Transport Declaration	9.5.1.3;9.5.1.4

Sub-system			Function		
No.	Name	Location	No	Name	User Needs
			F 8.1.1.3	Control Freight/Cargo Operations	9.5.1.6
			F 2.1.5	Provide Access and Maintain Data for Emergency	7.2.1.2; 7.2.0.5; 7.2.0.7

6.6.1 Internal Communications

6.6.2 Introduction

The P22 System is spread over two locations: In-Vehicle Sources/On-Board Processors and the Control Centre. There are exchanges of information between these two locations, hence P22 deals with the "Central ↔ Vehicle" communication links.

At the Central location, there is only one sub-system, which is the Control Centre. At Vehicle locations, only the equipment related to the Safety and Emergency System is taken into account for the Communication Architecture.

6.6.2.1 Central ↔ Vehicle

This link concerns P22.1 and P22.2. In one direction, it corresponds to the transfer of data that has been collected or produced by P22.1 and is for use in the P22.2. In the other direction it corresponds to the flow of data that has been collected or produced by P22.2 and is for use in P22.1 to avoid incidents and dangerous situations along the route of the vehicle.

The same communication link could be used to realise the link in both directions. Evidently, this link should be wireless – it is impossible to have a wired connection between a vehicle and the road infrastructure.

The amount of data that are exchanged between P22.1 and P22.2 is limited. Therefore, the bandwidth of the link is not the major requirement for a selection of medium to carry the information. The major requirement for this communication link concerns the response time. The second requirement is related to the security of the link. The control centre should be sure that a message will reach the vehicle concerned in quasi real time, and vice versa the vehicle is reliant on the Control Centre in case of emergency.

The third requirement for this link is in the authentication of the message sent by the vehicle towards the Control Centre and vice versa. Since the impact of a fraudulent intruder on the system could be significant for the surrounding traffic, the protection of messages should be taken into account.

A fourth requirement will be placed on priority management. The wireless link should be able to interrupt any non-urgent message transmission to place or accept any important message generated by pressing the emergency button.

From these requirements, a PMR system such as TETRA should provide a better and more complete answer to all these requirements than a GSM based solution. The response time and the availability of a GSM network for emergency cases is often not reliable in crisis situations.

6.6.3 Terminator Communications

The system exchanges data with the 17 terminators referred to in Figure 7. Only for a few of them are the interfaces of HMI (human-machine interface) nature.

6.6.3.1 Vehicle ↔ Location Data Source

This link corresponds to the P22.1 sub-system, which sends requests for location data. This link should be wireless and could be divided into sub-links. The main link is unidirectional and is the link between the vehicle and the positioning satellite constellation (GPS or GNSS). This link allows the vehicle to permanently determine its position.

The position provided by the GNSS system is not normally sufficiently accurate to give a precise vehicle location. Therefore, a correction could be applied to the raw satellite data by receiving data from a provider of correction data. This link should be wireless and does not require a very high capacity. This link could be of broadcast type and could use the existing broadcast network.

One other link is that related to the location function. The position of the vehicle provided by the GNSS system will be used to locate the vehicle on a map, to provide guidance assistance. The map on board the vehicles needs to be regularly updated. It is possible to have a permanent update process by the use of communication links. The first solution relies on the use of large bandwidth broadcast network like DAB to transmit the update data to the vehicle. The large bandwidth is requested to transmit the relatively large amount of data needed to keep the database updated. The second solution relies on cellular networks such as GSM to transmit the data at the request of the vehicle. The request will concern only the area surrounding the vehicle in order to limit the amount of data to be transmitted.

6.6.3.2 Vehicle ↔ Emergency Systems

This link corresponds to the P22.1 sub-system, which sends emergency request to the emergency system and receive response from it. This link should also be wireless. This link has the same requirements on security, availability as the internal link between P22.1 and P22.2. Therefore, the same recommendations apply also. The same equipment could be shared for both links to reduce the acquisition cost for the vehicle segment.

6.6.3.3 Vehicle ↔ Weather Systems

This link corresponds to the P22.1 sub-system, which receives weather information and weather forecasts from the weather systems. This link should also be wireless. This link is unidirectional and could be supported by any broadcast medium. It does not require any special requirement on the bandwidth; a low data rate link will be sufficient to transmit the information.

6.6.3.4 Vehicle ↔ Transport Planner

This link corresponds to the P22.1 sub-system, which converses with the transport planner. This link should also be wireless. This link does not have the same level of requirements on security and availability as the internal link between P22.1 and P22.2. Therefore, any kind of wireless link could be used. The requirement on the data rate is also relatively low.

However, to avoid the need to install a large amount of different equipment in the vehicle, and as the exchanges should be very infrequent, the equipment required for the internal communications could be shared for both links to reduce the cost of the on-board unit.

6.6.3.5 Vehicle ↔ Maintenance Organisation

This link corresponds to the P22.1 sub-system, which receives information from the maintenance organisation.

This link could be unidirectional and could be supported by any broadcast medium. It does not require any special requirement on the bandwidth; a low data rate link will be sufficient to transmit the information. RDS-TMC is a perfect candidate for such an application.

If a dialogue need to be made between the maintenance organisation and the vehicle, the same link used for the internal communication between P22.1 and P22.2 could also be used.

6.6.3.6 Vehicle ↔ Related Road Systems

This link corresponds to the P22.1 sub-system, which receives information from the related road systems.

As for the link with the maintenance organisation, this link could be unidirectional and could be supported by any broadcast medium at low data rate link. RDS-TMC is a perfect candidate for such an application.

If a dialogue needs to be made between the maintenance organisation and the vehicle, the same link used for the internal communication between P22.1 and P22.2 could also be used.

6.6.3.7 Central ↔ Operator

This link corresponds to the P22.2 sub-system, which exchanges with the terminator operator information about the hazardous goods management. These messages are small in size, and could be transmitted frequently. The resulting bandwidth is low, at around a few kB/s.

Any kind of connection could used to link the operator to the Central, e.g. lease line, PSTN, ISDN, etc. The choice of one solution will depend on the operator's need to access the control centre. The costs of operation will be one factor to consider in the selection.

There is nowadays, a different solution for linking the operator to the control centre. This solution is the use of Internet, which is able to provide a good service for a reasonable price.

6.6.3.8 Central ↔ Road Pavement

This link corresponds to the P22.2 sub-system, which exchange with the road pavement terminator to obtain information on the status of the road-surfacing. The road pavement terminator is out of the scope of the hazardous goods management system. Therefore the network required to collect data from different locations on the road network is not covered in this section.

The exchanged messages are small in size. The requested bandwidth is low, around a few kB/s. There is no need for real time performance: some delay up to few minutes is acceptable. Any kind of connection could be used to link the operator to the Central, such as lease line, PSTN, ISDN, etc. The choice of one solution will depend on the operator’s need to access the control centre. Operational costs will be one subject for the selection. Internet could also be a valuable choice for this link.

6.6.3.9 Central ↔ Consignor/Consignee

This link corresponds to the P22.2 sub-system, which interacts with the consignor/consignee terminator to obtain information on the status of the goods carried.

As with the Central ↔ Road Pavement link, the exchanged messages are small in size and the bandwidth demand is low (around a few kB/s). Any kind of connection could used to link the operator to the Central (lease line, PSTN, ISDN, etc) and the choice of solution will depend on the operator’s need to access the control centre. The costs of operation will be one item for the selection. Again, the Internet could be a valuable choice for this link.

6.6.3.10 Central ↔ Driver

This link corresponds to the P22.2 sub-system, which sends information toward the driver. This link should also be wireless. This link has the same requirements on security, availability as the internal link between P22.1 and P22.2. Therefore, the same recommendations also apply. The same equipment could be shared for both links to reduce the acquisition cost.

6.6.3.11 Central ↔ Vehicle

This link corresponds to the P22.2 sub-system, which exchange information with the vehicle. This link should also be wireless. This link has the same requirements on security, availability as the internal link between P22.1 and P22.2. Therefore, the same recommendations apply also.

6.6.3.12 Central ↔ Traffic

This link corresponds to the P22.2 sub-system, which exchanges with the traffic terminator to obtain information on the status of the traffic. The communication network required to collect data from different locations for defining the traffic data is not covered in this section. Only the communication link for the hazardous goods management systems is relevant to this section.

The messages exchanged are very diverse in their nature, and could require a large bandwidth to link the system to the terminator. The selected connection should be chosen by keeping in mind the bandwidth requirements. This requirement is related to the level of processing capability provided by the traffic terminator. If a large amount is transferred a high capacity connection such as ISDN, or better still, a lease line could be recommended. If the traffic terminator provides synthetic information to the control centre a PSTN link could be sufficient. Internet could also be a valuable choice for this link in this case.

6.6.3.13 Central ↔ Law enforcement Agency

This link corresponds to the P22.2 sub-system, which exchanges with the law enforcement agency terminator to get and transmit information to comply with the local regulations. The system shall provide sufficient data for the Authority to identify and initiate prosecution of offenders.

The messages exchanged are very diverse in their nature, and would need a large bandwidth to link the system to the terminator, particularly if pictures are to be transmitted. The selected connection should be chosen by keeping in mind the requirements on the bandwidth. This requirement is related to the level of processing power provided by the law enforcement agency terminator. If a large amount is transferred, a high capacity connection like lease line or ISDN could be recommended. If the traffic terminator provides synthetic information to the control centre a PSTN link could be sufficient. Internet could also be a valuable choice for this link in this case.

6.6.3.14 Central ↔ External Service Provider

This link corresponds to the P22.2 sub-system, which exchanges with the terminator external service provider information about the hazardous goods management. There are different actors behind this terminator. All of them have different requirements, but it could be assumed that the messages exchanged are small in size. A low data rate connection of around a few kB/s should cover this link.

Any kind of connection could be used to link the external service provider to the Central, e.g. lease line, PSTN, ISDN, etc. The choice of one solution will depend on the need to access the control centre. Depending on the architecture of the control centre, Internet could also be an alternative for the data exchange.

6.6.3.15 Central ↔ Multi-Modal Systems

This link corresponds to the P22.2 sub-system, which exchange with the multi-modal systems terminator information about the hazardous goods management. There are different actors behind this terminator. All of them have different requirements, but in any case the exchanged messages are small in size, and would not be transmitted frequently. The resulting bandwidth demand will be low (around a few kB/s).

Any kind of connection could used to link the external service provider to the Central, such as lease line, PSTN, ISDN, etc. The choice of one solution will depend on the need to access the control centre. Depending on the architecture of the control centre, Internet could also be an alternative for the data exchange.

6.7 Traffic Management: System P30

6.7.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P30 described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two subsections:

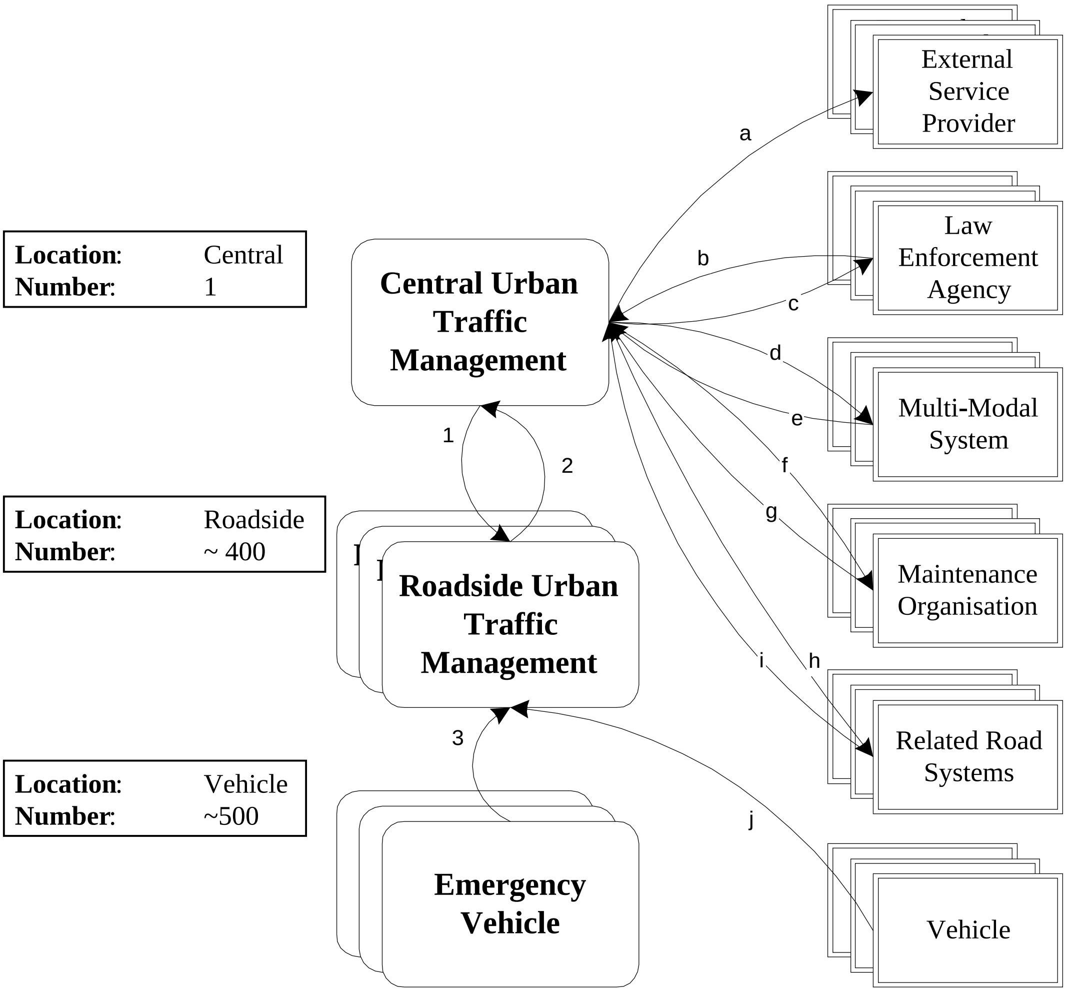
- Internal communications which deal with the communication flows between different locations of the system
- Terminator communications which deals with communication between the system and the terminators

In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The P30 System provides facilities that enable the management of road traffic that is using an urban road network. In addition to the actual traffic management facilities, the System includes additional facilities for the maintenance of the physical road network and the equipment used by the System for the management of traffic. Emergency Vehicle priority is provided in two ways. Firstly using equipment on-board the Vehicle that links to local System equipment at the Roadside to provide priority at individual junctions. The second way of providing priority is by requests from the Emergency Systems terminator. This will enable priority along particular routes to be requested. Links from this System to other Systems are also provided to enable co-ordination of traffic management across organisational and geographic boundaries.

This System has been included to show urban traffic management in its simplest form. For example, the urban road network includes no bridges or tunnels, and there is no control of inter-urban road networks. Also there are no facilities for Incident or Demand Management, nor any Environmental Monitoring. However there are three additional facilities not yet found in widespread use among traffic management systems currently implemented in many towns and cities across Europe. The first is lane management, which will enable such things as tidal flow control on multi-lane roads, the second is vehicle speed control, and the third is the links to the Multi-Modal Systems. The second facility has been the subject of recent testing in Europe and will enable vehicle speeds to be regulated without the need for physical devices such as speed ramps. The third facility will enable the movement of vehicles on other modes of transport such as railways and canals to be co-ordinated with road traffic movements.

Figure 8 P30 - Communications Diagram



The figure above shows the overall communication links of the P30 System for controlling up to 300 junctions. It may be one urban geographic area, or several small urban geographic areas spread over a larger rural geographic area, e.g. a German State, French Provence, or UK County.

Analysis of the communications links has been divided into two parts. These comprise Internal Communications - links *1*, *2* and *3* in the above diagram, and Terminator Communications - links *a* to *j* n Figure 8 above.

6.7.2 Internal Communications

The P30 centralised System spreads over three locations, Roadside, Central and Vehicle. There are exchanges of information between the Roadside and the Central locations, and data is sent form the Vehicle to the Roadside locations. Hence, P30 deals with the following communication links:

- Central ↔ Roadside - see links 1 and 2 in Figure 8

- Vehicle → Roadside - see link 3 in Figure 8

At the Central location, there is only one sub-system which is the Traffic Management Centre. In the centralised configuration described by P30, there is only one central physical entity[1] plus two other entities, one for Maintenance and the other for Law Enforcement.

At the Roadside location, roadside equipment (telemetry, detection, control, etc.) is usually put inside a single "box", the size of which varies from one country to another and from one supplier to another. The “box” is usually called a *cabinet* and this is placed at or near the physical roadside. Typically, up to three hundred cabinets can be spread in the urban geographic area for traffic management, and up to a hundred specific cabinets can be provided for law enforcement data collection.

At Vehicle locations, only vehicles making local priority requests are taken into account for the Communication Architecture.

6.7.2.1 Central ↔ Roadside

6.7.2.1.1 Requirements

The Centre ↔ Roadside links are spread over all the urban geographic area managed by the equipment at the Central location.

From the Central to the Roadside locations, every second, the next cycle of commands are sent to the cabinets. This will be called the down-link.

The up-link, from the Roadside to the Central, is richer; several kinds of data must be taken into account:

- data collected about the traffic flow, the car park situation and the traffic management are sent to the Central equipment;
- the cabinets also send data about the equipment state (monitoring and state data including failures);
- in addition, information collected by law enforcement equipment, which may include photo or video, is sent by the dedicated cabinets to the equipment at the Centre.

The commands sent on the down-link are executed by the cabinet during a whole “cycle” which lasts a second approximately. Then it has to be updated. As all the “intelligence” is centralised in this model and the cabinets do nothing more than execute orders, the link must always be available, and it must be very robust.

[1] It is technically reasible to split up the central physical entity into two or more parts that may be implemented in different places. The reason for not doing this is usually that it produces savings in communications costs, because a private network has to be used. Nevertheless, if multiple central sites are chosen, these sites should look as a unique entity for the rest the System, in particular from the roadside equipment. It is not the purpose of this analysis to describe the private network that could be used to link different sites. This analysis will consider the case which has a unique physical central entity.

The up-link is used to transmit the data that will enable the equipment at the Centre to elaborate the next cycles' strategies. As a consequence, it is best to transmit them at the same rate as the commands are sent on the down-link. This also enables the use of the communication link in both directions when the communication is open. It is also sensible to use the same session to transmit equipment and monitoring state data, so that subsequent actions can be performed immediately (e.g. repairing in case of failure). Hence, the two first kinds of data should be sent to the centre every 1~10 seconds[2].

In addition, a strong user requirement is to reduce the time needed to process law enforcement data. A sensitive objective can be that they should reach the Centre within an order of magnitude of the minute.

The amount of data transmitted from the Centre to the Roadside cabinets (down-link) is very little for each session. The order of magnitude is of a few (less that 10) bytes for each cabinet

For the up-link, the situation is quite different. Most cabinets do not send law enforcement data and so need to send messages which are again in the order of magnitude of 10 bytes. The up-link data for cabinets with law enforcement equipment depends on the type of application that is being used. This may require various types of data to be sent, ranging from simple data (in the order of magnitude of a 100 bytes), or photographs (in the order of magnitude of several kilobytes per photograph), or even video (in the order of magnitude of a 1 Mbyte per second).

Each cabinet must receive its own set of commands. So, it is not possible to make use of multi-point or broadcasted messages to reduce the amount of transmitted data[3].

This communication link is based on communication ends which are not mobile. This does not necessarily call for wireless communications.

As far as security requirements are concerned on the down-link, there is not very much to gain for an attacker in taking control of the Roadside Sub-system. In addition, it would be costly to purchase the required equipment and the knowledge required for its use would be considerable. There is thus very little risk that an attacker would try to take control of the Roadside Sub-system. Hence there is extremely little need for authentication of the central in this kind of communication.

Of course, confidentiality is not at stake either. The information transmitted is intended to be displayed to all citizens in the area. As there is no confidentiality, there is no need to authenticate the cabinets at the Roadside.

[2] These regular flows are in fact complemented by irregular flows. Irregular flows are triggered by events such as a failure of the system or the detection of a traffic problems. Since regular flows are based on messages sent every 1~10 seconds ,and that they are needed only from time to time, they can be considered as included in the regular flow from a telecommunication point of view. Hence, to simplify the discussion, they are not specifically considered in the rest of this study.

[3] However, this does not mean that broadcasting telecommunication technologies (such as satellite) cannot by used to send these messages. Technically, each message can be broadcasted to all cabinets where they can be filtered so that only the appropriate targeted cabinet actually uses the message. Hence, specific (and not broadcast) messages are sent to specific targets on a broadcast telecommunication technology.

However, there are security requirements in the field of data integrity. Messages are to be used almost in real time, and have a direct impact on the traffic flow. Any alteration of the information would result in disruption of the traffic flow. Hence, the information that is sent must not be altered, thus calling for special attention to data integrity. In addition, it must be ensured that the information reaches the appropriate cabinet. This is because each road junction has its own strategy which is quite different from any other strategy, and because the strategies of several junctions in the same neighbourhood are correlated. Hence, additional checking may be performed to avoid any data being sent to the wrong junction.

Security requirements are quite different for the up-link, especially because of law enforcement data. All data from cabinets needs some kind of protection for its integrity, but additionally, cabinets linked to law enforcement systems must provide features to authenticate and ensure integrity of the data that is being transmitted. This is so that it can be proved that the data has not been altered. For the sake of privacy, encryption should be used to protect these messages that contain information on the citizens.

6.7.2.1.2 Technical Recommendations

The total network useful load on the down-link is very low: there are approximately 300 cabinets updated approximately every second with approximately 10 bytes per cabinet[4], which results in a total of 3000 bytes per second for the whole network. The load is quite low, but the communication link to support it must be continuously available.

So far as the up-link is concerned, depending on the amount of data needed for law enforcement systems, the useful load can range from several kilobytes per second, to a gigabyte per second. However, in most cases, even if pictures or video is used at the Roadside, the relevant information (number plate data, speed, etc.) can be expressed in figures, the transmission of which is less demanding in terms of bandwidth.

6.7.2.1.2.1 Case A: low bandwidth needed for law enforcement data.

In that case, it can be considered that both down and up-links require less than several kilobytes/s of bandwidth. This can be handled by almost any technology.

Nevertheless, if the network load is not a problem, the number of points to be served continuously, almost without failure is quite large. This is a significant drawback for certain wireless technologies. For instance, GSM SMS cannot be used because it is not reliable in terms of latency and availability, and if data GSM is available in the area, it is still very costly. Dealing with 300 connections every second without failure is also too demanding for the network. TETRA should also be avoided for the same reason.

As far as costs are concerned, the System is by definition located in an urban area. In that case, wired telecommunication infrastructure is most of the time available, and thus relatively inexpensive. However in some countries the connection to and use of the available wired network can be very costly. In places where wired infrastructures are not very well developed, it may appear cheaper to use wireless technologies, but this is very unlikely.

[4] Depending on the system used, it is also possible to transmit around 100 bytes around every 10 seconds, which does not modify the required rate in anyway.

In addition, technologies limited in range, such as DECT, cannot be used on such a geographic wide area.

For robustness, the requirements are very clear. The System is completely centralised and the service must be continuously available. In an urban area; wireless communications are very likely to suffer from interference, multiple path trouble, obstruction, etc. Up-coming terrestrial wireless technologies such as LMDS could be used but are designed for wide bandwidth systems. This is not the case here, unless the network is shared for other purposes, which may prejudice the robustness requirement.

It must be stressed that satellite based communication could be difficult to use because of the size of the antenna. Also many locations cannot be reached by a single satellite in an urban area, as is evidenced by the need to use several satellites for GPS applications.

In conclusion, wired technologies are strongly recommended for this kind of System. Wireless technologies are not really suitable for the System and could only be used in very specific conditions (e.g. when wired networks are not available). In addition, their use would call for modification of the System such as “backup intelligence” at the Roadside or backup telecommunication technologies to resist any failures.

As far as wired technologies are concerned, dial-up connections do not seem to be the most adequate solution since the communications are almost continuous (an update every minute in both directions). Instead, solutions based on permanent connections are strongly recommended.

For instance, lease lines could be chosen. But, the amount of bandwidth needed is very little compared to the bandwidth available on leased lines and the number of points to be connected is very high. This makes it quite an expensive solution. It is not an appropriate solution unless spared bandwidth can be used for other purposes not considered in this System (management of Public Transport equipment for instance). If no other data is supposed to be transferred on this link, other kinds of permanent access such as via ISDN channel D (9.6 Kbits/s) and transfer over an X.25 network is much more affordable than leased lines, and very much more reliable.

In other cases, the use of a specific infrastructure deployed for this type of System is still a possible solution. This can be a solution for the road managers to implement, especially if it can use a network already in the pavement that they (or another part of the organisation) are already managing for other purposes.

In addition to this low level specification, for law enforcement flows from the Roadside to the Centre, which concern only part of the cabinets, specific security requirements must be covered. Mechanisms must be implemented to provide authentication of the source, signature of data and low confidentiality. But, over the wired technologies observed, which do not implement these features at their layer, these mechanisms should be implemented in higher communication layers such as the application layers.

In conclusion, the requirements made for the Road ↔ Centre communication links call for low bandwidth, wired and permanent technologies which provide good data integrity features. Apart from proprietary dedicated wired systems, a typical solution would be ISDN access over channel D to an X.25 network. In addition, particular attention should be given to law enforcement data flows which have their own security requirements.

6.7.2.1.2.2 Case B: high bandwidth needed for law enforcement data

This case is very similar to Case A, except that the up-links from part of roadside cabinets needs a larger bandwidth for transmission of photographs, even video sequences or even real time video.

As far as wired versus wireless solutions are concerned, remarks made in Case A also hold for Case B. This calls for a clear preference for wired solutions. In addition, most current wireless systems (like GSM or TETRA) which offer an up-link are bound to low bandwidth transmission, which is an unsuitable choice in that case.

Nevertheless, in that case, such permanent links as ISDN access over channel D to an X.25 do not provide enough bandwidth for the up-link. Technologies such as Frame Relay should be considered, or even SDH and ATM if affordable and available. With such a technology, much bandwidth will be made available on the down-link, it is recommended to make use of that bandwidth, for instance to transport information for Public Transport users.

Like in Case A, it should be stressed that additional security features should be provided to protect law enforcement flows with mechanisms implemented in higher communication layers (for instance the application layer).

In Case B, requirements for law enforcement transmissions are very much different from other kinds of transmission. In such condition it is wise to use different technologies to answer needs more specifically. At the moment, implementations are based on the use of two different networks separately operated. One for usual traffic and control data exchanges, the other for law enforcement data exchange.

However, in order to reduce telecommunication costs, it is also wise to look for the merging of these two data flows over the same telecommunication network.

In that case, a first solution could be to use a single technology to cover all needs. This would be unsuitable, because most cabinets do not serve law enforcement purposes and their link would be underused, which leads to the waste of bandwidth.

Then, a second solution, is to keep low bandwidth connections for traffic and control system and to send the two data flows over a single network only for those cabinets which deal with both flows.

With that second solution there will be no lost of bandwidth and reduction of the number of communication links to be managed. Direct telecommunication costs should be lowered. However indirect costs would be increased due to increase of the complexity of the solution (merge of different flows, sharing of bandwidth, etc.). Only thorough costs and benefits studies can tell if this second solution is preferable to the use of two separate networks.

6.7.2.1.3 Summary

The main elements of the discussion above can be synthesised in the table on the following pages. Only those technologies that are relevant for the P30 System described at the beginning of this section have been considered.

Table 2 P30 Analysis - Recommendations for Central to Roadside Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless mobile GSM	Reduced infrastructure costs for the telecom operator.	Not adapted to permanent links. Network sometimes saturated. Links are not robust. Case B: very low bandwidth[5]	Not recommended
Wireless, mobile DECT	Reduced infrastructure costs for the telecom operator.	Not adapted to so many permanent links. Not adapted to long distance. Links are not robust.	Not recommended
Wireless, mobile TETRA	Reduced infrastructure costs for the telecom operator.	Not adapted to so many permanent links. Links are not robust.	Not recommended
Wireless fixed (LMDS; MMDS)	Bi-directional high bandwidth	Links are not robust. Limited distance (3~10 miles).	Not recommended, except for specific purpose (e.g. video connection).
Broadcasting (MOBITEX, DAB, Satellite)	Low infrastructure costs	No uplink.	Not recommended
Satellite bi-directional (VSAT)		Needs a 1.2 m antenna (Case B: low bandwidth) Links are not as robust as wired links.	May be used for case B. The installation of the antenna must be taken care of.

[5] Will change with upcoming standards such as GPRS

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wired, Dial-up (PSTN-ISDN)		Most of the time unsuitable for permanent links	Not recommended in most countries where less expensive permanent links are available
Wired Permanent X25	Robust Permanent Available in most countries		Recommended (in particular case A), especially over ISDN channel D
Wired Permanent Frame Relay	Larger bandwidth as X.25. (up to 2 Mb per link)	Not as reliable as X.25 Deployment of infrastructure.	May be used for case B
Wired Permanent ATM, SDH	Very Large bandwidth	Complex deployment of infrastructure.	May be used for case B

6.7.2.1.4 Conclusion

In both cases examined above, it is very unlikely that current wireless technologies can be selected to answer the expressed needs. The exception will be perhaps in regions where adapted wired networks are not yet implemented or if the context requires it (e.g. a historic site where cables cannot be installed). In that case, the System must be adapted to deal with likely transmission failures.

Permanent links are needed to cope with the continuous data flow. Depending on the bandwidth needed by law enforcement transmissions, different wired technologies should be considered. These can be categorised according to whether the required bandwidth is high or low. If it is low a single network should be considered. In cases where the required bandwidth is high., a costs and benefits study should be carried out. This will highlight if it is preferable to use two different networks for each kind of flow, or if it is better to use two technologies for each kind of cabinet. With these wired technologies additional security features should be provided to protect law enforcement flows from disclosure, alteration or repudiation.

6.7.2.2 Vehicle → Roadside

6.7.2.2.1 Requirements

The P30 System deals with the case of direct communication links established by emergency vehicles with the control module at the Roadside. These communication links are used to send local priority requests to the Roadside, so as to open the route for the quick passage of the emergency vehicle and to let other traffic move ahead out of its way.

It must be stressed that in this System (P30), only direct communication with the Roadside is considered. Systems involving calls to a Centre are excluded. The Roadside is supposed to react directly to the request and does not receive information (e.g. on the vehicle, its route) from a Centre. This Vehicle based system will only be used when a priority route cannot be (or has not been) selected by the Emergency System and provided to the Centralised Urban Traffic Management System[6].

Because of the mobility of the vehicle the communication is necessarily wireless. The link must be established within a second, and there should be high possibility of establishing the communication at the first attempt.

Requests for priority can be sent simultaneously from several vehicles to one cabinet. However, a cabinet can only define one priority route per road junction. For each junction only one request can be taken into account at a time. So a maximum of one communication link needs to be established between a cabinet and surrounding vehicles per junction managed by the cabinet. In most situations, it means that a cabinet will have to deal with a single communication link.

A strong requirement is that rigorous authentication of the vehicle data is performed. This is to prevent unauthorised vehicles from obtaining priority routes.

6.7.2.2.2 Technical Recommendations

In such a System, the request can only be taken into account when the direction of the vehicle is clear. The vehicle must not turn off the expected route that it will take to reach the junction for which priority is requested. Under such condition, a close range radio system (~60 meters) is the most adequate. No general short range system is suitable because of the requirements above, hence specific systems have been developed.

There is no dedicated standard system in this field, which may cause several troubles, notwithstanding usual troubles due to lack of standardisation. For example a vehicle can only send request in the area where its system is compatible with the Roadside equipment that will detect the priority request. Therefore vehicle operators must synchronise technology choices with the traffic management operator. However, a frequency range has been reserved for that kind of applications (DSRC around 5.8 GHz), and the CEN/TC278/WG9 working group has defined level 1,2 and 7 layers of the OSI model for a similar application: contact free tolling. By reusing the level 1 and 2 specification, a standard could be easily presented for priority systems too.

One way communication systems are sufficient, since there is no need for interaction: the message is clear and unique, “give me priority for right of way”. However, two way communications systems allow additional features such as strong authentication based on challenge/response algorithms. These can be needed to prevent fraud, or the rejection of a priority request. Such a rejection may arise when the requested priority conflicts with that requested by another vehicle for the same junction.

[6] This system is very different from a centralised system where vehicles are directed from a Centre. In that case, the Vehicle is not likely to communicate directly with the Roadside, but would rather leave the Centre deal with the TMC on its behalf. The communications between this specific Centre and the Vehicles are very likely to take place over TETRA or GSM, and location system such as GPS or GNSS would be used to locate the Vehicles.

Another possibility may be to use wireless mobile systems, such as GSM, TETRA or DECT.

GSM and DECT should be avoided because of the time needed to establish the telecommunication. This could be exacerbated in urban areas because the network may be saturated by other communications.

PMR systems, such as TETRA, offer the possibility to set up calls in a very short time frame, and to place a priority call, with the ability to cancel other calls when needed. In that case, the standard does not offer the possibility to locate the vehicle. It means that a system must be added to locate the vehicle (e.g. GPS). Unfortunately, this is not sufficient, as the cabinet must know in which direction the vehicle is heading. Either a specific system must be used at the Roadside to detect the direction of the signal, or the vehicle must be able to transmit the direction of its movement to the roadside, and this is not in the standard.

Of course, with such telecommunication systems, a centralised and managed route optimisation, which would be much more efficient, can easily be supported. But this is excluded in the case examined here were the communication goes only to the roadside.

Most satellite based systems are not relevant, because of the need for specific antennas, which may be difficult to install at the roadside. In addition there is also the difficulty of ensuring continuous satellite communication in urban areas for the roadside, and especially with mobile vehicles. This is exemplified by the need (and use of) several satellites simultaneously as the source of data for GPS applications.

6.7.2.2.3 Summary

The main elements of the discussion above can be synthesised into the table that is shown on the next page. Only those technologies that are relevant for the P30 System have been considered.

Table 3 P30 Analysis - Recommendations for Vehicle to Roadside Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and other remarks
Wired Technologies			Only mobile communication
Satellite Communication		Need for specific antennas. Complex. Not adapted to urban areas.	Not recommended if used only for priority request
Wireless, mobile (GSM or DECT)	Availability	Communication establishment time. Possible saturation of the network.	Not recommended

Technology	Main Advantages	Main Drawbacks	Conclusion and other remarks
Wireless, mobile, PMR (TETRA)	Instantaneous communications, and priority call possible. Private network		
Short range radio system	Absolutely adapted	No standard	This solution is recommended but there is a need for a standard. A possibility is to adapt existing solutions such as DSRC

6.7.2.2.4 Conclusion

When this Vehicle based system is used, that is to say when a priority route cannot (or has not) been selected by the Emergency System and provided to the Centralised Urban Traffic Management System, only short range radio proprietary solutions are really adequate. The spreading of such a solution would call for a standard.

6.7.3 Terminator Communications

As described above, the system exchanges data with 10 terminators. Only five out of these 10 terminators are considered in this section, others are human-machine interfaces that do not require telecommunication support[7]. These six terminators, are Public Transport Vehicle, Related Road Systems, Maintenance Organisation, Multi-Modal System, Law Enforcement Agency, and External Service Provider. They are shown in Figure 7.

6.7.3.1 Central → External Service Provider

6.7.3.1.1 Introduction

In System P30, data collected by the central on the traffic is sent to broadcasters and traffic and travel information providers. In that context, the function of the P30 System is only to provide the information to the ESP (External Service Provider). This information on traffic and travel conditions is then formatted and sent to users by these broadcasters and travel information providers. In this section, ESP is restricted to these two providers.

It is a Central → Central interface.

[7] These interface are addressed in Chapter 8 of this Document.

6.7.3.1.2 Requirements:

Typically there are one to ten ESP's each requiring a different level of details and kinds of information.

Since the broadcasting function is left to the ESP, there is only a single communication link from the central to each ESP. The level of detail and kind of information transmitted depends on the contracts between the ESP and the traffic management operator. Hence it is very unlikely that the same information is sent to all ESP. In consequence, most of the time, there will be a point to point communications with each ESP and no broadcasting.

The information transmitted must be updated rapidly, around every minute. The data rate is approximately the same as the quantity of information collected, around 3 Kbytes/s. This data rate is also absolutely continuous and permanent.

The information transmitted is valuable and must be protected against disclosure. Hence authentication and confidentiality are required. Integrity of the information must be ensured, but there is no need to protect the receiver against repudiation of the origin, and no need for signature of the information sent by the traffic management centre.

6.7.3.1.3 Technical recommendations:

It may happen that the traffic management operator also plays the part of an ESP, and that both sub-systems are located in the same building or campus. In that case, any local area network will do as long as required data rate (usually, around 3Kbytes/s) is always available between the sub-systems performing the two functions. This can be ensured by any local area network technology available today, provided that it is configured properly.

The link is permanent, which leads to the exclusion of dial-up systems (either wireless, such as DECT, TETRA, or GSM, or wired such as PSTN and ISDN). However in some countries where PSTN and ISDN are very inexpensive they can be an alternative. Alternatively, for communications within buildings or large campus sites, an internal form of PSTN may be used.

If the distance allows it, wireless terrestrial systems such as LMDS or MMDS can be used although it causes the waste of a lot of bandwidth. Unless more bandwidth is needed for other purposes, leased lines are also not useful in that case as they will tend to be expensive.

Broadcast technologies without return links (satellite, DAB, etc.) are not really recommended because they do not allow the establishment of a real communication link (with retransmission in case of failure, authentication handshake at the initiation, etc.). Of course, it is possible to make use of another technology such as PSTN on the return channel, but then, why not use this technology in both directions?

An inexpensive connection means can rely on Internet. This implies a lower quality of service that can hinder the quality of service offered by the ESP. The delay will not be guarantied, information will be lost and will have to be resent or ignored, data rates will not be guarantied and strong security means will have to be set up to protect data against disclosure and to protect the system itself since the network is public. This is not really recommended, but can be used in some cases where an inexpensive solution is desired.

For remote areas, or places where wired networks are not available or too expensive, bi-directional satellite systems, such as VSAT can be very suitable, especially if the number of ESP is quite large. In that case, the cost of the central station is quite important and the system should be used with all ESP's.

Finally, the usual wired networks should be the most suitable in most cases. Depending on the amount of data exchanged a choice can be made between X.25 networks over ISDN channel D (which offer only up to 9,6 Kb/s), and wired frame relay networks (which usually offer up to 2Mb/s, and can be extended to 8Mb/s).

6.7.3.1.4 Summary

The main elements of the discussion above can be synthesised into the table that is shown below. Only those technologies that are relevant for the link between the P30 System and the External Service Provider (ESP) terminator have been considered.

Table 4 P30 Analysis - Recommendations for Central to External Service Provider Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless mobile technologies (DECT, TETRA, GSM,…)		Not permanent Expensive	Not recommended
Broadcasting technologies (Satellite, DAB,…)		No return channel No need for large bandwidth on the down link	Not recommended
Leased line	Private	Expensive Not so much bandwidth needed	Not recommended except if more bandwidth needed.
Bi-directional satellite (VSAT)	No infrastructure	Antennas and amplifier (in particular at the centre)	Recommended if several ESP use this technology.
Bi-directional satellite (VSAT)	No infrastructure	Antennas and amplifier (in particular at the centre)	Recommended if several ESP use this technology. May also be shared with other terminators (e.g. Law Enforcement Agency).
Internet	Inexpensive	Uses public network No quality of service	Not recommended except if very low costs are looked for.

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Local Area Networks			If the ESP is at the same place as the Traffic Management Centre
Dial-up connections	Easy installation	Can be expensive	Can be interesting in some countries where these connection are inexpensive
Wired Private Networks	Adapted bandwidth. Manage by a Telecom provider Secured		Recommended

6.7.3.1.5 Conclusion:

This is a typical Central to Central communication where many technologies are at hand. In most situations, the preferred ones should be any well configured local area network (for local connection), X25 or Frame Relay. VSAT systems can also be used if several ESP are involved and wired networks to complicated or expensive to use. PSTN and ISDN solutions are possible depending on the cost in the area considered. Of course, for specific situations, there are other possibilities as shown above.

6.7.3.2 Central ↔ Law Enforcement Agency

6.7.3.2.1 Introduction

In System P30, there are exchanges between the Traffic Management Centre and one Law Enforcement Agency.

The Law Enforcement Agency sends information about the "rules" by which prosecutions can be reported for offences that have been detected within the urban road network. This information is received and processed by the Traffic Management Centre. The activities of road vehicles are monitored to ensure that they do not break any of the “laws” relating to vehicle movements. These “laws” will be both general ones (driving on the correct side of the carriageway) and those that particularly apply to vehicle movements within the road network.

The Traffic Management Centre collects information from the roadside about vehicle behaviour and identity. When a violation is detected, data about it is sent to the Law Enforcement Agency by the Traffic Management Centre for the eventual prosecution of the offender.

It is a Central ↔ Central interface.

6.7.3.2.2 Requirements

Typically, there is only one Law Enforcement Agency that exchanges information with the Traffic Management Centre. Hence, it is a simple point to point connection.

The amount of data transmitted depends on the format of the prosecution files transmitted, and the quantity of files sent. In particular, depending on the violation monitored and the monitoring system adopted, the information can contain simple text (e.g. number plate data, speed, etc.), image (e.g. a picture of the vehicle), or even a short video (e.g. short film illustrating the violation). Also, the quantity of files sent depends on the type of violation observed, the drivers' behaviour and the number of locations monitored. Accordingly, the data rate needed can vary a great deal.

Information could be transferred in batch mode, for instance, once every day. Nevertheless, in order to reduce the time needed to process prosecution files, it is preferable to send them at least every hour, and preferably within the minute.

The nature of the information transmitted calls for some security requirements. Information, such as the identity of the vehicle or its driver, must be protected against disclosure for obvious privacy reasons. The rules used to determine how the law will be applied (level of tolerance, etc.) should also not be disclosed. A Law Enforcement Agency is also likely to be attacked simply because it is an executive instance of the government. Elements of the network should be protected against attack. Prosecution files and rules must also be protected against alteration, and an electronic signature may be required[8]. To ensure these security requirements, authentication of both parties is needed for all transmissions.

6.7.3.2.3 Technical recommendations

Case A: The Law Enforcement Agency has a dedicated link with the Centre

If the Law Enforcement Agency has a dedicated link with the Centre, a simple point to point communication means must be set up.

The advantage of wireless solutions is not obvious at all for such a simple point to point communication link. In particular, broadcasting technologies such as DAB or satellite are not obviously suitable.

Traditional wired links are recommended. Depending on the data rate to be transmitted, the whole range of wired technologies should be considered. In particular, a private leased line between the Agency and the Centre should be an adequate solution. Even the alternative wireless terrestrial solution such as LMDS and MMDS should be examined, if the distance is not higher than several miles and the required data rates are quite high.

If costs need to be reduced, and if the amount of data to exchange is not very large, it is possible to use dial-up connections (such as ISDN or PSTN). In this case the data exchanges

[8] Electronic signature is currently being examined by most legal instances of European countries. It is almost sure that it will become accepted proof of authenticity by all tribunals very soon.

would have to be concentrated into short duration calls, which could be made at regular intervals.

A solution based on the use of Internet is not recommended. This is because of the security requirements exposed above.

Case B: The link with the Law Enforcement Agency is based on the same technology as other terminators.

A way of lowering telecommunication costs is to use the same technology for the Law Enforcement Agency as for the other terminators. This would have to be done in the, knowledge that security constraints are higher for the Law Enforcement Agency data and that the information sent to the other terminators is (probably) of a different nature.

However this does broaden the number of solutions available for linking the System to the Law Enforcement Agency. The technologies chosen to link the other terminators can also be used with the Law Enforcement Agency by simply adding a link of the kind. In particular, bi-directional satellite communications, such as VSAT, could be used.

Another possibility is to use broadcasting solutions, such as satellite or DAB. They can be also used to connect the Law Enforcement Agency provided that a return channel is set up for sending “rules” from the Law Enforcement Agency to the Traffic Management Centre. In that case, confidentiality mechanisms (encryption) must be used very carefully, since broadcasted messages can be received by anyone.

6.7.3.2.4 Summary

The main elements of the discussion above can be synthesised in the table below. Only relevant technologies for the link between the P30 system and the Law Enforcement Agency terminator have been considered.

Table 5 P30 Analysis - Recommendations for Central to Law Enforcement Agency Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless, mobile and broadcasting technologies (DECT, TETRA, GSM, Satellite, DAB)	No infrastructure required.	Not designed for that kind of application	Not recommended
Broadcasting technologies (DAB, Satellite)	No infrastructure required.	Not designed for that kind of application	Not Recommended, except if already used with other Terminators (e.g. ESP). A return channel (e.g. PSTN or ISDN) must be set up.

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Bi-directional satellite (VSAT)	No infrastructure required.	Antennas and amplifier needed in particular at the Centre.	Not Recommended. Except if already used with other Terminators (e.g. ESP).
Internet	Inexpensive	Uses public network No quality of service	Not Recommended. Not compatible with security requirements.
Local Area Networks	Inexpensive	No quality of service	Can only be used in a rare case: when the Law Enforcement Agency is at the same place as the Traffic Management Centre
Wireless Terrestrial (LMDS, MMDS,…)	No infrastructure required.	Specific terminal Equipment required	May be recommended if high bandwidth is needed and distance is not too high.
Dial-up connections	Easy installation Connections can be released between two connections Inexpensive in some countries.	Can be expensive for continuous data flows. Use of batch mode can increase the delay of the prosecution process.	May be recommended
Leased line	Private	Cannot be shared with other Terminators	Recommended (depends on bandwidth needed).
Wired Private Networks (X.25, Frame Relay, ATM).	Adapted bandwidth Managed by a Telecom provider Secured	Cannot be shared with other Terminators	May be recommended. May be shared with other terminators (e.g. ESP)

6.7.3.2.5 Conclusion

This is a typical Central ↔ Central point to point link with additional requirements concerning security. There are many possible methods that can be used to provide such a link, and must be chosen according to the needs of the local Traffic Management Centre. In particular, the bandwidth needed will have to be assessed. For most cases, the traditional wired technology is the solution. If sufficient care is taken to answer the specific security requirements of this link, it can be simpler to connect the Law Enforcement Agency with the same kind of link proposed to other terminators, which leads to reduction of costs.

6.7.3.3 Central ↔ Multi-Modal System

6.7.3.3.1 Introduction

The Traffic Management Centre exchanges priority requests with multi-modal systems. This enables to manage multi-modal crossings by giving the priority to one mode over an other.

In fact there are two possible cases. First case, the Multi-Modal System which communicates with the Traffic Management Centre is directly implemented at Multi-Modal Crossings, on the Roadside. Second case, Multi-Modal crossings are managed from a Centre, which communicates with the Traffic Management Centre.

Hence, it can be a communication interface of two kinds:

- Central ↔ Central, or
- Central ↔ Roadside

These two cases are studied separately below.

6.7.3.3.2 Requirements (Central ↔ Central case)

In the Central case, only a simple point to point communication link is required.

Requests are sent regularly in both directions, around every minute for each crossing managed by the central. The needed bandwidth is nevertheless very low, since each message is in the order of magnitude of several bytes.

Data must be transferred without delay, at least within a second so that the appropriate strategy can be applied at the crossing.

The channel must be very secure, since an alteration of the messages may lead to a misunderstanding in the priority requested. Such a misunderstanding may cause troubles at the crossing, and, in the worst case, contribute to the cause of an accident. Authentication of the sender is a very good way to facilitate the implementation of strong integrity protection mechanisms.

6.7.3.3.3 Technical recommendations (Central ↔ Central case)

Case A: The Multi-Modal system has a dedicated link with the Centre

If the Multi Modal Central system has a dedicated link with the Centre, a simple point to point communication link must be set up.

The advantage of wireless solutions are not obvious at all for such a simple point to point communication link, and is likely to be too expensive. In particular, broadcasting technologies such as DAB or satellite are not suitable since a return link should be set up.

Traditional wired links are recommended. The data rate is likely to be quite low, but the link will have to be permanent and fast. Here an X.25 link over ISDN channel D (9,6 kb/s) may be an adequate solution if available. Otherwise it is also possible to use PSTN or ISDN access, but in most countries this will appear too expensive because the link is permanent. Solutions such as Frame Relay are not suitable to such a low data rate, and ATM is excluded.

A private leased line between the two points can be the best solution, although the quantity of data exchange only for this purpose may not justify this choice.

A solution based on the use of Internet is not recommended, because of the security requirements. In particular, delays in data transmission would not be guarantied.

Case B: The link with the Multi-Modal system is based on the same technology as other terminators.

A way of lowering telecommunication costs is to use the same technology to link the Multi-Modal system and other terminators (e.g. ESP – see a previous section). Then, the specific security requirements of this link must be taken into account.

This broadens the number of solutions available for linking the Multi-Modal System. Some technologies chosen to link other terminators can also be used with Multi-Modal System by simply adding another link of the same kind. In particular, bi-directional satellite communications, such as VSAT, could be used.

6.7.3.3.4 Summary (Central ↔ Central case)

The main elements of the discussion above can be synthesised in the table below. Only relevant technologies for the link between the P30 system and the Multi-Modal System terminator have been considered.

Table 6 P30 Analysis - Recommendations for Central to Multi-modal System Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless, mobile and broadcasting technologies (DECT, TETRA, GSM, Satellite, DAB)	No infrastructure required.	Not designed for that kind of application	Not recommended
Broadcasting technologies (DAB, Satellite)	No infrastructure required.	Not designed for symmetric bi-directional application	Not Recommended
Bi-directional satellite (VSAT)	No infrastructure required.	Antennas and amplifier (in particular at the centre)	Not Recommended. Except if already used with other Terminators (e.g. ESP).
Internet	Inexpensive No quality of service	Uses public network	Not Recommended. Not compatible with security requirements.

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless Terrestrial (LMDS, MMDS,…)	No infrastructure required.	Specific terminal Equipment. Short distance. High bandwidth solution.	Not recommended
Dial-up connections (PSTN, ISDN)	Easy installation Connections can be released between two connections Inexpensive in some countries.	Can be expensive for continuous data flows. Use of batch mode can increase the delay of the prosecution process.	May be recommended
Leased line	Private	Cannot be shared with other Terminators	Recommended (depends on bandwidth needed).
Wired Private Networks low bandwidth (X.25).	Adapted bandwidth Managed by a Telecom provider Secured	None.	May be recommended. Should be shared with other Terminators (e.g. ESP)
Wired Private Networks, high bandwidth (Frame relay, ATM)	Managed by a Telecom provider Secured	Excessive cost for the low bandwidth that is needed.	Not recommended

6.7.3.3.5 Conclusion (Central ↔ Central case)

This is a typical Central ↔ Central point to point link with additional requirements concerning security. There are many possibilities to offer such a link, but traditional wired technologies seem the best at first sight.

If sufficient care is taken to answer the specific security requirements of this link, it can be simpler to connect the Multi-Modal System with the same kind of link proposed to other terminators. This will lead to reduction of costs and reduction of the complexity of the communications network.

6.7.3.3.6 Requirements (Central ↔ Roadside case)

In the case the Multi-Modal system is located at the Multi-Modal crossing on the Roadside, several point to point connections will be established between the Central and the Roadside locations.

Requests are sent regularly in both directions, around every minute for each crossing. The needed bandwidth is nevertheless very low, since each message has a size in the order of magnitude of several bytes.

Data must be transferred without delay, at least within a second so that the appropriate strategy can be applied at the crossing.

The channel must be very secure, since an alteration of the messages may lead to a misunderstanding in the priority requested. Such a misunderstanding may cause troubles at the crossing, and, in the worst case, contribute to the cause of an accident. Authentication of the sender is welcome to facilitate the implementation of strong integrity protection mechanisms.

6.7.3.3.7 Technical recommendations (Central ↔ Roadside case)

The requirements above are less demanding than those needed to link cabinets to the central – see previous section. If possible, to reduce the complexity and thus the costs, the best solution is to use the same technology to link the few Multi-Modal points to be connected to the Central location. Whenever possible, the merging of these two flows on the same lines should be studied. It should not be forgotten that it may also be possible to use the communication links that are required by other cabinets, such as those for traffic management.

Nevertheless, if the Multi-Modal points must be connected with dedicated lines (e.g. if there is no other cabinet in the area), or if the technology chosen for the connection of the other cabinets is too expensive to be extended to Multi-Modal points, inexpensive solutions[9] can be chosen. In particular, PSTN, ISDN, leased lines solutions should be studied and compared.

6.7.3.4 Central ↔ Maintenance Organisation

6.7.3.4.1 Introduction

The Traffic Management Centre monitors the road network, looking for the need to carry-out maintenance activities. This need may arise because of the use that road traffic has made of the network, the detection of faults in equipment, or weather conditions. Once the need for maintenance activity has been established, details are sent to the Maintenance Organisations for action. In return, the Maintenance Organisations send results from previous outputs requesting maintenance activities that affect the urban road network, or equipment used in its management.

It is a Central ↔ Central interface.

6.7.3.4.2 Requirements

This is a point to point communication link. There may be several Maintenance Organisations connected to the Traffic Management Centre. Regularly (e.g. as must as every hour), files of several kilobytes is transferred from the Maintenance Organisations to the Traffic Management Centre and from the Traffic Management Centre to the Maintenance Organisations.

[9] Prices and availability vary between countries

It is better if the files can be transmitted within a minute or preferably within several seconds, so that the sender has a quick result on the success of sending of the files.

Files must be protected against alteration and should be protected against unauthorised reading. Thus, authentication of the parties is necessary as well as mechanism to protect the content. Mechanisms such as signature of the files are also welcome, in order to avoid repudiation of the origin.

6.7.3.4.3 Technical recommendations

Unless other technologies are preferred because they were chosen to link other terminators, very simple links are recommended. PSTN links are very suitable. Costs may be lowered by sending several files together instead of sending them when they are produced, but that increases the time need to process files, and a priority system must be set up so that urgent needs are communicated immediately.

The use of Internet (through the building of an Extranet) may also be an inexpensive solution, since it is very likely that both parties will be linked to Internet in any case. Then, the security requirements must be met carefully, and the needed mechanisms will have to be implemented, e.g. authentication, encryption and signature.

6.7.3.5 Central ↔ Related Road Systems

6.7.3.5.1 Introduction

This section considers the physical interface between two Traffic Management Centres. This interface enables data flows between Systems covering adjacent jurisdictional or geographic areas to communicate with each other. These adjacent areas may cover urban systems, or inter-urban systems.

Such an interface may be needed in several cases. When there are two towns close enough together so that the traffic conditions and management in one has an impact on the other, their traffic management systems should communicate with each other. Also, when a town has an inter-urban road running through it, then the Urban Traffic Management System for the town should exchange data with the Inter-urban Traffic Management System.

This is a Central ↔ Central interface.

6.7.3.5.2 Requirements

A Centre my be connected with at least one other. When this happens, they should be able to interact with each other.

In some System installations the data will be transferred when exceptional conditions occur, in which case it would have to be fast and accurate as there will be a need for the receiving System to respond instantly. This type of data will be exchanged because of exceptional circumstances, for instance an incident, congestion and the clearance of either of these. In other System installations the first type of data transfer may be supplemented by a periodic exchange of data – say every 15 minutes. This second kind of data will probably cover general traffic conditions and be for information only.

The first kind of exchange requires point to point data connections, whereas the second may be based on diffusion. In this case broadcasting may be used.

The amount of information exchanged between Centres may vary very much. This is related to the mutual dependence of the regions controlled by the two Centres, and the complexity of the System used to manage the different infrastructures. The distance between the Centres can be either short (e.g. between two towns) or longer (e.g. between a remote inter-urban centre and a city centre).

With respect to security requirements, the transferred data is valuable and should not be disclosed. Data integrity should be protected especially because of emergency messages which may be included in the data that is exchanged.

6.7.3.5.3 Technical recommendations

The emergency data that is exchanged between Centres call for reliable and rapid data exchanges. This excludes dial up solutions such as dial-up over PSTN or ISDN, and connections over the Internet.

There is no need for mobility, which excludes mobile systems such as GSM, TETRA, and mobile technologies based on satellite etc. In most cases, the distance should exclude wireless solution such as LMDS and MMDS. Exchanges are quite likely to be bi-directional and there are few counterparts. This excludes most fixed satellite systems, except if they already used for other purposes. For instance, VSAT could be used if it is already set up for communications with ESP.

The most likely solutions are traditional wired networks, either based on leased lines or permanent ISDN access (X.25 over ISDN), X.25. If the amount of data to be exchanged requires it, Frame relay or even ATM may be envisioned.

The second type of data exchange (broadcast) does not call for severe requirements. Hence the network chosen for the first kind should also fit. Nevertheless, it may be necessary to carefully evaluate the amount of data being exchanged. This will apply in the case where the choice between networks is driven by the cost of the amount of data exchanged (such as X.25), or other networks such as leased lines.

6.7.3.5.4 Summary

The main elements of the discussion above can be synthesised in the table below. Only relevant technologies for the link between the P30 System and the Related Road System terminator have been considered.

Table 7 P30 Analysis - Recommendations for Central to Related Road System Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless, mobile and broadcasting technologies (DECT, TETRA, GSM, Satellite, DAB)	No infrastructure required.	Not designed for that kind of application	Not recommended
Broadcasting technologies (DAB, Satellite)	No infrastructure required.	Not designed for symmetric bi-directional application	Not Recommended
Bi-directional satellite (VSAT)	No infrastructure required.	Antennas and amplifier (in particular at the centre)	Not Recommended. Except if already used with other Terminators (e.g. ESP).
Internet	Inexpensive No quality of service	Uses public network	Not Recommended. Not compatible with security requirements.
Wireless Terrestrial (LMDS, MMDS,…)	No infrastructure	Short distance. Specific terminal Equipment. High bandwidth solution.	Not recommended
Dial-up connections (PSTN, ISDN)	Easy installation Connections can be released between two connections Inexpensive in some countries.	Can be expensive for continuous data flows. Use of batch mode can increase the delay of the prosecution process.	Not recommended
Leased line	Private	Cannot be shared with other Terminators	May be recommended (depends on bandwidth needed).
Wired Private Networks low bandwidth (X.25).	Adapted bandwidth Managed by a Telecom provider Secured		May be recommended. Should be shared with other Terminators (e.g. ESP)
Wired Private Networks, high bandwidth (Frame relay, ATM)	Managed by a Telecom provider Secured	Excessive cost for the low bandwidth that is needed.	May be recommended (depends on the bandwidth).

6.7.3.5.5 Conclusion

This peer to peer Central ↔ Central interface must be customised according to the specific needs of the exchanging counterparts. Nevertheless, the most likely solution should be found among traditional wired private networks, especially to fit the requirements for emergency messages.

It is important to notice that the Traffic Management Centre is also linked with other kinds of terminators, and although information exchanged with them differs, the telecommunication infrastructure that is used may be the same. The use of the same solution must be studied because it is likely to lower the complexity of the management of telecommunication, and thus to reduce the costs.

6.7.3.6 Roadside ← Vehicle

The communications with this terminator are exactly the same as those observed in section 6.7.2.2 except that priority vehicles considered here are Public Transport Vehicles instead of Emergency Vehicles. Requirements and recommendation do not differ much from that presented in 6.7.2.2, the recommendations and the conclusion are the same. Bearing in mind that priority requests from Public Transport vehicles should be overridden by that of Emergency Vehicles, please refer to this section 6.7.2.2 and the following for the analysis of this Roadside ← Vehicle interface.

6.7.4 Conclusion

In this section, the P30 System presented in the European ITS Physical Architecture is analysed from a telecommunication point of view. This System gives an example of traffic management where the intelligence is fully centralised in a Traffic Management Centre.

Both internal communication links and communication with Terminators have been observed.

From this analysis, several main conclusions may be emphasised:

1. The development of priority systems for Emergency and Public Transport vehicles based on local communication between the Roadside and Vehicles would benefit from the creation of a common standard.

2. In the case of P30, the communication between the Central and the Roadside must be especially reliable, but the amount of data exchanged is quite low. It is the kind of link that would benefit from being shared with other information such as information of Public Transport for the citizens

3. The Traffic Management Centre holds all the data about the equipment state and the traffic. This data has a great value and is interesting for a large number of different actors. The exact nature of the data as well as the requirements concerning their transfer is quite different for each actor, but it does not mean that the majority should not use the same kind of network. This would reduce the complexity of the network to access data and thus would lower the indirect costs linked to the management of such infrastructures. In other words, choosing the most effective network for each actor would be less efficient than choosing the most effective

network for a large number of communicating actors. A typical solution for most actors to access the information would be a TCP/IP/Frame Relay or X.25 private network with differentiated level of security features.

6.8 Traffic management: System P31

6.8.1 Introduction

This section deals with the analysis of telecommunication requirements of the P31 System described in the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c). This section falls in two sub-sections:

- Internal communications which deal with the communication flows between different locations of the system
- Terminator communications which deals with communication between the system and the terminators

In each of these sections, requirements for communications links are exposed, then technical recommendations are derived from these requirements.

The P31 System is very similar to the P30 System in terms of communication requirements. In order to avoid discussion of the same issues twice, the analysis of P31 is often built upon that of the P30 System. Hence, the reader will often be invited to refer to the analysis of that System (see previous section).

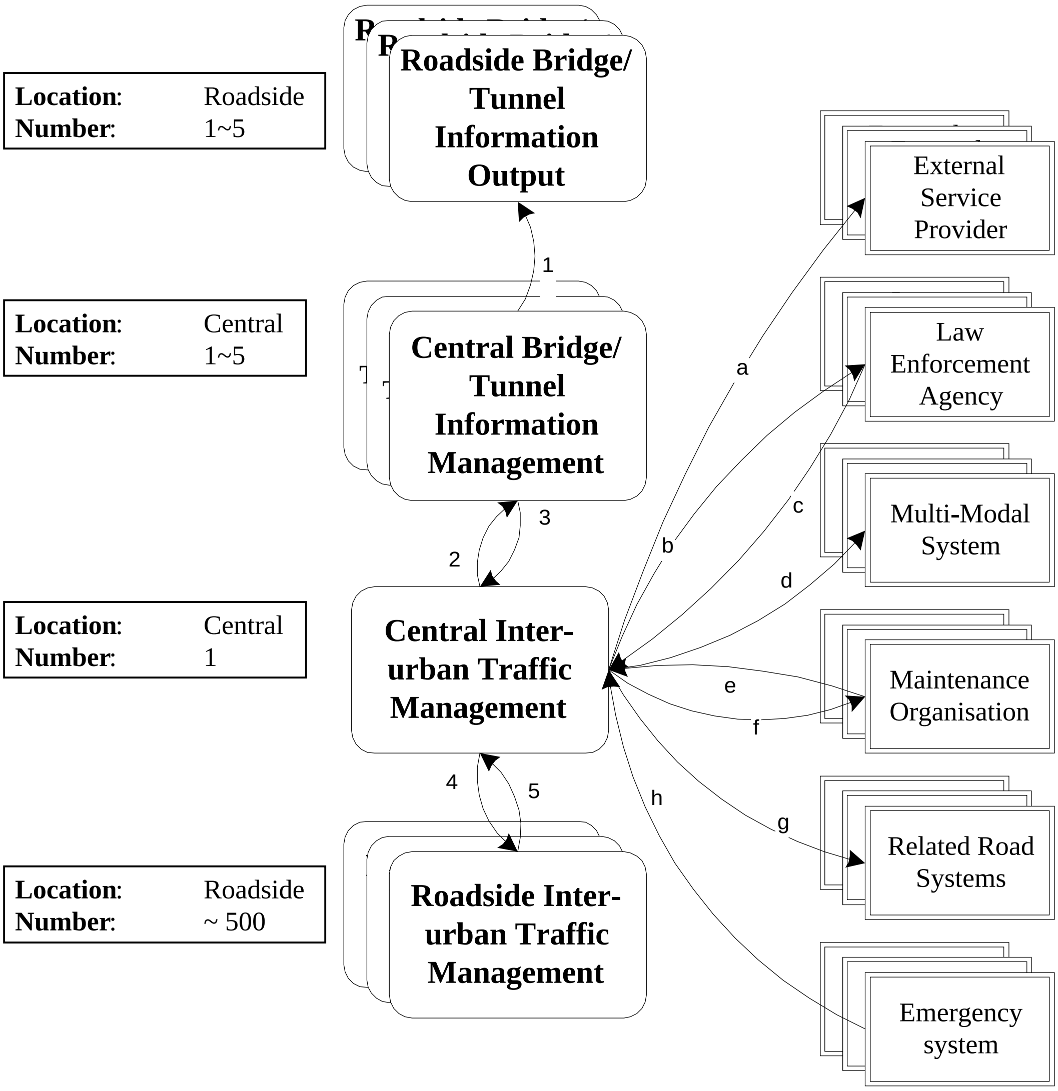
This System provides facilities that enable the management of road traffic that is using an inter-urban road network. In addition to the actual traffic management facilities, the System includes additional facilities for the maintenance of the physical road network and the equipment used by the System for the management of traffic. Links from this System to other Systems are also provided to enable co-ordination of traffic management across organisational boundaries.

Like the previous System for urban networks (P30), this System has been included to show inter-urban traffic management in its simplest form. For example, there are no facilities for Incident or Demand Management, nor any Environmental Monitoring. However bridges and tunnels are included and there are two additional facilities not yet found in use among inter-urban traffic management systems currently implemented across Europe. The first is vehicle speed control, and the second is the links to the Multi-Modal Systems. The first facility has been the subject of recent testing in Europe and will enable vehicle speeds to be regulated without the need for physical devices such as speed ramps. The second facility will enable the movement of vehicles on other modes of transport such as railways and canals to be co-ordinated with road traffic movements.

Figure 9 on the next page shows the overall communication links of the P31 System for controlling up to 500 pieces of roadside equipment. They may be signs, or detection equipment of various types. Interfaces to bridge and tunnel control systems and roadside equipment are also included. The system may serve one particular inter-urban road or network, or alternatively all those in a large geographic area, e.g. a German State, French Provence, or UK Region.

Analysis of the communications links has been divided into two parts. These comprise Internal Communications - links 1 to 5 in the Figure, and Terminator Communications - links a to h in the Figure below.

Figure 9 P31 - Communications Diagram



6.8.2 Internal Communications

The P31 System is a centralised system that is spread over two locations: Roadside and Central. There are bi-directional exchanges of information between the Roadside and the Centre (link 4 & 5 in Figure 9), bi-directional communications between two Central locations (link 2 & 3 in Figure 9), and a mono-directional communications between the Central location to the Roadside (link 1 in Figure 9). Hence, the P31 System deals with the following communication link:

- Central ↔ Roadside

- Central ↔ Central
- Central → Roadside

At the Centre location, there are two kinds of sub-systems: the Traffic Management Centre and the Bridge/Tunnel Information Management Centre.

In the centralised configuration described by the P31 System, there is only one central physical entity[10] which implements the Traffic Management Centre sub-system. However it can be linked with several Bridge/Tunnel Information Management Centres. In fact the Bridge and Tunnel Information Management Centre can be either located in the same building as the Traffic Management Centre, or be located at a different site.

At the Roadside location there are two kinds of sub-systems: Roadside Bridge/Tunnel Information Output and Roadside Interurban Traffic Management. The first one manages output equipment, such as variable signs, the second does this too and also deals with additional roadside equipment (telemetry, detection, control, etc.). Equipment is usually put inside a single "box", which size varies from one country to another and from one supplier to another. The “box” is usually called a *cabinet* and this is placed at or near the physical roadside. Typically, up to five hundred cabinets can be spread over the interurban network, and there can be around a hundred specific cabinets for law enforcement data collection.

6.8.2.1 Central ↔ Roadside

6.8.2.1.1 Requirements

The Centre ↔ Roadside links are spread over all the inter-urban road network area and are managed by the equipment at the Central location. Hence, scope of communication links can be the national level.

From the Central to the Roadside, commands are sent to the cabinets, usually to activate the output of messages or instructions to drivers, as part of traffic management strategies. This will be called the down-link.

The up-link, from the Roadside to the Central, is richer; several kinds of data must be taken into account:

- Data collected about the traffic flow, the Service Area situation and the traffic management state are sent to the Central equipment.
- The cabinets also send data about the equipment state (monitoring and state data including failures).

[10] It is technically reasible to split up the Central physical entity into two or more parts that may be implemented in different places. The reason for not doing this is usually that it produces savings in communications costs, because a private network has to be used. Nevertheless, if multiple central sites are chosen, these sites should look as a unique entity for the rest the System, in particular from the Roadside equipment. It is not the purpose of this analysis to describe the private network which could be used to link different sites. Therefore only the case where a unique physical central site is used will be considered.

- In addition, information collected by law enforcement equipment, which may include photo or video, is sent by the dedicated cabinets to the equipment at the Centre.

The commands sent on the down-link are executed by the equipment managed form the cabinet. These commands are sent sporadically when a change has to be implemented (management of lanes, displays of variable signs). As all the “intelligence” is centralised in this model and that the cabinets do nothing more than execute orders, the link must always be available, and it must be very robust.

The up-link is used to transmit the data which will enable the equipment at the Centre to monitor the Roadside equipment and the traffic conditions. This kind of information is transmitted around every minute.

In addition, a strong user requirement is to reduce the time needed to process law enforcement data. A sensitive objective can also be that they should reach the Centre within an order of magnitude of a minute.

The amount of data transmitted from the Centre to the Roadside cabinets is very little for each session, in the order of magnitude of a few (less that 10) bytes for each cabinet.

For the up-link, the situation is quite different. Most cabinets do not send law enforcement data and so need to send messages which are again in the order of magnitude of 10 bytes. The up-link data for cabinets with law enforcement equipment depends on the type of application that is being used. This may require various types of data to be sent, ranging from simple data (in the order of magnitude of a 100 bytes), or photographs (in the order of magnitude of several kilobytes per photograph), or even video (in the order of magnitude of a 1 Mbyte per second).

Each cabinet must receive its own set of commands. So, it is not possible to make use of broadcasted messages to reduce the amount of transmitted data[11]. However, locally, it may happen that the same message is displayed on several variable message signs, if not managed by the same cabinet. In this case, multi-point protocols may then be useful.

This communication link is based on communication ends which are not mobile. Therefore it does not necessarily call for wireless communications.

As far as security requirements are concerned on the down-link, there is not very much to gain for an attacker in taking control of the Roadside sub-system. In addition, it would cost a great deal to purchase the adequate equipment, and the knowledge needed to use it successfully would be great. There is thus very little risk that an attacker would try to take control of the Roadside sub-system. Hence there is extremely little need for authentication of the down-link communications.

[11] However, this does not mean that broadcasting telecommunication technologies (such as satellite) cannot be used to send these messages. Technically, each message can be broadcasted to all cabinets where they can be filtered so that only the appropriate targeted cabinet actually uses the message. Hence, specific (and not broadcast) messages are sent to specific targets on a broadcast telecommunication technology.

Of course, confidentiality is not at stake either: the data that is transmitted is intended to be displayed to all citizens in the area. As there is no confidentiality, there is no need to authenticate the data when it arrives in the cabinets at the Roadside.

However, there are security requirements in the field of data integrity. Messages are to be used almost in real time, and have direct impact on the traffic flow. Any alteration of the information would result in disorganisation of the traffic flow. Hence, the information sent must not be altered, this calls for special attention to data integrity. In addition, it must be ensured that each set of data reaches the appropriate cabinet, because what is output to drivers by the equipment connected to a cabinet may be unique to its location. Hence, additional checking may be performed to avoid any mistake in the destination of the data.

Security requirements are quite different for the up-link, especially because of law enforcement data. All data from the cabinet needs some kind of protection for its integrity so that each set of data can be attributed to a particular location. Additionally, cabinets linked to law enforcement systems must provide features to authenticate and ensure integrity of the data that is being transmitted. This is to enable it to be proved that the data has not been altered since it left the cabinet. For the sake of privacy, encryption should be used to protect this messages which contain information on the citizens.

6.8.2.1.2 Recommendations

The requirements defined above, show that three types of link must be in fact distinguished:

1. Sporadic low rate communication links: such equipment as informative VMS that only need an update from time to time.

2. Permanent low rate communication links: such equipment as traffic flow monitoring systems are reporting the traffic flow permanently

3. High rate permanent (or quasi-permanent) communication links: some law enforcement systems may transmit images continuously to the Centre.

These three types of links have different communication needs, which call for different communication systems. In addition they are not necessarily located at the same place, which makes it difficult to merge communications over the same link. However, for the sake of the reduction of complexity and costs, searching for a common technology can appear fruitful.

Inter-urban road network operators often operate their own telecommunication wires buried in the pavement alongside the actual roadway. These networks are or will be, based on fibre optics and therefore capable of carrying data at high speeds.

These networks are mostly appropriate for the third kind of link (law enforcement), which can appear very expensive otherwise. This can be also appropriate for the second kind of link, and even for the first kind, provided that the cost of linking low data rate equipment to these high speed wires is not too high[12].

[12] Some protocols (such as PDH) require very costly equipment to extract low data rate communication. It is possible to lower this costs by using other kind of protocols (such as SDH compared to PDH).

In the situation where there is no operator owned communications network, the possibility of being connected to a X.25 or Frame Relay wired network can be studied with the local telecommunication operators. As the connection is not established with a usual building, special tariffs may well be applied. It is the same with PSTN and ISDN access, and the tariff may very much vary from one country to the other. It is likely that usual tariffs will not apply and that the solution will appear expensive. The question of the bandwidth will lead to wired solution such as X.25 for links of the first or second kind. More bandwidth efficient wired technologies such as Frame relay or even ATM/SDH will be needed for the second kind. Dial-up access such as PSTN and ISDN are not suitable for permanent access.

Broadcasting technologies, such as satellite or DAB are not appropriate since all communications are bi-directional. An exception can be made for informative VMS systems, and more generally for the first kind of link. In that case, it is not necessary to report failures immediately. A simple link such as a GSM link is then sufficient. If available at a reasonable price, a PSTN line is also suitable.

On the other hand, bi-directional satellite systems such as VSAT may be very suitable. This type of wireless solution applies very well on a national level and avoids the cost of a large terrestrial infrastructure. However these technologies do not provide high bandwidth yet, but this is likely to be improved in the future. At the moment this makes them unsuitable for the links of the third kind.

Mobile wireless terrestrial networks, such as GSM or TETRA, may be suitable for the first kind of link, but are not suitable for permanent communication links 1 and 2. Of course, technologies limited in geographical scope such as DECT, LMDS or MMDS cannot cope with the distances involved with inter-urban road networks.

In addition to this low level specification, for law enforcement flows from the Roadside to the Centre, which concern only part of the cabinets, specific security requirements must be covered. Mechanisms must be implemented to provide authentication of the source, signature of data and low confidentiality. However for the wired technologies that do not implement these features at their layer, this should be implemented using higher communication layers such as the application layer.

6.8.2.1.3 Summary

The main elements of the discussion above can be synthesised in the table below and on the next page. Only relevant technologies for the link within the P31 System that enables data to be exchanged between the Central and the Roadside locations have been considered.

Table 8 P31 Analysis - Recommendations for Central to Roadside Bi-directional Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless mobile (DECT; GSM; TETRA…)	Reduced infrastructure costs for the telecom operator.	Not adapted to permanent links. Network sometimes saturated.	Not recommended

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
		Links are not robust.	
Wireless fixed (LMDS; MMDS)	Bi-directionnal high bandwidth	Links are not robust. Limited distance (3~10 miles).	Not recommended
Broadcasting (MOBITEX, DAB, Satellite)	Low infrastructure costs	No up-link.	Not recommended except for first kind of communication and with a dial-up return link (e.g. GSM).
Satellite bi-directional (VSAT)	Low infrastructure costs	Needs a 1.2 m antenna (Case B: low bandwidth) Links are not as robust as wired links.	May be recommended for the first and second kind of link. The third kind of link may require more bandwidth.
Private owned wired network	Lowered infrastructure costs	May be difficult to extract low data rate connections.	Recommended if available.
Wired, Dial-up (PSTN;ISDN)		Most of the time unsuitable for permanent links	May be recommended for links of the first kind, if installation costs are not too high. Not recommended for permanent links.
Wired Permanent X25	Robust Permanent Available in most countries	Installation and infrastructure costs may be high because of the location of the roadside	Recommended if access costs not too high.
Wired Permanent Frame Relay, ATM, SDH.	Wide bandwidth Low delay	Quite expensive. Installation and infrastructure costs may be high because of the location of the roadside	May be used for third kind of link.

6.8.2.1.4 Conclusion

This Centre ↔ Roadside interface is very specific for two reasons. Firstly because of the potential distance between the Roadside and the Centre and secondly because the Roadside is not a common location for telecommunication links to be installed by a telecommunication operator.

However it can benefit form the telecommunication networks usually owned by the road network operator. If not, several wireless solutions are at hand and enable remote locations to be reached. Closer locations, or those requiring more bandwidth may require traditional wired links.

Of course, what ever the telecommunication link is selected, the specific security requirements mentioned above must be taken into account carefully.

6.8.2.2 Central → Roadside communications

This communication link enables the output of messages from the Bridge/Tunnel Information Management Centres on the Bridge and Tunnel infrastructure.

There are three variations in the location of the Bridge/Tunnel Information Management Centre to consider. They can be defined as follows.

1. The Centre is not located at the same place as the Bridge or Tunnel it manages and it is located at the same place as the Traffic Management Centre. Then from the telecommunication point of view, the same requirements apply as those of the Traffic Management Centre for its own output systems. Using the same network would of course limit the complexity of the communication system and costs. Please refer to the analysis in section 6.8.2.1. Note that in the technical recommendations, only the first two kinds of link are relevant, since the communication with Law Enforcement Agencies is not considered here.

2. The Centre is not located at the same place as the Bridge or Tunnel it manages and it is not located at the same place as the Traffic Management Centre. Then from the telecommunication point of view, the same requirements also apply as those of the Traffic Management Centre for its own output systems. Using the same kind of network would provide some limitation of the complexity of the communication system and its costs, but it is not possible to use the same physical wires. Please again refer to the analysis in section 6.8.2.1.

3. The Centre is located at the same place as the Bridge or Tunnel. In this case the most suitable solution is to use traditional wired or wireless local networks. Often it will be possible to use a proprietary solution to connect equipment such as VMSs to the Centre.

6.8.2.3 Central ↔ Central communications

6.8.2.3.1 Introduction

This section analyses the Central ↔ Central communication link between the Traffic Management Centre and the Bridge/Tunnel Information Management Centres.

This section only takes into account the case when they are not located at the same physical place. When they are, a traditional area network can provide a simple cost effective solution.

6.8.2.3.2 Requirements

This is a point to point telecommunication link. If there are several Bridge/Tunnel Centres, there may be several point to point telecommunication links of the same kind.

There are several kinds of data exchanged between the two Centres. Depending on the autonomy of each Centre, there may be many different requirements concerning those exchanges.

From the Bridge/Tunnel Centre to the Traffic Management Centre the data flows may be the following:

1. Information about the traffic and other measures made on the Bridge/Tunnel;
2. Information that can be used in displays to drivers on the inter-urban network as they approach the Bridge/Tunnel;
3. Current strategy applied for the management of the Bridge/Tunnel.

From the Traffic Management Centre to the Bridge/Tunnel Centre the data flows may be the following:

4. Information about the traffic and other measures being implemented on the inter-urban road network;
5. Information that can be used in displays to drivers on the Bridge/Tunnel;
6. Current strategy applied for the management of the inter-urban traffic road network.

And also, especially if there is little autonomy at the Bridge/Tunnel Centre:

7. Commands to influence or even set the Bridge/Tunnel strategy;
8. Information to be displayed “as is” on the Bridge/Tunnel infrastructure.

Numbers 1, 3, 4 and 6 need to be sent about every minute. This data need not be protected against disclosure but against alteration. It should represent only a few bytes, thus requiring very low bandwidth.

Numbers 2 and 5 depend very much on the application. For some, a continuous update must be received, for others messages must be sent when an event occurs. Some applications will require that the data must not be corrupted, for example when the closing/opening of lanes is being signalled. Most other data will contain informative messages that can afford some error in the transmission. In all these cases, the amount of data to be exchanged is quite low.

Numbers 7 and 8, which are needed when the Bridge/Tunnel Centre completely relies on the Traffic Management Centre, require a very reliable permanent bi-directional link The bandwidth is again likely to be very low.

6.8.2.3.3 Technical recommendations

There are many different situations for the location of the two Centres. They may be close to each other, the Bridge/Tunnel Centre may be in an urban area or in a remote place were no wired infrastructure is available, or the Bridge/Tunnel Centre may be autonomous, or it may rely completely on the Traffic Management Centre.

Since there is no general case, the whole range of telecommunication technologies may be used. However some recommendations can be made and they are presented below.

Most communication links are likely to be permanent – especially those in Numbers 1 and 4 above. If available, the use of the telecommunication infrastructure owned by the Road Operator should be the less expensive solution. Otherwise, wireless links are very likely to be the second best solutions in a non-urban area. In urban areas, wired links are likely to be more suitable.

Although there is little need to have a very short delays in most cases (Numbers 1 to 6), making use of an existing connection to Internet as a medium is not likely to be a proper solution. This is because the connection between the two Centres must be very reliable, and when emergency situations are involved, no delay is acceptable. A (virtual)[13] private network solution would be much more suitable, providing that the costs are affordable, and that there is proper protection against data being available to unauthorised third parties.

As the communication is mostly bi-directional, it is unlikely that broadcasting communication technologies (such as DAB or broadcasting satellite systems) are suitable. However, if there are very few communication from the Bridge/Tunnel Centre to the Traffic Management Centre, such a solution can be chosen by building a return link on low bandwidth dial-up networks (mobile, like GSM or TETRA, or wired like PSTN or ISDN).

In most cases, the Traffic Management Centre is likely to be linked with many other similar Centres. However there are likely to be very few Bridge/Tunnel Centres connected with the Traffic Management Centre. To reduce the complexity of the telecommunication management and the corresponding costs, it is worth examining to see if the same technology can be used with Bridge/Tunnel Centres as with other Centres that are linked with the Traffic Management Centre.

6.8.3 Terminator Communications

6.8.3.1 Introduction

As will be seen from Figure 9, the P31 System exchanges data with 14 terminators. Only 6 out of these 14 terminators are considered in this section. The others are based on human-machine interfaces which do not require telecommunication support[14]. These 6 terminators, are Emergency Systems, Related Road Systems, Maintenance Organisation, Multi-Modal System, Law Enforcement Agency, and External Service Provider.

6.8.3.2 Emergency Systems ↔ Central

6.8.3.2.1 Introduction

This section considers the physical interface between Emergency Systems terminator and the Traffic Management Centre.

So that Emergency Vehicles may by-pass other traffic, it may be required that they are granted priority, by measures, such as giving them the sole use of a particular lane of the carriageway. This may thus require that the use of a lane by other vehicles is restricted. To

[13] Virtual private network: several different companies use the same telecommunication infrastructure but the operator guaranties that each company can access only their own data and not that of others.

[14] These interface are addressed in Chapter 8 where there is a general discussion of interfaces including those using HMI.

set up the lane restriction, the Emergency Services must send a priority request through the Emergency Systems ↔ Traffic Management Centre interface.

This is a Central ↔ Central interface.

6.8.3.2.2 Requirements

Typically, Emergency Services collect data about the position of their vehicles through mobile telecommunication systems. When an incident occurs, they chose the best strategy to send emergency vehicles to the incident location. To optimise the rescue time, they need to send a priority request to the Traffic Management Centre. The Centre will reply with a response that tells the Emergency Services whether priority has been provided, and (for example) a reserved lane has been created.

When the lane is reserved for emergency vehicles, the Emergency Services tracks their progress. It can then sends reports to the Traffic Management Centre so that reserved lanes are opened again to normal traffic once the emergency vehicles have passed.

There may be several Emergency Services connected to a single Traffic Management Centre, and this may be typically around five. They must each be able to communicate with the Centre simultaneously.

Only a simple point to point communication link is required for the system operated by each Emergency Service. The communication link will be needed each time that an incident occurs, which can vary. The main factors governing the variation will be the geographic scope of the road network served by the Traffic Management Centre, the size of the area managed by the Emergency Service, and the rate of incident occurrences. Typical requirements are the establishment of a communication for priority request up to once every hour.

Each request will require less than a kilobyte, and should be sent at least within a second. A low bandwidth connection is sufficient, but should be established rapidly (at least within a second). The Centre will have to make a decision (computer aided or not), and when the decision is taken, the transmission of the acknowledgement, the proposal of an alternative route, or a refusal of the priority request should also reach the Emergency System at least within a second.

Of course, it is possible that higher interactivity is required by the routing systems of the Traffic Management Centre, and Emergency Services Centre. It may be that additional functionality will be provided, such as the negotiation of the best route between the two Centres, transmission of the location of the vehicles, etc. This will simply lead to an increase in the required bandwidth and the availability of the communication link.

The link must be very secure, since any corruption of the data may lead to a misunderstanding in the priority requested. Such a misunderstanding would hinder the efficiency of Emergency Services. Authentication of the sender is useful to facilitate the implementation of strong integrity protection mechanisms. For some Emergency Services (e.g. Police), additional confidentiality mechanisms are also required.

6.8.3.2.3 Technical recommendations

There is no need for a mobile communication link. The opposite is in fact the case, i.e. the link must be permanently established. Solutions such as wireless solutions as GSM, TETRA, DECT etc. are therefore not suitable.

The advantages of wireless solutions are not obvious for such a simple point to point communication links, and they are likely to be too expensive. In particular, broadcasting technologies such as DAB or satellite are not suitable since a return link should be set up.

Unless other kinds of data are to be transmitted, virtual private networks based on ATM and even Frame Relay appear to offer to much unneeded bandwidth.

Also a solution based on the use of Internet is not recommended, because of the security requirements, and because in particular, delays would not be guarantied.

Dial-up systems such as PSTN or ISDN would deal well with the fact that the exchanges are very sporadic. Nevertheless, emergency situations require that the connection is established without delay, which makes such a solution a little risky. However, it may be possible to anticipate the call establishment (e.g establish the call once the incident occurs and before establishing the intervention strategy), so that the communication link is already available at the moment the priority request is to be sent.

Permanent connections, such as leased lines or connection through an X.25 network, can appear more expensive, but they offer the possibility to send priority requests immediately, which is a major feature in emergency situations.

A good solution, if available, is to provide the connection for the link using X.25 over the D channel of an ISDN access. The access is permanent and calls can be performed on the B channels for other purposes. The bandwidth is usually limited to 9,6 kb/s, but this should be sufficient in most types of data.

More generally, the problems resulting from the need for a permanent link that is only used from time to time may be avoided if the Emergency Services can make other uses of communication link. For example, the Emergency Services may have, or be planning to have, a direct connection with the Traffic Management Centre to obtain continuous updates of data about current traffic conditions. A link for this purpose can be utilised for both types of data – i.e. priority requests and the collection of traffic conditions data. In addition, such a link can be secured with a PSTN or an ISDN dial-up connection.

6.8.3.2.4 Summary

The main elements of the discussion above can be synthesised in the table shown on the next page. Only relevant technologies for the link within the P31 System between the Traffic Management Centre and the Emergency Systems terminator have been considered.

Table 9 P31 Analysis - Recommendations for Central to Emergency Systems Communications

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wireless, mobile and broadcasting technologies (DECT, TETRA, GSM, Satellite, DAB)	None	Not designed for that kind of application	Not recommended
Broadcasting technologies (DAB, Satellite)	None	Not designed for symmetric bi-directional application	Not Recommended
Bi-directional satellite (VSAT)	None	Antennas and amplifier (in particular at the centre)	Not Recommended. Except if already used with other Terminators (e.g. ESP, Multi-Modal systems).
Internet	Inexpensive No quality of service	Uses public network	Not Recommended. Not compatible with security requirements.
Wireless Terrestrial (LMDS, MMDS,…)	No infrastructure reuired.	Specific terminal Equipment. Short distance. High bandwidth solution.	Not recommended
Dial-up connections (PSTN, ISDN)	Easy installation. Connections can be released between two connections. Inexpensive in some countries. Private.	Delay needed for connections.	Not really adapted except if connection can be anticipated.
Leased line	Private	Cannot be shared with other terminators	Recommended (depends on bandwidth needed).
Wired Private Networks low bandwidth (X.25).	Adapted bandwidth. Managed by a Telecom provider. Secured	None	May be recommended. Should be shared with other terminators (e.g. ESP)

Technology	Main Advantages	Main Drawbacks	Conclusion and Other remarks
Wired Private Networks, high bandwidth (Frame relay, ATM)	Managed by a Telecom provider. Secured	Excessive cost for the low bandwidth that is needed.	Not recommended except if the System needs more bandwidth for extra functions.

6.8.3.2.5 Conclusion

This is a typical Central ↔ Central point to point link with additional requirements concerning security. There are many possible ways to offer such a link, but traditional wired technologies seem the best at first sight.

If the specific security issues required by this link can be resolved, it can be simpler to connect this terminator with the same kind of link proposed to other terminators. This will lead to reduction of costs and reduction of the complexity of the System.

6.8.3.3 Central → External Service Provider

This interface is similar to that analysed for the P30 System. Please refer to the corresponding section 6.7.3.1.

6.8.3.4 Central ↔ Law Enforcement Agency

This interface is similar to that analysed for the P30 System. Please refer to the corresponding section 6.7.3.2.

6.8.3.5 Central ↔ Multi-Modal System

This interface is similar to that analysed for the P30 System. Please refer to the corresponding section 6.7.3.3.

6.8.3.6 Central ↔ Maintenance Organisation

This interface is similar to that analysed for the P30 System. Please refer to the corresponding section 6.7.3.4.

6.8.3.7 Central ↔ Related Road Systems

This interface is similar to that analysed for the P30 System. Please refer to the corresponding section 6.7.3.5.

6.8.4 Conclusion

In this section, the P31 System described in the European ITS Physical Architecture Deliverable Document (D 3.2) is analysed from a communications point of view. This System provides an example of inter-urban traffic management in which the intelligence is mainly centralised in a Traffic Management Centre.

Both internal communication links and those communication links that connect with terminators have been analysed. From this analysis, several overall conclusions have been produced. They are as follows.

1. Many interfaces with terminators are similar to those used for urban road network management - see section 6.7 for an analysis of the P30 System. It is possible to profit by the knowledge gathered while implementing one System to implement the other.

2. In the case of the P31 System, the Central ↔ Roadside interface is very specific and represents in fact several kinds of links. Using the same kind of solution with the objective to reduce the telecommunication costs is not necessarily the best solution.

3. The Traffic Management Centre holds all the data about the equipment state and the traffic. This data has a great value and is interesting for a large number of different actors. The exact nature of the data as well as the requirements concerning its transfer is quite different for each actor, but it does not mean that the majority should not use the same kind of network. This would reduce the complexity of the network to access data and thus would lower the indirect costs linked to the management of such infrastructures. In other words, choosing the most effective network for each actor would be less efficient than choosing the most effective network for a large number of communicating actors. A typical solution for most actors to access the information would be a TCP/IP/Frame Relay or X.25 private network with differentiated levels of security features.

6.9 Traveller Assistance: System P60

6.9.1 Introduction

This section deals with the analysis of telecommunication requirements of the system P60 described in the European ITS Physical Architecture Document (D 3.2) – see reference 10(c).

The System Traveller Assistance and Route Guidance System (P60, Area Traveller Assistance) provides facilities that enable a traveller to plan journeys in advance and then execute them. Additional facilities are provided that enable the traveller to take account of changes in relevant conditions for the journey and thus update the journey plan. The means to provide the user with on-line guidance while the journey is in progress, even if the user is located inside the vehicle and on the move, are added to the system

This system exchanges data with 13 terminators. Three of these, Static Traveller, Dynamic Traveller and Driver, provide Human-Machine Interfaces (HMI’s). These interfaces do not require telecommunication support are not further discussed within this section, but are discussed in general terms in Chapter 8.

The other ten terminators are External Service Providers (General Information Provider, Multi Modal Travel Information Provider, Vehicle Renting Agency, Planned Event Organiser, Bookable Service Provider, Geographic Information Provider), Financial Clearinghouse, Parking Operator, Related Road System and Location Data Source. The following sections will discuss the communication of the System with these terminators and the internal communication within the System.

6.9.2 Communications

Within the P60 System the following communication links are addressed:

- Kiosk ↔ Kiosk
- Central ↔ Kiosk
- Kiosk → Vehicle
- Central → Vehicle

It should be noted that the Kiosk location can sometimes be seen as being of the Central type. The instance of this will depend on the actual structure of the System implementation.

6.9.2.1 Kiosk ↔ Kiosk

The Kiosk ↔ Kiosk communication depends on the set-up of the actual implemented System. Depending on the System developer’s decisions, some of these Kiosks may have the character of something at a Central location. However, within this Chapter it will be assumed that the Kiosk location is somewhere different.

The communication between the different Kiosks will take place when a Traveller asks for information or communication procedures that the particular Kiosk being used cannot supply or perform. This may be a special information the Kiosk has not stored in its database or it may be a requested communication to external terminators this Kiosk is not connected to via a direct communication link.

Thus the definition of these communication links depends on the intelligence of the Kiosk itself and of its connectivity to the external terminators. Thus the following demands on communication links must be taken into account by the system developer:

- The needed information may either be transmitted as a result of a users request or some means of broadcast communication may be used to update the database of the Kiosks within the system on a regular base.

- Security requirements are only needed when any means of payment are involved. Thus the demand of authentication, confidentiality or data integrity depends on the commercial model used to set up the real system. E.g. if the system is financed by advertising and all information transfer with the user is free of charge any means of security would increase the System’s complexity.

6.9.2.2 Central ↔ Kiosk

The Central ↔ Kiosk communication is part of the communication links to the external terminators. These external terminators within this System are supposed to be organised as

Central Systems. Within the P60 System they are External Service Provider, Parking Operator and Financial Clearing House.

Again, these communication links will only be used when the user asks for a special service (or information) coupled with the particular terminator. In addition, the communication will only take place immediately after the request is performed and only if the required information is not stored within the Kiosk's own database.

Only in direct dependency on the needed service (or information) the requirements on the communication link can be defined. Thus first the service itself must be defined before all the demands on the communication link can be identified. However, depending on the Terminator the following basic requirements can be identified:

- Financial Clearinghouse: When payment procedures are involved all communication must be performed under high security aspects. Thus authentication, confidentiality or data integrity must be supported. Only point to point communication can be used. The needed bandwidth for each transaction may be low. The overall latency (as seen from the Travellers point) for the financial transaction should be as low as possible.

- External Service Provider: The databases within the Kiosk can be updated via different kinds of media. The requirements on this communication depend on the services offered by the External Service Provider and the means of display of this information.

- Parking Operator: The communication with the Parking Operator must be live, thus no long-term databases within the Kiosk may be used. If the service offered at the Kiosk will include the booking of parking lots, point to point communication is needed. In addition, some means of low or medium security (e.g. authentication) may be needed (maybe even high security for payment reasons). If only the amount of available parking space is displayed to the customer (dynamic) broadcast media may be useful.

6.9.2.3 Kiosk → Vehicle

The communication Kiosk → Vehicle takes place when the Traveller Assistant is directly coupled with the In-Vehicle Device.

This communication is short range by nature. Only the information the Traveller Assistant has gathered from the Traveller Support Centre is transmitted to the In-Vehicle Device. Thus the amount of transmitted data depends on the size of the data storage within the Traveller Assistant. Finally the information will be presented to the driver of the vehicle with special in car devices via human-machine interfaces.

Because of direct connection between both devices no means of security are recommended. As the Traveller Assistant holds all the information the In-Vehicle Device can be seen as a special device for information presentation developed for the use by the driver of a vehicle.

As the In-Vehicle Device of P60 System has no means to perform any communication to the Traveller Support Centre no service can be initiated by the In-Vehicle Device where payment may be involved. Thus no means of security involved with payment transactions are needed.

6.9.2.4 Central → Vehicle

The communication Central → Vehicle takes place when the information stored within the In-Vehicle Device must be updated.

As the communication is only defined from Central to Vehicle no request can be sent from the Vehicle (e.g. Driver) to the Central. Thus in first way broadcast media are fitted to perform these updates on a regular time base.

The only possibility to perform any personalisation of this service is to save a users profile and send any change of this profile via broadcast services to all possible recipients.

6.10 Conclusions

This Chapter has provided several analyses of the data flows in "example Systems" from the European ITS Physical Architecture. It would be miss-leading to make any generalisations of the results, however there are some key issues that can be highlighted.

1. When producing a System, or National Architecture from the European ITS Framework Architecture, it is recommended that a communications analysis is carried out. This should consist of the following simple steps.

   (a) define all of the Physical Data Flows in terms of their constituent Functional Data Flows;

   (b) assign sizes and frequencies to each Data Flow, particularly where they cross physical boundaries;

   (c) from (b) produce an estimate of the required bandwidth;

   (d) identify any operational constraints for each link, e.g. one end of the link is mobile, e.g. in a Vehicle, or high security is needed;

   (e) determine the most suitable communications medium for each link, bearing in mind the results of (c) and (d).

   When carrying out the work in (b) and (c) above, tables should be created to identify the parameters for each link. Chapter 3 in Annex 2 of this Document contains the tables used for the "example Systems" analysed in the previous sections of this Chapter, and they can be used as templates for this work.

   Once the work in (e) has been completed, the next step will be the definition of the interfaces across which each of the Data Flows will pass. It is recommended that the work in Chapters 7 and 8 of this Document are consulted before the definitions are finalised.

2. It is almost certain that the communications requirements of any System or National Architecture will form an insignificant part of the data being transmitted by any

telecommunications provider (sometimes called a “Telco”). Therefore the interface definitions produced in point 1 above should be take account of what “standards” are already available.

3. As a follow on to point 2, where possible, the aim should be to ensure that the required infrastructures are shared with other users. This will provide economies in the cost of use and maintenance. The main reasons for not doing sharing the infrastructure can be one or more of the following:

   (a) the data exchange is very time critical;

   (b) the data requires a high degree of security that can only be guaranteed by making sure that there is no other data on the physical link;

   (c) the volume of data is such, that a new (or extra) physical link will have to provided anyway.

4. Another important consideration in the producing the definition of communications links as described in point 1, is the availability of communications equipment, e.g. modems, high speed interfaces, etc. It is prudent to check that they can support the required interface definition, and that they are capable of surviving in the location environments at each end of the links.

The above provides a list of the most important points in the definition of communications links. It is therefore not exhaustive, and should be used as a reference. The requirements of particular Systems (or National Architectures) may themselves create other additional points for consideration.

7 Typical Telecommunication links at Physical Interfaces

7.1 Introduction

This Chapter presents the telecommunication links at physical interfaces. This Chapter is based on the analysis in Chapter 6 which has studied some of the “example Systems” presented in the Physical Architecture. However this Chapter is not limited to these “Systems” and reflects the conclusions for the whole Physical Architecture.

The next section shows the relationship between “example Systems” and Physical Interfaces. The sections after the table provide a brief overview of the characteristics of each Physical Interface separately.

7.2 Relationship between “example Systems” and Physical Interfaces

7.2.1 Sink / Source couples for the different systems

The following table gives for each category of example systems the list of sink / source couples for which data flows are described in the systems of the European ITS Physical Architecture – see reference 10(c). Each line corresponds to a different type of physical interface. For each couple the number of the system is placed in the column corresponding to the area of the system. Hence, each cell of the table shows in which system, and in which area each interface can be found in the Physical Architecture.

In this table, the following abbreviations have been used:

Cent.:	Central;
EFC:	Electronic Fee Collection Systems;
FFM:	Freight and Fleet Management Systems.
ITM:	Integrated Traffic Management Systems;
LE:	Law Enforcement Systems;
Pers.:	Personal device;
Road:	Roadside;
S&E:	Safety and Emergency Systems;
TM:	Traffic Management Systems;
TRG:	Traffic Assistance and Route Guidance Systems;
V:	Vehicle Systems;
Veh.:	Vehicle;

Table 10 Source/Sink Couples in different Systems

	System Category							
Sink/Source Couple	**ITM**	**EFC**	**S&E**	**TM**	**V**	**TARG**	**LE**	**FFM**
Pers. / Pers.								
Pers. / Kiosk		P10				P60		
Pers./ Cent.		P10						

	System Category							
Sink/Source Couple	**ITM**	**EFC**	**S&E**	**TM**	**V**	**TARG**	**LE**	**FFM**
Pers./ Road.		P10						
Pers./Vehi.						P60		
Kiosk / Kiosk								
Kiosk / Cent.	P1	P10						
Kiosk / Road.								
Kiosk / Vehi.		P11						
Cent. / Cent.	P1, P2	P10, P11						P81
Cent./ Road.	P3	P11		P30, P31				
Cent. / Veh.		P11	P22					
Road. / Road.	P3						P70	
Road. / Veh.		P11		P30				
Veh. / Veh.					P50			

7.3 Link Characteristics

7.3.1 Introduction

The following sections provide an overview description of the main characteristics of the physical interfaces needed for each type of link. In some cases alternatives are given because the adopted solution will depend on installation constraints.

Some terms have been used throughout the following sections. Their definitions are as follows.

Wireless - Any form of radio based communication. It can be a dial-up connection using some form of mobile telephony, or be radio based.

Wireline - Any form of link that uses a physical connection. It may use copper or fibre for the actual connection medium.

7.3.2 Personal Device / Kiosk

This link will need to cover short distances and use wireless technology based connections. Some form of radio technology may be used since it avoids the need for “line of sights” between the ends of the link. The link would enable several Travellers with Personal Devices to access the same Kiosk simultaneously, there by decreasing or removing the waiting time for Travellers. It could also make the use of Kiosks safer and enable Travellers to use them from passing Vehicles. The main constraints will be the speed with which the Traveller passes within range of the Kiosk and the potential need to implement frequency re-use. Traveller speed will depend on whether the a vehicle is being used. If so then the vehicle speed will dictate the time available for data transfer and will thus effect the choice of transmission rate. Use of a common frequency for all Kiosks would reduce the complexity of the communications equipment required in the Personal Device.

7.3.3 Personal Device / Central

This link will need to cover long distances and use wireless connections. It will enable Travellers to "roam" and to obtain access to services from where ever they are currently located. Services using mobile telephone technology are starting to appear, although the cost of their use may be a barrier to all but business users. Therefore in order to maximise the take-up of services in the short term, it will be necessary to offer a wireline connection. This should use a dial-up link and be available from fixed points, such as public telephones.

7.3.4 Personal Device / Roadside

This link will need to cover short distances and have the same characteristics as the Personal Device/Kiosk link discussed in a previous section.

7.3.5 Personal Device / Vehicle

This link will enable Travellers to use services whilst they are in Vehicles. It should be provided in two ways. For Public Transport Vehicles, it should be through a very short range link using wireless technology. This should operate inside the vehicle and should not be available to others standing outside. For other Vehicles such as private cars and taxis, the link should be available through some type of physical connection such as a plug. This would also enable Drivers to use their Personal Devices to deliver services through in-car interfaces and may avoid the need to provide dedicated in-car equipment.

7.3.6 Kiosk / Kiosk

This type of link is not required by any of the "example Systems" currently in the Physical Architecture. It would probably need some form of wireline connection if it were ever needed.

7.3.7 Kiosk / Central

This link will enable Kiosks to use centrally based systems to support the provision of some services to Travellers. It will be made in one of two ways. Firstly, in so called "difficult" locations, e.g. rural areas, wireless type links will have to be used. This will be because there is no other form of communications infrastructure in these areas. In some cases the traditional "mobile telephone" type of service may not be available, in which case the links will have to use some other type of communication, such as micro-wave. In urban areas where infrastructures are more likely to exist, wireless or wireline type links can be used. With the increasing availability of mobile telephone infrastructures the need to use wireline links may disappear. This may be aided by the fact that the use of the link may be intermittent, depending on the numbers of Travellers using the Kiosks and the nature of the services that they require.

7.3.8 Kiosk / Roadside

This type of link is not required by any of the “example Systems” currently in the Physical Architecture. It would probably need some form of wireline connection if it were ever needed.

7.3.9 Kiosk / Vehicle

This type of link will use wireless based technology so that Vehicles can communicate with the Kiosks as they pass by. The range of the link will probably be short, e.g. < 100 metres. Many of its other characteristics will be similar to those of the Personal Device/Kiosk link discussed in an earlier section. The main constraints will be similar to those of that link, i.e. the speed of the vehicle and the potential need to implement frequency re-use. Vehicle speed will dictate the time available for data transfer and will thus effect the choice of transmission rate. Use of a common frequency for all roadside devices would reduce the complexity of the communications equipment required on-board the vehicle.

7.3.10 Central / Central

This type of link will be made using wireline technology and be used to link adjacent Control Centres, or distributed equipment for a single Control Centre. It will have to be capable of operating over short to medium distances (e.g. < 100 km) and at high speed. In some cases it may be possible to use existing infrastructures and services, but this will depend upon the type of data being transferred, the volume of data and the frequency of transfer. Long distance capability will not be needed since there may be little value in exchanging data between Control Centres that are so far apart.

7.3.11 Central / Roadside

This link will enable Roadside equipment to be controlled by, and/or supply data to, the “Central” part(s) of systems. It will be made in one of two ways. In so called “difficult” locations, e.g. rural areas, wireless type links will have to be used. This will be because there is no other form of communications infrastructure in these areas. In some cases the traditional “mobile telephone” type of service may not be available, in which case the links will have to use some other type of communication, such as micro-wave. Another reason for not using “mobile telephone” services may be the high speed, volume and frequency of the data being transmitted. Elsewhere, particularly in urban areas and other places where communications infrastructures exist, wireline rather than wireless type links can be used. The choice will depend on the type of data, its volume and frequency of transmission.

7.3.12 Central / Vehicle

This type of link will use wireless technology to enable vehicles to “roam” over the road network. It may include both voice and data channels in order to facilitate direct communication with the vehicle driver. Other forms of link such as beacons could be used where they can be readily (and cheaply) supported by an infrastructure. However it will depend on the services being supported by the data that is being exchanged and the need for “instant” communications, i.e. does it matter if there is a time delay (possibly many minutes) before the vehicle passes a beacon and is able to send and receive data.

7.3.13 Roadside / Roadside

This type of link will be made in one of two ways. The first way will be to use wireline links, especially where an infrastructure is already available and easily accessible. This is most likely to be in urban areas. The other way of making the link will be using some form of wireless communications. In many cases the link will be from one particular Roadside unit to another (point to point) so that communications technologies such as infra-red and micro-wave can be used. However many links will use radio based technologies if they are available as they can be easier to use and can be the responsibility of on organisation other than the service provider.

7.3.14 Roadside / Vehicle

This type of link will use wireless based technology so that Vehicles can communicate with the Roadside equipment as they pass by. The range of the link will probably be short, e.g. < 100 metres. Many of its other characteristics will be similar to those of the Kiosk/Vehicle and Personal Device/Kiosk links discussed in earlier sections. As with the Kiosk/Vehicle link, the main constraints will be the speed of the vehicle and the potential need to implement frequency re-use. Vehicle speed will dictate the time available for data transfer and will thus effect the choice of transmission rate. Use of a common frequency for all roadside devices would reduce the complexity of the communications equipment required on-board the vehicle.

7.3.15 Vehicle / Vehicle

This type of link will need to use short range wireless technology. The main factors in this choice are the mobility constraints of the vehicle to vehicle environment and the potential need to implement frequency re-use. Depending on the access method, this may be required to increase the number of communications channels and avoid interference problems. Research is currently being conducted on the vehicle-to vehicle communications link for many varying applications using either radio frequency (RF) or infra red technologies. The RF systems developed so for have used an RF link that operates at different frequencies throughout the RF spectrum, although in Europe, CEPT have (provisionally?) allocated the frequency band 63 -64 GHz for future vehicular systems such as vehicle-to-vehicle communications.

There are many types of systems currently under research from RF spread spectrum systems to infra red systems. Due to the highly dynamic nature in which vehicle-to-vehicle communications system must operate and the different applications for which this link will be used, there are many potential research problems that need to be overcome. The potential problems include interference issues, security, data reliability, frequency re-use, processing time, to name but a few examples. Since the technology required to implement vehicle-to-vehicle communications is still under development, there has as yet been no move to develop standards for this technology. It is impossible therefore to predict the exact technologies which will be used to implement vehicle- to-vehicle communications systems.

7.4 Message Sets and Data Communications Protocols

7.4.1 Introduction

This section covers points that are common to many if not all of the communication links described in the preceding sections of this Chapter. It is therefore not considered appropriate to highlight them under one, or very type of links to which they are relevant. These points cover attributes of communications such as the use of standards, common data, data communications across time zones.

7.4.2 Use of standards for messages and protocols

In all cases, the Telecommunications Links described in the previous sections should be made using a defined group of message sets and/or data communications protocols. Rather than providing a new “custom” definition for each application, it is **very strongly recommended** that existing standard definitions are used. It is incumbent upon system purchasers, designers and manufacturers to pursue this policy with great vigour, as it is all too easy to decide that a “custom” definition is the only solution.

Using a standard definition for the message sets and/or the data communications protocols should provide at least the following two benefits:

1. the actual time taken to produce the definitions will be shorter;
2. products using the standard definitions should already be available from manufacturers.

Depending on the type of physical communication link that is required, there may be a number of standards that are already available. Examples are TCP/IP and DATEX, information about which can be obtained from National Standards organisations, e.g. NNI, BSI, etc.

If a “custom” definition has to be provided for the message sets and/or data communications protocols, then as far as possible it should be based on existing standards. An important feature of any “custom” definition must be that there is a clear distinction made between what is data and what is needed to define the communications protocol. It is **very important** that the two are not combined or mixed, especially when a “standard” definition is being used as the source for the “custom” definition. Once the “custom” definition has been completed, it should be promoted as a new standard with CEN through the appropriate national standards organisation.

7.4.3 Common Data Items

There will be several items of data that will be included in several (or all) of the messages sent across the various types of communications links described in the previous sections in this Chapter. Examples of the most obvious data items that are likely to be common include: date, time and location. There are also some less obvious data items which could include:

time zone: Europe has at least two time zones, and travel information (particularly for other modes, e.g. rail, air etc.) may have to include travel outside of Europe;

day number: the number of the day in the week, e.g. Monday = 1, Tuesday = 2, through to Sunday = 7;

road traffic flow: the volume of vehicles flowing along a single carriageway;

road occupancy: the percentage of time for which road traffic has occupied a part of a single carriageway;

car park occupancy: number of spaces that are available in a car park.

When specifying the communications links as part of a System design, or as part of a National Architecture development programme, efforts should be made to use a “standard” data definition for all common data items. This will make the understanding of the data itself much easier. The definitions of these items should cover not only the way that the data is presented, but also the size of the data elements themselves.

Rather than “invent” a new “standard”, the results of work already undertaken in this area should be consulted. In the first instance, organisations such as CEN (for Europe) and ISO (for the whole World) must be consulted. If actual standards are required, these can usually be obtained from the local National standards organisation. Alternatively the work of individual European projects can be consulted. One example is the DATEX Project whose task has been to create European standards for data exchange between Control Centres. There have also been other European projects that have concentrated on specific areas. Examples are COMETA (Freight and Fleet Management from the Vehicle) and EUROBUS/TRANSMODEL (Public Transport Management).

7.4.4 Data Units

Another issue concerning data definitions is the use of the most appropriate units. At the moment in Europe, there are two units for measuring speed and distance. Any message exchanging this data must include a specification of the units that are being used. The same is also true of time, for which there are two zones currently being used within Europe.

Again rather than inventing something new, it is recommended that the local National standards organisations are consulted. The European projects identified in the previous section have also been active in the field, and again it is recommended that their work is used as a source of reference.

8 Typical communication links at the interface with Terminators

8.1 Introduction

This Chapter presents the telecommunication links between Systems and Terminators. The section below is based on the analysis of Chapter 6, which studies the systems presented in the Physical Architecture, but this Chapter is not limited to these systems and reflects the situation all known systems in the framework of architectures considered by the KAREN Project.

The next section categorises the different Terminators according to the nature of their links with the systems. The following sections lists all the physical interfaces between systems studied in the Physical Architecture and the Terminators.

8.2 Terminators and Systems

The European ITS Physical Architecture – see reference 10(c), provides a list of external systems (terminators) with which the different example systems exchange data flows. This list consists of the following entities:

- Ambient Environment,
- Bridge / Tunnel Infrastructure
- Consignor / Consignee
- Driver,
- Emergency systems,
- External Service Provider,
- Financial Clearinghouse,
- Freight Equipment
- Law Enforcement Agency,
- Location Data Source,
- Maintenance Organisation,
- Multi-modal system,
- Operator,
- Related Road System,
- Road Pavement,
- Traffic,
- Transport Planner,
- Traveller,
- Vehicle,
- Weather Systems.

Each "example System" exchanges data and/or information with some (not all) of these terminators. The communication requirements related to the interface with these Terminators therefore have been defined. However, for some of these terminators, the data flows do not represent a transfer of information via telecommunication means. Instead they use a physical link either to and/or from, the Systems. For example the colour light of the traffic signal is the final link in the flow of data from a Traffic Management System to a Driver. Another example is the simple Human-Machine Interface (HMI) between a Traveller and an information Kiosk.

The different terminators can be divided into three categories. They are as follows:

- those requiring to exchange data with the System using electronic means;

- those whose state the System either detects or controls through an interface;
- those that have links with Humans.

The following table shows the allocation of terminators among these three categories. Note that some may belong to several categories. For example, the Traveller is concerned with physical links when they are on the pavement waiting for the traffic light to turn to green. However they will be concerned with HMI when they consult a Kiosk for travel information, and be involved with communication links when they use a PC to get information on bus schedule.

Table 11 Categorisation of links with Terminators

Terminator	Type of link		
	Communication	Physical	HMI
Ambient Environment (ae)		X	
Bridge/Tunnel Infrastructure (bti)		X	
Consignor / Consignee (cc)	X		
Driver (d)		X	X
Emergency Systems (es)	X		
External Service Provider (esp)	X		
Financial Clearinghouse (fc)	X		
Freight Equipment	X		
Law Enforcement Agency (lea)	X		
Location Data Source (lds)	X		
Maintenance Organisation (mo)	X		
Multi-modal System (mms)	X		
Operator (o)		X	
Related Road System (rrs)	X		
Road Pavement (rp)		X	
Traffic (trfc)		X	
Transport Planner (tp)	X		
Traveller (t)	X	X	X
Vehicle (v)		X	
Weather Systems (ws)	X		

8.3 List of terminators interfaced with the different systems

The table on the following page shows for each Terminator the “example System” (or Systems) presented in the European ITS Physical Architecture – see reference 10(c), with which it has an interface. The cells in the table are filled with a "I" (Input) when the Terminator sends data to the System and with an "O'" (Output) when the Terminator receives data from the System. An "I/O" signifies that both occur, although this is not necessarily a simultaneous exchange of data.

Table 12 Dataflows between Systems and Terminators

Terminator Name	**“example System” number**												
	P1	**P2**	**P3**	**P4**	**P10**	**P11**	**P22**	**P30**	**P31**	**P50**	**P60**	**P70**	**P81**
Ambient Environment (ae)	I						I						
Bridge/Tunnel Infrastructure (bti)	I/O						I/O						
Consignor / Consignee (cc)							I/O						I/O
Driver (d)			O		I/O		O	O	O	I/O	I/O	O	I/O
Emergency Systems (es)	I/O						I/O	I	I	I/O		O	
External Service Provider (esp)		O			I/O		I/O	O		I/O	I/O		
Financial Clearinghouse (fc)					I/O	I/O					I/O	O	
Freight Equipment													
Law Enforcement Agency (lea)							I/O	I/O	I/O			I/O	I/O
Location Data Source (lds)		I					I			I	I		I
Maintenance Organisation (mo)							I/O	I/O	I/O	I/O		I/O	
Multi-modal System (mms)	I/O						I/O	I/O	I/O				I/O
Operator (o)	I	I/O	I/O		I/O	I/O	I/O	I/O	I/O		I/O	O	I/O
Related Road System (rrs)	I/O	I	I/O				I/O	I/O	I/O	I/O	I/O	I/O	
Road Pavement (rp)							I	I	I	I			
Traffic (trfc)			I				I	I	I	I/O		I	
Transport Planner (tp)							I/O	I/O	I/O				
Traveller (t)	I/O		I/O		I/O	I/O		I/O	I/O		I/O		
Vehicle (v)					I	I	I/O	I		I/O		I	I
Weather Systems (ws)	I						I	I					

8.4 Consideration of Link characteristics by Type

8.4.1 Introduction

As noted in a previous section the terminators can be divided into three categories according to the type of Link that they will use for their connection to the System. The three categories of terminator and the types of link that have to be provided for each one are as follows:

- those requiring to exchange data with the System using electronic means (Telecommunication Links);
- those whose state the System either detects or controls through an interface (Physical Links);
- those that have links with Humans (HMI Link).

The rest of this section will consider the characteristics of each of these three types of terminator in turn. The type of technology used to provide each Link and the actual communications devices at each end of the Link will be ignored, except in the case of HMI type Links. The reasons for this will be explained in the section about that type of Link.

8.4.2 Terminators using Telecommunication Links

For the purposes of this analysis, a Telecommunications Link is defined as one that is used to transfer data by electronic means. Both ends of the Link will be provided by electronic devices that will either send or receive the data. There are several terminators with Links of this type, and they are as follows:

- Bridge/Tunnel Infrastructure
- Consignor / Consignee
- Emergency Systems
- External Service Provider
- Financial Clearinghouse
- Freight Equipment
- Law Enforcement Agency
- Location Data Source
- Maintenance Organisation
- Multi-modal System
- Related Road System
- Transport Planner
- Traveller
- Weather Systems

An analysis of the characteristics of the links to the above terminators is shown in the following table. It has been assumed that for each of the terminators, the System end of the link will be connected to some type of computing resource. This resource will be that which is used to provide the services that are available from the System.

Table 13 Terminator Telecommuications Links Characteristics

Terminator Name	Terminator Computer Resource	Typical Frequency	Typical Size	Typical Other	Comments
Bridge/Tunnel Infrastructure	Small System	Periodic but extra for "incidents"	<50Kbytes	High Speed for extra messages.	Provides atmospheric conditions on bridges and inside tunnels. May also warn of emergency situations that are "possible incidents".
Consignor / Consignee	Small System (PC)	Intermittent	<1Mbyte		Freight shipping data and updates.
Emergency Systems	Resilient System	Intermittent	<50KBytes	High Speed High Security	Emergency System input will request Emergency Vehicle route(s) and will be small (<50Bytes).
External Service Provider	Small system, e.g. PC	Intermittent	<1Mbyte		Information Requests and/or details of future events that are to be treated as "possible incidents".
Financial Clearinghouse	Resilient System	Variable, very high during peak travel times	<50KBytes	High Security	
Freight Equipment	Resilient System for use in hostile environments	Intermittent	<50KBytes	High Speed High Security	Freight Equipment location and contents, as and when either of them change.
Law Enforcement Agency	Resilient System	Intermittent	<1Mbyte	High Speed High Security	High size for digital images of offenders.
Location Data Source	Resilient System	Continuous			Data used to determine receiver's location.
Maintenance Organisation	Small system, e.g. PC	Intermittent	<50Kbytes		Details of equipment faults and clearance.

Terminator Name	Terminator Computer Resource	Typical Frequency	Typical Size	Typical Other	Comments
Multi-modal System	Resilient System	Intermittent	<50Kbytes	High Speed (crossings)	Used to control use of road/other mode crossings and to provide trip planning information.
Related Road System	Similar System	Periodic - ≤4/hour	<1MByte		Exchange of data with a System that is similar to the System being considered.
Transport Planner	Small system, e.g. PC	Intermittent	<500KBytes		Output - travel data for analysis. Input – new strategies or static data.
Traveller	Small system, e.g. PC	Intermittent	<50KBytes		Requests and provides travel and/or trip planning information.
Weather Systems	Resilient System	Periodic - ≤4/day	<500KBytes		Provides weather information for "possible incidents", Traveller trip requests, etc.

8.4.3 Terminators using Physical Links

For the purposes of this analysis, a Physical Link is one that has a physical object at one of its ends. This will always be the end that is outside the System, i.e. at the terminator. Inside the System there will be sensors that are capable of detecting the state of the physical object, or providing it with output. The input sensors will convert the state of the object into a digital electronic representation, that can be used by other parts of the System. The terminators with Links of this type are as follows:

- Ambient Environment
- Bridge / Tunnel Infrastructure
- Driver
- Road Pavement
- Traffic
- Traveller
- Vehicle

An analysis of the characteristics of the Links to each of the above terminators is shown below. Again it has been assumed that for each terminator, the System end of the link will be connected to some type of computing resource. This resource will be that which is used to provide the services that are available from the System.

- Ambient Environment
  Inputs: Detection of atmospheric pollution levels, particularly those concerned with transport, e.g. carbon monoxide, nitrous oxide, carbon dioxide, hydrocarbons and particulates, plus weather conditions, e.g. temperature, humidity, fog, rainfall, ice, wind speed/direction.

- Bridge / Tunnel Infrastructure
  Input: Detection of conditions in side tunnels or on bridges, e.g. temperature, fog, rainfall, ice, wind speed/direction, fire, flooding. Note that this data may also be provided by specialist systems – see section on Telecommunications Links.

- Driver
  Output: Display of visual indications to Drivers such as, traffic lights and signs of various types, e.g. static (fixed), electronic (led for variable message), mechanical (rotating plank for fixed message and flip dot, both variable and fixed message). All display must be clearly visible in all ambient lighting conditions, including direct sunlight and with the sun behind the display. Sign texts must be unambiguous, even for those with no native language skills.

- Road Pavement
  Input: Detection of road pavement conditions such as presence of ice and flooding. In the future it may be possible to detect wear and tear and general deterioration of the road surface.

- Traffic
  Input: Detection of the presence of Vehicles using one of a variety of images such as, magnetic, or infra-red, or visual, or through particular forms of detection such as micro-wave and on-board Vehicle units. The on-board units may also be used for special vehicle detection (Public Transport and Emergency Vehicles). Other forms of detection may also be used, such as pressure pads for Vehicle axle weight detection.

- Traveller
  Input: Detection of Travellers who are currently Pedestrians and wishing to cross a road, or are Public Transport Passengers and waiting for a service to arrive at a stop. The detection may be through video, or infra-red image analysis, or the use of micro-wave detection units, or manual input. All methods must be able to detect and/or accept inputs from those that are Elderly or Disabled. The devices for manual inputs must therefore be accessible to those in wheelchairs. Alternative forms of input must be found for those who are blind. At Public Transport stops, it may be necessary for any detection units to pass on details of any disabilities that the Traveller has to the approaching Vehicle.
  Output: Display of visual and audible indications to Travellers who are currently pedestrians that it is safe to cross a road, or that a Public Transport Vehicle is ready for passenger boarding. The visual indicators may take the form of static signs that are illuminated when needed, or variable text signs. It should also be possible for the variable text signs to be used to display more general travel information. All forms of indication should be accessible to those that are Disabled, so that for example, both visual and audible indications are provided simultaneously. Visible indications

must be clearly seen under all ambient lighting conditions, including direct sunlight and with the sun behind the display.

- Vehicle
  Input: Detection of Vehicle state and of things outside the Vehicle. This will include such things as attitude, speed, headway, lane location, nearby objects and the field of view seen by the Driver. The field of view may be detected using infra-red sensors and used to supplement the visual image currently available to the Driver.

8.4.4 Terminators using Links with Human Machine Interfaces

For the purposes of this analysis, a Link that uses a Human Machine Interface (HMI) is one that has an electronic device with which Humans can interface, at one of its ends. This will always be the end that is outside the System, i.e. at the terminator. Thus it enables Humans to either receive information from the System, or to both receive and provided information from and to the System. The terminators with Links of this type are as follows:

- Driver
- Operator
- Traveller

An analysis of the characteristics of the links to these three terminators is shown in the following table. Again it has been assumed that for each terminator, the System end of the link will be connected to some type of computing resource. This resource will be that which is used to provide the services that are available from the System.

The characteristics of Links to the Traveller have only been assessed for inputs and outputs using Kiosk based displays. However services are also expected to be provided to Travellers through Home PC’s or Travel Agents.

Services through Home PC’s should be provided by facilities already available from the PC itself and there should be no need for anything extra, other than Multi-language capability. The PC should have already been modified to include the provision of facilities for the Elderly or Disabled as it is expected that it will be used to provide other (non-ITS) services to the same users. The only “special” facilities that may be needed by some ITS services will be the display (and printing) of coloured images such as maps and guidance notes.

Services through Travel Agents should be provided to meet the same requirements as those shown in the table for the Operator. It is assumed that the “Operator” will in this case be a member of the Travel Agent’s staff and will therefore receive the appropriate training in the use of the facilities that provide the ITS service. It has been assumed that the “Operator” will be responsible for interfacing with the Traveller and that therefore the Traveller will not have to use the facilities themselves.

Table 14 Terminator HMI Links Characteristics

	Driver	Operator	Traveller
General	Common symbols should be used across all vehicle makes/models. Multi-language interface needed.		Common symbols and interface layout should be use for all Kiosks. Multi-language interface needed.
Input (General)	Audio/Manual. No special training required for use. Minimum distraction from driving task	Audio/Manual. Training may be needed for use. Manual – simple "click and pointing" device.	Audio/Manual. No special training required for use. Manual – simple "click and pointing" device.
Input (Elderly)	Bigger manual input devices and adjustable microphone volume.	N/A	Bigger manual input devices and adjustable microphone volume.
Input (Disabled)	Special input facilities plus adjustable microphone volume and position.	Special input devices with wheelchair access plus adjustable microphone volume and position.	Special input devices with wheelchair access plus adjustable microphone volume and position.
Output (General)	Audio/Visual Minimum distraction from driving task. No special training required for understanding of outputs. Audio must be different from others in vehicle	Colour with map based and large display options. Capable of integration with other displays. Training may be needed for understanding of outputs. Supplementary audio output.	Audio/Visual. Colour with map, picture and symbol based displays, plus not affected by changes in ambient light in Kiosks. No special training required for understanding of outputs. Audio at Kiosks must not reach outside to "passers by".
Output (Elderly)	Adjustable speaker volume.	N/A	Adjustable speaker volume.
Output (Disabled)	Adjustable speaker volume.	Adjustable speaker volume. Moveable display to enable wheelchair access.	Adjustable speaker volume. Moveable display to enable wheelchair access.

8.4.5 Development of a "Presentation Architecture"

When Systems for larger applications are being considered, there is a need to look more closely at the HMI standards that will be used. Examples of these "larger" Systems are those for State (County or Province), National, or International applications. In order to produce the standards, there will be a need to identify the System functionality that will support the HMI, in its different forms. The results of this identification and standardisation process can be called a “Presentation Architecture”.

A “Presentation Architecture” will thus define all the HMI of each type, and the standards with which each type must comply. In the following Tables, examples of the definition of two “Architectures” are shown.

The first definition covers the Operator Interface for a System containing facilities for the management of traffic using both urban and inter-urban road networks. The System includes emergency, incident, demand and maintenance management, plus environmental conditions monitoring.

Table 15 Example of Presentation Architecture for Operator Interfaces

Function	Function Name	Characteristics
2.1.4	Provide Emergency Control to the Operator	Platform: MS Windows Presentation: Window Date/Time: Yes Text Font: Arial Bold allowed: Yes Output Text: Blue Background: Yellow Input text: Red Audio Alarm: Yes Visible Alarm: Yes Alarm Status: Overwrite Inputs: kbd, mouse, audio Other: smart key Help: Context Driven
3.1.1.5.7	Provide Operator Urban Traffic Control Facilities	
3.1.2.5.7	Provide Operator Inter-urban Traffic Control Facilities	
3.1.3.3	Provide Bridge and Tunnel Operator Interface	
3.2.5	Provide Incident Management Operator Interface	
3.3.5	Provide Demand Management Operator Interface	
3.4.5	Provide Environmental Conditions Operator Interface	
3.5.5	Provide Operator Maintenance Operations Interface	

Systems that do not have all of the above facilities would remove some of the Operator interfaces shown in the two left-hand columns. The details in the right-hand column can be used in the specification for the Operator interfaces of any new facilities that are added to the System.

The second example of the definition of a “Presentation Architecture” (shown in the Table on the next page) is for the Traveller interface at Kiosks. It is assumed that the Kiosks will be situated in Germany, or a county where German is the natural language. The interface has to be more comprehensive and robust as the device is not in a controlled environment and is for use by a variety of people. Some of these people may not be “computer literate” and therefore the interface must cover their needs and expectations.

Table 16 Example of Presentation Architecture for Traveller Interface at Kiosks

Function	Function Name	Characteristics
6.1	Define Traveller's GTP	Platform: Windows NT Presentation: Full Screen Date/Time: Yes Text Font: Arial Bold allowed: Yes All Text: Black Background: Grey Audio Output: Yes Audio Input: Yes Input Conf: Yes Printed Output: Yes Help: Context Driven All Weathers: Yes Tamper Proof: Yes E/D facilities: Yes Foreign Lang: Yes (F/En)
6.2.1	Define Traveller's ATP	
6.2.2	Define Prime Criteria	
6.2.3	Propose Trip Alternatives	
6.2.4	Select and Define Bookings	
6.2.7	Produce Itinerary and Trip File	

The work to define the “Presentation Architecture” should be completed as part of the creation of the Physical Architecture for the System itself. It would thus be included in the steps to create this type of Architecture that are described in Chapter 3 of the European ITS Physical Architecture Deliverable Document (D 3.2) – see reference 10(c).

8.5 Conclusion

The characteristics of the Links between the System and its terminators need to be carefully analysed for each implementation. When specifying the HMI, special attention must be paid to the needs of the Elderly and the Disabled where their capabilities may be different to those available from other human beings. Note that in some cases special provision may also have to made for parents whose children are in push-chairs, buggies, or prams.

9 Information Exchange Standards

9.1 Introduction

Various means of communication are available for the design of different ITS applications. The content of the data exchanged on the network involved in a given System is only relevant for that System. There are three reasons why it will be necessary to have a common definition of the data transmitted across the different systems and subsystems. They are:

(1) to enable a wider use of an ITS architecture framework;

(2) to obtain cost reduction by the mass market effect;

(3) to allow systems from different countries to offer interoperable services to their users.

Therefore, in the ITS area, a certain number of information exchange standards already exist to facilitate the interoperability of such equipment. The main major standards defined in Europe in the ITS field are DATEX, RDS-TMC, TPEG and EFC applications based upon DSRC.

9.2 DATEX

A major emphasis in TAP-T (Telematics Application Programme for Transport) and other European programmes has been the need to set up effective arrangements for the exchange of information between Traffic Information Centres (TIC's), particularly across National borders. There are currently some sixty TIC's across Europe implementing this technology. In addition to these centres, many countries have national data exchange plans, involving DATEX, that will link road administrations, road operators, information centres, the Police and broadcasters.

DATEX is an EC led initiative, formed during the DRIVE 2 EC research and development programme on Advanced Transport Telematics. It has played a major role in creating European standards for traffic information and data exchange. The associated data dictionary of terms is used widely in database development.

The DATEX-GO study was aimed at strengthening the work undertaken on communication exchanges between Traffic Information and Control Centres across Europe. This resulted in a new European standard covering road traffic exchanges and greater co-operation with initiatives in both the US and Japan. The scope of data which can currently be exchanged includes traffic measurement data, such as speed and flow, traffic incidents and events and weather data, suggested diversion routes, traffic equipment status, public transport delays and cancellations and parking availability.

The standards concerning DATEX are developed by the CEN Technical Committee 278, Working Group 8. The following table provide the list of the standards already adopted by the CEN and the items on which the TC 278 / WG8 is working at the present time.

Table 17 DATEX-Net standards

Document	Title	Status
ENV 13106-1:1998	Traffic and travel data dictionary - Part 1: General definitions, entities, attributes	Adopted
prENV 13106	DATEX traffic and travel data dictionary (version 3.1.a) (review of ENV 13106-1:1998)	Adopted
prENV 13777	DATEX specifications for data exchange between traffic and travel information centres (version 1.2.a)	Adopted
	Road traffic data - Elaboration, storage, distribution - Exchange formats (low level)	Under development
	Road traffic data - Elaboration, storage, distribution - Physical interfaces	Under development

The comments by the national standards bodies on these standards divide into those that can readily be incorporated (short term) and those that would require a major revision (long term). The long term comments largely request additional functionality and the use of another data representation (ASN.1).

The latest official release of the DATEX-Net Specifications is Version 1.2a and the latest release of the DATEX Data Dictionary is Version 3.1a.

The full set of documents have been designed to provide instructions and assistance to system developers wishing to develop DATEX-Net compatible traffic and travel information exchange systems. The DATEX-Net Specifications provide a detailed methodology for the implementation of UN EDIFACT based messages, using data defined in DATEX Data Dictionary, and utilising message management guidelines provided within the Specifications.

Such a standard should remain compatible with the Memorandum of Understanding signed by 16 authorities from 13 European countries which commits them to using DATEX until 1st January 2002.

CEN has a close co-operation with ISO on this domain. WG8 works closely with ISO Technical Committee 204, Working Group 9 to develop a standard that will meet the long term requirements of all. The ISO committee has based its work on the European DATEX, but, whereas DATEX is really aimed a point-to-point cross-border communication between traffic control centres, the ISO standard is structured for increased functionality for the future. The ISO standard is likely to be based on ASN.1 rather than EDIFACT and thus the standards would be incompatible.

DATEX is a major element to enable the different TICS across Europe to work in a co-operative mode by exchanging data. The dictionary defined by DATEX is a solution to overcome problems presented by different languages in Europe.

An application of DATEX to exchange data is the use of it for the transmission of data between traffic centre and TMC providers.

9.3 RDS-TMC

RDS-TMC (Radio Data System - Traffic Message Channel) provides continually available traffic information using the RDS radio technique. RDS is a radio technique whereby inaudible information is transmitted alongside a normal radio programme. The information transmitted in RDS is divided into a number of groups, one of these groups is reserved for TMC.

The objective of TMC is to provide continuous and interoperable traffic information which, in conjunction with various functionalities (for example ALERT), can be targeted at specific areas or regions. This can be an area as small as a city conurbation or can cover the main transit roads of a complete region (for example the European Union).

The advantage of the system is that drivers can receive up-to-the-minute traffic information in their own language regardless of the country in which they are travelling. The inaudible RDS digital information is decoded in the user's receiver and presented to the user in either audio or visual form. Potential refinements to the system include the facility for drivers to filter information according to their own itinerary.

Message codes

Traffic Message Channel (TMC) information is conveyed using a “virtual” language, in which the transmitted codes comprise addresses of information stored in decoder databases. These databases contain lists of:

- Weather and traffic situations;
- Advice;
- Duration and other information;
- Locations.

Standard TMC-user messages provide the following five basic items of explicit broadcast information:

- Event description;
- Location;
- Direction and extent;
- Duration;
- Diversion advice.

Protocols

The RDS-TMC traffic message coding protocol comprises two standards, the Alert-C protocol and the Alert Plus protocol.

The Alert-C protocol is used to transmit event-related messages while the Alert Plus protocol allows the transmission of status-orientated messages.

To cater for these two standards, two Application Identifiers (AID) have been assigned within the Open Data Application (ODA). The first AID allows the implementation of the Alert-C service only, while the second AID allows for the implementation of both services (Alert-C and Alert Plus). As the Alert-C with Alert Plus protocol is exactly the same as the pure Alert-C protocol, both AIDs are compatible. This allows a service provider to use either or both AIDs at will, with selection of the required service being made by the user's receiver.

The RDS-TMC is a typical example of the use of data exchange standards to enable the creation of new ITS services for the mass market. The existence of standards allows the manufacturers to produce the same products for the whole of Europe. For the end users, the existence of RDS-TMC permits the drivers to access traffic data when travelling outside their own country. RDS-TMC overcomes language problems by encoding the different events independently of the language.

9.4 TPEG

In recent times the profile of data service provision has increased, with European Commission support for the development of technology to achieve pan-European TTI data services with language independence. The development of RDS-TMC has been the result.

Throughout Europe, there are now a number of RDS-TMC implementations – many are funded by various EC sources. The largest implementations are intended to give coverage over the strategically important Trans European Road Network, with its complex interfaces between cultures, countries, languages and road conventions.

The European Broadcasting Union (EBU), having recognised these developments, now seeks to develop a bearer independent TTI delivery technology which builds on the infrastructures, but which will be more flexible. The technology envisaged is one for a near universal protocol. This is important, both from an end-user viewpoint and from a Service Provider’s need to deliver services via one or more delivery technologies as the multimedia age develops.

As a result in 1997 the EBU established, through its normal procedures, the B/TPEG Project Group, TPEG stand for Transport Protocol Experts Group. The target of this Project Group is to develop a new protocol for Traffic and Travel Information, for use in the multimedia broadcasting environment. B/TPEG will develop applications, service and transport features which will enable travel-related messages to be coded, decoded, filtered and understood both by humans (visually and/or audibly) and by agent systems.

The TPEG Specifications comprise a number of parts, defining the mechanisms that permit Service Providers to operate services which can use one or more delivery technologies (e.g. DAB, Internet, etc.) from one message generation process. Furthermore, they will allow a range of receiver types to be used simultaneously, ranging from sophisticated agent receivers serving navigation systems, through to simple receivers (perhaps a Personal Digital Assistant plug-in receiver/decoder card) only able to decode ‘top level’ information.

The first priority for the Project Group was to develop an end-user oriented Application for Road Traffic Messages, together with the core protocol, network and services layers. The Road Traffic Messages Application uses a deconstruct of the DATEX Data Dictionary to ensure that much of the prior knowledge regarding RDS-TMC and such services is reflected in this Application.

The TPEG Specifications are being designed to allow an existing Service Provider (e.g. RDS-TMC), to migrate towards the multimedia age by employing the TPEG Specifications to achieve the delivery of several services, yet only undertake a single message generation process, and be able to offer services for significantly different end-user situations. One of the key objectives is to free the end-user from the need to have a location database, on a smart card or CD-ROM, before using a service.

The TPEG Specifications are now being developed by the EBU B/TPEG Project Group and the CEN TC 278 WG 4 Project Group 7 which meet concurrently. It has been agreed that both the EBU and CEN have the same objective. CEN TC 278 WG4 is concerned with the development of standards for telematics in the road traffic and transport sector. The work has been adopted by CEN and ISO as work items within their procedures, with a view to producing a European pre-standard. The TPEG Specifications work will be ongoing during the year 2000.

The B/TPEG Project Group has completed work on the first four key TPEG specifications needed to enable pilot technology trials to go ahead. The following table provides the references of these specifications.

Table 18 TPEG standards

Document	Title
prENV ISO 18234-1	Traffic and Traveller Information (TTI) - TTI via Transport Protocol Experts Group (TPEG) data streams - Part 1: Introduction, Numbering and Versions (INV)
prENV ISO 18234-2	Traffic and Traveller Information (TTI) - TTI via Transport Protocol Experts Group (TPEG) data streams - Part 2: Syntax, Semantics and Framing Structure (SSF)
prENV ISO 18234-3	Traffic and Traveller Information (TTI) - TTI via Transport Protocol Experts Group (TPEG) data streams - Part 3: Service and Network Information (SNI) Application
prENV ISO 18234-4	Traffic and Traveller Information (TTI) - TTI via Transport Protocol Experts Group (TPEG) data streams - Part 4: Road Traffic Message (RTM) Application

TPEG will in the near future provide a more flexible way for the service providers to distribute information to users independently of the media used to access to the service. The availability of the high data rate media like DAB or Internet allow a more rich and flexible protocol than the one used for the RDS-TMC. Therefore one of the major advantage of TPEG is that it will be not require a location database before using the service. The issue related to permanent location database inside the vehicle is how to keep it accurate. This is a major problem on how to update the database for navigation system. TPEG will overcome this problem by the transmission of the location information along with the events information.

9.5 EFC application based upon DSRC

Dedicated Short Range Communications (DSRC) provide a means of communication between vehicles and roadside beacons. Currently used for Electronic Fee Collection (EFC) DSRC can also be used for traffic information, vehicle identification and other services.

The DSRC link is defined according to the OSI layers model. Standards have been established for layer 1,2 and 7. These standards are sufficient for the exchange of data between an on-board unit (OBU) and roadside equipment (RSE). The data transfer will be done according a fully proprietary protocol.

To enable Pan-European use of any OBU, there is a need to define an EFC application that could be supported across Europe by each RSE. This need is covered by a standard ENV ISO 14906. This standard provides specifications for the EFC transaction model, EFC data elements and functions from which an EFC transaction can be built. The EFC transaction model provides a mechanism that allows handling of different versions of EFC transactions and associate contracts.

This standard defines the functions required to build an interoperable EFC transaction. These functions have enough capabilities to cover the user requirements across Europe. The following table provides the functions allowed by the standard.

Table 19 Overview of EFC functions

Action Parameter	Response Parameter	Remarks
GetStampedRq	GetStampedRs	retrieves data with an authenticator from the OBE
SetStampedRq	OCTET STRING	sets data in the OBE, which generates an authenticator
OCTET STRING	OCTET STRING	gets data securely from the OBE
OCTET STRING	OCTET STRING	sets data securely in the OBE
GetInstanceRq	GetInstanceRs	retrieves a number of entries out of an attribute’s multiple instances
SetInstanceRq	n.a.	sets one entry at a specified position in an attribute’s multiple instances
n.a.	OCTET STRING	retrieves a nonce - typically used against replay attacks
OCTET STRING	n.a.	sets a nonce - typically used against replay attacks
ChannelRq	ChannelRs	sets and/or retrieves data from the addressed OBE component (e.g. ICC)
CopyRq	n.a.	Copies data from a source EID to a destination EID

Action Parameter	Response Parameter	Remarks
SetMMIRq	n.a.	invokes an MMI function (e.g. signal Ok via buzzer)
SubRq	n.a.	subtracts the given value to the addressed value
AddRq	n.a	adds the given value to the addressed value
DebitRq	DebitRs	debits purse
CreditRq	CreditRs	credits purse
OCTET STRING	OCTET STRING	OBE echoes received data
Container	Container	future CEN EFC use

Within the context of EFC, the following EFC Attributes or a subset thereof shall be available to perform an EFC transaction:

Table 20 EFC Attributes

AttributeID	Attribute	Length in Octet	Data Group
0	EFC-ContextMark	6	Contract
1	ContractSerialNumber	4	
2	ContractValidity	6	
3	ContractVehicle	variable	
4	ContractAuthenticator	variable	
5	ReceiptServicePart	11	Receipt
6	SessionClass	2	
7	ReceiptServiceSerialNumber	3	
8	ReceiptFinancialPart	variable	
9	ReceiptContract	9	
10	ReceiptOBUId	variable	
11	ReceiptICC-Id	variable	
12	ReceiptText	variable	
13	ReceiptAuthenticator	variable	
14	ReceiptDistance	3	
15	EquipmentOBUId	variable	Equipment
16	EquipmentICC-Id	variable	
17	EquipmentStatus	2	

AttributeID	Attribute	Length in Octet	Data Group
18	DriverCharacteristics	2	Driver
19	PaymentMeans	12	Payment
20	PaymentMeansBalance	3	
21	PaymentMeansUnit	2	
22	PaymentSecurityData	variable	
32-96	ReservedForFutureCENuse		
96-127	ReservedForPrivateUse		

This set of data with a common acceptance of data definition for the purpose of EFC is an efficient tool to enable the creation of interoperable service between different operators.

10 References

(a) European ITS User Needs Deliverable Document, Issue 1, May 2000.

(b) European ITS Framework Architecture Functional Architecture Deliverable Document (D 3.1), Issue 1, August 2000.

(c) European ITS Framework Architecture Physical Architecture Deliverable Document (D 3.2), Issue 1, August 2000.

(d) European ITS Framework Architecture Overview Deliverable Document (D 3.6), Issue 1, August 2000.

(e) European ITS Framework Architecture Deployment Approach and Scenarios, (D 4.2), Issue 1, May 2000.

(f) European ITS Framework Architecture Cost Benefit Study Report (D 3.4), Issue 1, July 2000.

A copy of any of the above Documents can be found on the European ITS Framework Architecture CD-ROM, or at “http://www.trentel.org/transport/frame1.htm” by selecting “Deployment Information” and then “System Architecture”.

Annex 1 Supporting information for Communications Analysis

This Document contains the first Annex to the Main part of European ITS Framework Architecture Deliverable Document D 3.3, which provides a description of the European ITS Communication Architecture. It provides additional and supporting information to the Main Document. This information comprises a list of European ITS User Needs that are concerned with communications, and tables of data that were used to produce some of the results in the Main Document.

Annex 2 Details of ITS related communications technologies

This Document contains the second Annex to the Main part of European ITS Framework Architecture Deliverable Document D 3.3, which provides a description of the European ITS Communication Architecture. It provides additional and supporting information to the Main Document. This information comprises a description of the various technologies being currently used for system communications, an analysis of their main characteristics and a description of the OSI Model.