EUROPEAN COMMISSION
Directorate-General XIII Information Society:
Telecommunications, Markets, Technologies –
Innovation and Exploitation of Research

TRANSPORT TELEMATICS SYSTEM ARCHITECTURE

Constraint analysis, mitigation strategies and recommendations

Telematics Applications Programme

Abstract

During the first phase of the study a ″Constraints Analysis″ for the implementation and the deployment of Intelligent Transport Systems within the European Union was produced. It contained a list of risks that could affect its implementation and deployment. In the second phase of the study the database was completed with the recommended mitigation strategies to handle the higher rated risks in given implementation environments. From these a small number of “high level” overall strategies was initially proposed. A consultation process was undertaken involving European stakeholders to produce a consolidated set of strategies that are presented as “recommendations” in this final RAID report.

Keywords

Architectural Framework, ITS, risk analysis, threats, Transport Telematics, mitigation strategies, scenario.

Project Number:	TAP97/9 Study on System Architecture for Transport Telematics : **Constraints analysis, mitigation strategies and recommendations**
Project Title:	**RAID**
Deliverable Type:	Report

Deliverable Number:	D03 Version 4
Contractual Date of Delivery:	28/02/99
Actual Date of Delivery:	24/05/99
Title of Deliverable:	FINAL REPORT: Constraint analysis, mitigation strategies and recommendations.
Work Package contributing to the Deliverable:	All phases
Nature of the Deliverable:	Public
Authors:	L.Berghout (TNO-Inro); R.Bossom (Siemens Traffic Controls); M.Chevreuil (ISIS); A.Burkert (HB); G.Franco (Mizar), JF Gaillet (ERTICO); B.Pencole (Alcatel Space Industries); HJ.Schulz (HB).

Further information can be obtained from:

European Commission,
DG XIII-B5
Information Society Technologies: Systems and Services for the Citizen
Applications relating to transport and tourism
Wetstraat, 200
BU29 2/20
B-1049-Brussels, Belgium
e-mail: infob5@dg13.cec.be
fax: +32-2-2962391

Table of Contents

Part II

DOCUMENT CONTROL

Report Number	*Issue Date*	*Main characteristics*
D01 Issue 1	19/06/98	First report titled “Constraints Analysis Report”
D01 Issue 2	11/9/98	First report revised by including EC comments on issue 1: includes more details on the scenario based approach.
D02 Issue 1	30/09/98	Second report issued as evolution of the first one by completing the constraint analysis with the proposal for mitigation strategies.
D02 Issue 2	18/12/98	Second report revised according the EC comments on the previous version. The structure of the report is also substantially revised.
D03 Issue 1	04/03/99	Third report issued as evolution of the second report including the consolidated mitigation strategies after consultation with stakeholders.
D03 Issue 2	08/04/99	Third report revised according to the EC comments on the previous version
D03 Issue 3	24/05/99	This report

EXECUTIVE SUMMARY

The RAID study on System Architecture focuses on the identification of the threats which can slow down the deployment of a Transport Telematics European Framework Architecture and which are related to the deployment of ITS in general. Threats are clustered and analysed by using a scenario-based approach that facilitates analysis of relationships between the contents of the RAID database and the actual implementation environment. For those threats that were found to be most critical, mitigation strategies are recommended by RAID.

RAID's activities are complementary to those of the KAREN project, as KAREN (Keystone Architecture Required for European Networks) should consider RAID mitigation strategies, along with the user requirements, when defining the KAREN architecture.

This document is the final report produced by the RAID Project consortium and includes the results of all the Project phases.

During the first phase a ″Constraint Analysis″ for the implementation and the deployment of Intelligent Transport Systems (ITS) within the European Union was produced. It contained a set of risks that could arise and affect the implementation and deployment of these Systems. The risks were rated by probability of occurrence and level of impact. In the second phase mitigation strategies were devised for highly rated risks, in given implementation environments. These strategies have been stored on a database together with the risks with which they are associated. Finally, in the third phase, both the identified risks and the proposed strategies were consolidated and discussed with representatives of European ITS stakeholders. Analysis of the resulting mitigation strategies has been approached from different angles, providing a synthesis of the proposed mitigation strategies according to selected Strategy Categories, Basic Scenarios and Strategy Actors.

By combining the major elements of the identified mitigation strategies, a set of twelve high-level strategies have been identified and are summarised below. The strategies are numbered according to the scheme adopted in Section 7 of this document and their order does not correspond to any rating by priority. It should also be pointed out that the defined strategies are complementary and often imply the execution of common or similar actions.

1. The **KAREN Project** must endeavour to ensure that its Framework Architecture includes facilities provided by currently deployed systems. Where this is not practically possible, or does not fit with the KAREN User Needs, the Architecture must clearly show in its deployment plan how it is possible to make systems compatible. The migration strategies that are proposed to achieve compatibility must be easy and cost-effective to implement. A detailed deployment plan including education and continuous training is needed and adoption of KAREN should be encouraged at the National and local levels in order to facilitate the implementation of this strategy.

2. Participation in European and International standards activities must be better organised through the preparation of a strategic plan defined by **European Authorities** in consultation with **Standardisation Groups** and **European Organisations**. Then, according to priorities, actions to further develop harmonisation (both on the technical and on the legal sides) and interoperability should be encouraged in domains such as interfaces between ITS systems, Human-Machine Interfaces (HMI), data exchange, enforcement electronic fee collection and after-theft systems. Support to standardisation activities should be limited to areas where benefits are expected for European manufacturers and users, and support should be reinforced in these cases.

3. **European and National Authorities** must actively encourage the use of a framework to make sure that data is exchanged between different organisations and between neighbouring countries,

as members of a European data exchange network. The quality of exchanged data must be stated by the data provider, and continuity of ITS services across national borders within the Community must be provided to travellers using all modes of transport. To achieve this aim a suitable body of experts with the role of data administrator should be appointed in order to maintain the description of the features necessary for guaranteeing proper data exchange.

4. **Organisations**, such as ERTICO, POLIS, UITP, ACEA at the European level and similar organisations at a national level, should co-operate with **European Authorities** and other actors (e.g. Automobile Associations, Insurance Companies, Industries) in a concerted promotion of the benefits and limits of ITS. Development of this activity should be supported by professionals in communication and training/education and co-ordinated at European level. The aim should be to increase the demand for ITS systems and services, thus reducing their deployment and operational costs.

5. In each European country, the role of Public Authorities and the Private Sector vary enormously. There is a need for **National Governments** and **Local Authorities** to ensure that all Public Authorities are aware that involving the private sector in the provision of ITS services can produce benefits. These include risk sharing plus a reduction in the financial burden that Authorities have to bear. Public Authorities should be encouraged to create strong Partnerships between themselves and the Private Sector. If needed they should also facilitate the creation of partnerships that only involve members of the Private Sector. The European Commission should encourage and facilitate this strategy by developing model agreements and model contract clauses and enlarge the work conducted for traffic information to all relevant ITS services. The precise roles of each of the partners must be defined and agreed on a case by case basis before any partnership is created.

6. Advanced driver assistance systems should be widely implemented in Europe as they can provide more efficient and safer road use. Such systems must be sufficiently reliable and safe to ensure drivers' acceptance and government support. Extension of the work initiated on legal aspects should be supported by **European Authorities** in order to prepare suitable extension of the existing EC directives. In addition to efforts from **Industry**, resources must be provided by **National Governments** and **Local Authorities** to assist with the development of reliable and safe systems and the subsequent operation of large-scale test trials. When these has been completed, resources must also be provided to develop strategies for the installation of any required infrastructure and provide regulations to ensure common standards of safe operation. They must also work with Road Users' associations to promote awareness amongst drivers of the existence and use of these systems.

7. The definition and implementation of demand management technologies must be actively promoted by **National Governments** and **Local Authorities** at different geographical levels (city, regional, national and/or European) and including all relevant transport modes. These technologies should be capable of proposing and implementing strategies to manage travel demand and to enable different transport policies to be pursued. Support for this work must come through the development of sophisticated modelling tools that requires suitable R&D funding from European and National Authorities. These must enable real data to be used to explore the different ways in which demand can be managed across all transport modes in a way that produces benefits and is acceptable to travellers.

8. The development of incident management strategies must be actively promoted by **National Governments** and **Local Authorities** to minimise disruption and reduce the time it takes for those involved in incidents to receive assistance. Sophisticated on-line modelling tools must be developed with suitable funding from **European** and **National Authorities** that enable the

reliance on comprehensive network monitoring, the use of off-line tools and operator intervention to be reduced. These tools must also enable a variety of different scenarios for incident locations and response actions to be explored.

9. **National Governments** and **Local Authorities** must promote with Service Providers and Network Operators the idea that sharing data will increase the size of the market for ITS related products and systems, as well as the patronage of ITS services. This requires steps to be taken in order to establish or extend existing legal frameworks so that the required data is available from certain organisations, such as the Police. Reference models of organisational structures should be developed and promoted **by European Organisations**, based on the best practices . The general exchange of data between providers should be encouraged so that a more comprehensive range of ITS products and services can be provided to more travellers. Promotion of data sharing schemes are also essential to achieve efficient multimodal facilities for travellers and freight.

10. The safeguarding of travellers' personal privacy using ITS is essential and must be actively promoted by **European Commission, National Governments, ITS organisations and automobile, Privacy and Consumer protection associations** amongst Service Providers and Network Operators. The measures that have to be made to ensure a maximum level of privacy for travellers must also be clarified when new ITS services are launched. In parallel with these activities, the social awareness and acceptance of the need to identify movements, whilst preserving privacy, must be actively promoted amongst travellers.

11. Steps must be taken to ensure that road users can move from one geographic area of Europe to another without losing access to ITS services. To achieve this **Private Industry** must develop ITS products that use technologies which enable services to cover more easily all geographic areas (proper actions of **KAREN** and **European Authorities** could facilitate the process by providing guidelines and priorities). In parallel, plans should be established in a concerted manner between **National and Local Authorities** and **Information Service Providers**, in order to prepare smooth evolution towards new technologies and adopt transitory solutions if necessary. This work must make sure that the interfaces enable in-vehicle equipment to be updated as system and vehicle technology evolves with time, and make it possible for more comprehensive system self-testing and fault diagnosis. Co-operation between the communication network providers and Information Providers is also necessary for establishing roaming agreements.

12. **Private Industry** must develop ways of making it easier to deploy the infrastructures needed to support ITS services. This can be achieved in several ways, including a reduction of their capital and operating costs, and the sharing of the infrastructures with other services, some of which may not be ITS related. The work of Private Industry on the use of generic infrastructure and on the sharing of infrastructures must be enhanced through the active promotion by **National** and/or **European Authorities** of its benefits and cost savings.

It is evident that European Authorities and National Authorities are key actors in most of the strategies. This reflects the fact that the initial action generally has to be launched by an authority that bears the strategic view for ITS deployment. In all strategies, however, co-operation between several actors is needed.

1. INTRODUCTION

1.1 Background

Applications in the field of Transport Telematics (TT) in Europe are currently developing very quickly for all mode of transport as a consequence of the proved benefits obtainable, mainly in terms of efficient and safe use of transport networks, for both operators and travellers, and comfort for travellers.

Real systems are already operational in Europe, for example, in the Paris metropolitan region, there are over 375 real-time traffic information display panels operational covering 500 km of motorways, 70 km of Ring Road and 300 km of main city arterial roads, providing information to thousands of users every day. In the UK the majority of major towns and cities are covered by traffic management facilities. In some cases as in Southampton, this is integrated with public transport systems and other systems providing traffic and travel information in real time.

In the city of Torino in Italy a fully automated and integrated Telematics system is operating to optimise over 2.5 millions of trips per day by dynamically controlling over 130 signalised intersections, monitoring the whole fleet of 1300 public transport vehicles and giving them priority when needed, providing real-time information and guidance by using displays at bus stops and variable message signs, as well as other co-ordinated applications. Recent large-scale field trials demonstrated an average reduction of travel time up to 20% for both public transport travellers and motorists.

Such systems will be soon widely operating throughout Europe and when integrated with each other will provide even greater benefits to travellers, industry and the citizens of all Member States. In order to help these technologies to emerge, the barriers to implementation need to be identified and actions to overcome them have to be recommended. This task should not be underestimated as many of the new Transport Telematics systems do not fit comfortably into traditional categories of responsibility, as they tend to breakdown barriers and blur boundaries between different authorities and between public and private sectors.

1.2 The need for Risk Analysis

Improvements to the current market situation for Transport Telematics in Europe will benefit the deployment of a European Transport Telematics Framework Architecture to co-ordinate the various efforts in standardisation, deployment plans and medium term investments. A suitable Framework Architecture will be developed and proposed by the KAREN project by the year 2000.

However, there is no insurance that the Framework Architecture can indeed be established as a viable and permanent structure that will effectively smooth the introduction of Transport Telematics in the European market. This is the reason why obstacles to the deployment of such a Framework Architecture need also to be identified and analysed together with the risks linked to the deployment of ITS in general.

The purpose of this Study on System Architecture (in this document often referred to as the RAID Project) is to identify the main obstacles/constraints (i.e. risks) and then recommend specific measures (known as mitigation strategies in the text of this document). These strategies are based upon a scenario deployment analysis, that should be adopted in order to support the Framework Architecture deployment for Transport Telematics in Europe and the deployment of ITS in general.

A risk assessment process was performed in order to understand the circumstances that could hinder the build-up of a framework regulating the successful deployment of ITS systems in Europe and which consequences would exist if such a framework would not be implemented correctly then failing in assuring basic overall requirements such as interoperability, modularity, compatibility, etc. The RAID risk assessment process is classical in nature [8, 9] and this is reflected as such in the RAID project phases.

1.3 Overview of Methodology

The RAID project started producing a first report focused on the methodology used to build the database of risks that may represent the obstacles to ITS deployment and the analysis of their relevance and importance with reference to implementation scenarios. Based on this initial version of the database, mitigation strategies have been devised for highly rated risks. A database has been completed with the recommended mitigation strategies to handle the risks in given implementation environments. The analysis of the resulting mitigation strategies was then approached according to different points of view:

I. on the basis of the identified categories of recommended actions;

II. on the basis of the selected main implementation scenario;

III. on the basis of the key identified actors who are recommended as responsible for the action implementation.

The relevance of the scenario-based approach is higher in this stage of the study because the mitigation strategy-reference scenario pairs represent the basis for the understanding and applicability of the results of this study.

Both the risks and the mitigation strategies included in this report have been discussed with a selected group of European stakeholders in a two step approach:

- Step 1: provided a more comprehensive view of the possible threats.

- Step 2: validated the proposed overall recommendations.

The results of the RAID study finally provide an important complementary part of the European Framework Architecture currently being developed by the KAREN project with which liaisons have been established since the very early stages of the work.

From the content point of view, this report represents an evolution of those previously submitted of which it includes all the information revised and updated. Consequently it can be considered as a self-standing document which does not requires the reading of the previous reports as background. In addition to the updated contents, if compared with previous issues, this report is completely revised in the structure. The main body of the document is designed to provide and easy-to-read and synthetic description of the activities performed, methodology used and most relevant interpreted results. Annexes are also provided in the form of separated documents which provide more details about the methodology used and the contents of the database produced.

1.4 Structure of the document

The structure of this document is designed to take readers through an overview of the work that has been carried out by the RAID Study. A series of Annexes are provided to enable areas of the work to be explored in more detail if desired. The contents of the document are as follows:

- Chapter 1: introduces the context in which the RAID activities are focused.
- Chapter 2: describes the main goals and objectives of the RAID study.
- Chapter 3: explains how the RAID project relates to the KAREN activities.
- Chapter 4: describes the scenario approach used
- Chapter 5: provides highlights on the methodology applied to compile the different fields of the RAID database.
- Chapter 6: includes a synthesis of the most relevant results emerging from the performed risk analysis.
- Chapter 7: summarises the most important issues resulting from the analysis of the proposed mitigation strategies.
- Chapter 8 : proposes an action plan

Further details on methodology used and results of activities performed are also available as separated document provided as annexes to this document:

- Annex 1: include a print out of the main fields of the database in a table format (i.e. excel-like format).
- Annex 2
  - Part A: includes a detailed description of the fields in the database and the format of the information included.
  - Part B: provides some background information that was used during the project
  - Part C: includes the first level of detailed risk analysis performed on the database content
- Annex 3
  - Part A: holds some advice on how to use the Microsoft Access version of the database.
  - Part B: is the Microsoft Access file including the RAID database.

2. THE OBJECTIVES OF THE STUDY

The study objectives are to identify the obstacles that might prevent the successful deployment of ITS systems in Europe and recommend possible solutions for overcoming them. In order to achieve those objectives a Risk assessment process is performed. This process is organised around three consecutive phases:

- Phase 1: Identification of the Risks - the implementation constraints - for an Intelligent Transport System plus identification of the deployment scenarios and of their influence on the important threats;

- Phase 2: Identification and evaluation of alternative solutions (mitigation strategies) to overcome the identified Risks, and assessment of those alternatives with respect to possible deployment scenarios;

- Phase 3: Compilation of a list of recommendations for the deployment of the systems supporting ITS services and the services themselves, based upon the scenario deployment analysis and reflecting discussions with stakeholders.

The risks that are considered are those that hinder or prevent the implementation of the KAREN Framework Architecture and that hinder or prevent the implementation of ITS systems. All the areas of ITS are considered by exploiting the knowledge and the expertise of the members of the team, the informal contacts established by the members of the team with external organisations through the involvement in national activities, the close liaison with the KAREN consortium and the consultation structure established by the KAREN project.

It is envisaged, although it is not a specific RAID objective, that the work performed during the study will serve as supplementary background information to the KAREN Project by providing ″additional requirements″ that will be analysed during its work.

The experts who work on the study represent companies that have solid know-how and experience in the field of large and complex Transport Telematics systems development and are actively involved in national ITS initiatives or in ITS America. This fact constitutes a warranty with respect to the pertinence of the results produced. However the study carries its intrinsic limits such as:

- the inherent subjectivity of the experts' opinions specifically when having to decide about the most critical threats and their probability of occurrence, or

- the incomplete representation of all points of view specifically when having to evaluate non technical issues such as cost or political ones; thus resulting in an incomplete understanding of all the issues related to deployment of the KAREN Framework Architecture and ITS systems, or

- the possible lack of knowledge in the team of most recently launched actions in the domain of ITS with consequent identification of threats that are not likely to occur any more.

All the above mentioned points of weakness cannot be eliminated completely, but measures are taken to reduce the effects. Decisions and judgements are always averaged among the team members in order to limit subjectivity. The other two limitations are smoothed by involving actors external to the team who can complement the knowledge available within the team; external consultation is started in the current phase of the project and will be expanded further during the third phase. Key ITS actors

throughout Europe have been and will be approached including: government authorities, transport operators, infrastructure owners, service operators, manufacturers and freight operators.

Risks and mitigation strategies are derived using comments and opinions from several countries, some of which are represented by the members of the RAID team. It is recognised that Member States have sometime very peculiar characteristics and differences in the national laws, role of organisations, regulatory frameworks, kind of financial support, infrastructure available and other factors that might affect the analysis of the threats and the interpretation of the mitigation strategies the analysis of the strategies was performed taking into account these differences when possible.

The strategies finally proposed and analysed in this report were consolidated through a comprehensive consultation of representatives of the relevant ITS sectors.

3. CONNECTION TO KAREN

The KAREN (Keystone Architecture Required for European Network) consortium in the period 1998-2000 will carry out the KAREN project TR4108, sponsored by the European Commission's Telematics Application Programme. The final objective of the KAREN project is to develop a Framework Architecture for Transport Telematics applications in Europe needed to ensure the wide-scale deployment of ITS in a co-ordinated and progressive way. The Framework Architecture has been defined as the minimum stable framework necessary for the deployment of working and workable ITS within the European Union until at least 2010.

3.1 Impact on the KAREN Architecture definition

The Framework Architecture definition follows a typical Systems Engineering life cycle. A comprehensive set of user needs and systems requirements has been identified. The identification is based on those identified by the previous and on-going European projects and on the national needs. Then the needs and requirements are translated into Architectures that form part of the overall Framework Architecture. There are four Architectures: Functional, Information, Physical and Communication. The Functional Architecture provides functionality that will support all the fundamental services covered by the Framework Architecture. The information architecture describes the information used by the processes. The Physical Architecture describes the components into which the functions can be grouped to provide objects that can be implemented and deployed. The Communication Architecture indicates how the different physical objects will exchange data. The Functional Architecture will be closely related to what has already been developed in Europe and elsewhere.

The RAID Project work-plan was initially chosen so as to best take advantage of the KAREN intermediate results, in particular to make use of the user requirements analysis, the identification of existing systems and their characteristics, and of the list of fundamental services as defined during the functional analysis. The whole intention was to structure the RAID Risk analysis according to the KAREN work in order to relate the two sets of Project results more easily. This would have been achieved by structuring the Risk analysis according to the KAREN User Needs.

Due to a late start for KAREN this became impossible and the RAID Project had to revise its strategy. Different alternative solutions could have been chosen for structuring the Risk analysis. The list of services selected as reference for the definition of the clustering of Risks is the ISO list of services [1]. It was chosen because it is supported by ISO (neutral and internationally valid) and because the analysis produced by the CONVERGE project [2] shows that it is possible to draw one-to-one correspondences between the services of the existing lists (e.g. ITS America, VERTIS, and CORD list of function). Consequently the choice of the reference list of services was not critical.

The actual time synchronisation of the KAREN project and the RAID study has its own benefits with respect to the KAREN Project. This is because the Risk assessment work in RAID enables threat(s) to be identified for each fundamental service. Each threat has its own probability of occurrence and impact. When a threat is identified, if it is an important one, then a mitigation strategy is identified. The goal of such a strategy is, by definition, to lower the probability of occurrence of the Risk.

The mitigation strategies are of particular importance for the KAREN Project because they could be included as additional requirements that need to be considered during the definition of the Framework Architecture. Recommended strategies, when further analysed in the context of the KAREN activities, can originate the need for the introduction or adaptation of specific elements (i.e. either in

the functional, physical or communication architecture) to support or allow their actuation. This characteristic of the KAREN Framework Architecture will consequently enforce the probability of full success for ITS implementations based on KAREN conforming system architectures.

3.2 RAID and KAREN are complementary

The KAREN Project focuses on the Architecture definition whilst the RAID Project analyses the obstacles associated to the Architecture deployment. The KAREN Framework Architecture is based upon the User Needs that are identified by the Project. The User Needs consist of those requirements that users will expect to be met for the successful implementation of each Service.

The RAID Project focuses at the implementation of the Services from the point of view of the User, but also (and crucially) those in charge of operating, deploying, maintaining, marketing or selling systems which will conform to the KAREN Framework Architecture.

The first meeting of the KAREN Permanent Consultation Group (PCG) in September 1998 was used as a mechanism to derive input from professionals in the transport sector, industry experts and stakeholders. A presentation on the RAID Project was given and first intermediate results were distributed in this occasion, establishing the first contact with organisations external to the team that can complete and complement the know-how of the project team. After receiving first general comments, which confirmed the necessity to support the Framework Architecture with a set of recommended measures to facilitate its deployment, selected stakeholders have been met personally to discuss specific issues of the RAID activities in order to identify gaps and weakness of the current version of the analyses. The RAID activities were also presented in occasion of the first KAREN forum held in December 1998, the audience feed-back stressed once more the importance of consolidating the recommendation produced by RAID by means of consultation with external professionals in the field. Also in this occasion appointments were fixed to meet directly stakeholder representatives. Consultations then continued in the next phase of the RAID study with the aim to complete and consolidate the results of the study as reported in the current version of this report.

Thus the KAREN final output can count on this complementary document containing practical indications to ease the context for ITS deployment by proposing solutions to obstacles perceived as critical by ITS actors.

4. THE RAID SCENARIO APPROACH

The risk analysis performed by RAID follows a scenario based approach that aims, by the end of the study, at delivering a set of risks and corresponding mitigation strategies analysed according to the context or the environment in which the risk is considered.

The scenarios are needed for defining the boundaries within which the deployment of ITS systems is considered and for which risks and mitigation strategies were analysed. The strong link between scenarios and mitigation strategies is reflected in the definition of a scenario. This has been agreed to be as follows: *"a scenario is a set of circumstances in which a risk might occur and for which a mitigation strategy is recommended"*.

While the initial list of risks was compiled by considering a unique reference 'macro scenario', that includes all the characteristics of the conventional European ITS environment, further analysis and revisions of the highly rated risks allowed to distinguish between scenarios at a lower level - the reference basic scenarios. Detailed reference scenarios are needed for defining the context in which each risk is relevant, and determining the critical elements of the scenario for selected risks.

In order to be useful the number of reference basic scenarios has to be limited (i.e. less than ten) so that the scenarios can be handled and combined as needed. In other terms, each scenario has to represent a simplified abstraction of a real ITS deployment environment. On the other hand a scenario must not be too abstract otherwise it cannot be linked to actual experiences. It also appeared evident that the definition of scenarios can be done only while working with the definition of threats, risks and mitigation strategies in an iterative way and in successive refinement steps.

The final objective is not to provide a set of scenarios each representing in details the specific ITS environment valid for one country or even for one region, but to provide a sound reference basis for modelling any possible environment instead. An example of a possible use of the basic reference scenario is provided later in this chapter.

4.1 Elements of the scenarios

Each scenario is identified by a selected combination of elements that describes the main characteristics of the ITS deployment environment. Each risk can be allocated to one or a set of scenarios highlighting those elements that are critical for the risk and/or those that are not significant for the impact of the risk. When an element is found to be critical for a risk then a set of mitigation strategies is expected to be recommended: one for each different value of the element. The risk analysis is completed for each risk when the corresponding pairs scenario-mitigation strategy are defined.

The elements that should be considered in each scenario are of different nature and all important for defining the ITS deployment environment. A description of the elements composing the scenarios is as follows:

- the geographical scope - description of the kind of geographical area in which the risk applies. Some risks make sense only on particular geographical scopes, others may apply to any of them and others may be entirely independent. **Urban**, **Interurban** and **Rural** are considered as possible values. The same risk may be relevant to all geographical scopes although the corresponding mitigation strategies can be different for each of them;

- the main trends for ITS development planning - description of the main trends for investments currently in use throughout Europe. Three pure possibilities were selected to be considered although actual environments are always a combination of them:

  a) ITS strategy focused on the use of Telematics for disseminating real-time multi-modal and multimedia information to both end-users and operators/authorities/police as a means for facilitating pre-trip and on-trip choices. Technologies used are Internet, VMS, Information terminals, on-board terminals etc.

  b) ITS strategies focused on the provision of Telematics infrastructures to improve the efficiency and safety of the transport network, and on the provision of public transport services. Applications used are bus priority, dynamic route guidance, speed control, traffic light control etc.

  c) ITS strategies aimed at using Telematics applications for traffic demand management by introducing access restrictions and other dissuasion measures. The technologies used include Electronic payment, Car pooling, Access control, Road pricing schemes etc.

A risk may be applicable only to scenarios in which one trend is dominant or it may be independent on this element and different mitigation strategies may suit the different situations.

- the level of public and private co-operation – description of the leading actor in the ITS deployment. This element completes the scenario description distinguishing between two complementary situations in which (i) the **Public** sector is leading and ruling the ITS development and (ii) the Private sector is the driving force of the ITS development. In addition the case of a **Mixed** situation is also considered where public and private sectors find a co-operative way of introducing ITS, with the public sector introducing ITS in their basic service components and leaving space for public-private partnership;

- the time horizon - it is the description of the reference time period in which the risk, its potential consequences and the recommended measures are considered. Short, medium, and long-term time frames with reference to the plan for the development of the KAREN Framework Architecture or the availability of new technologies are taken into account. They are: 2002: KAREN Framework Architecture is issued; 2005: maturity of the KAREN Framework Architecture; 2010: the KAREN Framework Architecture will have to be revised significantly.

4.2 Scenario definition

From a purely mathematical point of view, the resulting number of scenarios should correspond to the number of possible combination of the values for the above mentioned elements. Practically, not all-possible combinations are meaningful, thus only the most representative scenarios are defined and discussed against the most critical risks.

The methodology used in RAID aims at defining the details of the scenarios in a ″step-by-step″ approach.

First Step ²Global Scenario based²

A global ″overall″ scenario is considered to collect as many threats as possible. The ″overall″ scenario is not formally described but there is a common understanding that threats and risks are looked at while thinking of the current conventional European environment for ITS deployment. For instance neither the effect of the ″global warming″ nor the existence of a law allowing the sole use of electric cars are considered because these are implicitly assumed to be elements outside the considered ″

overall scenario". This is because the changes that they could introduce would probably make all of the threats and strategies null and void.

Second Step ²Elements of Scenario a Priori²

All the listed risks are successively revisited keeping in mind the main elements (i.e. those described above) that are selected as descriptive of the reference scenarios. The scenario elements that are critical for each risk, as well as those that are not critical, are identified and discussed so that a first view of what the reference scenario is likely to be is depicted.

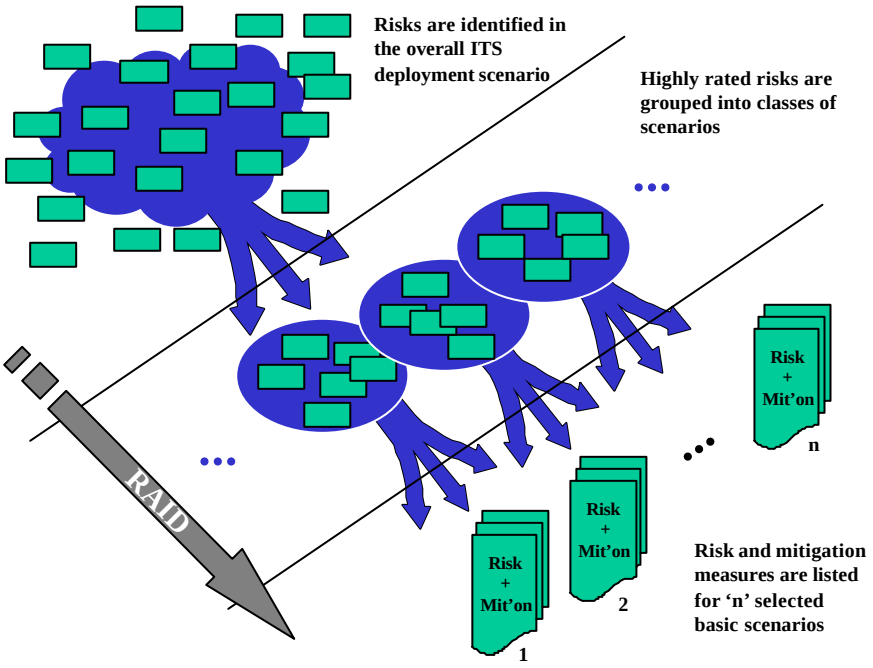
Example: for a given risk named "A" it can be said that it depends neither on the "geographic scope" nor on "main trends for ITS deployment". For the same risk it can be also said that it is relevant only if the purely "public" funded scenario is considered while the "time horizon" is a critical element and different implications can be envisaged if different time horizons are considered.

Third Step ²Define Mitigation Strategies²

Given a risk, different recommended mitigation strategies are to be expected for the different values of the elements identified as critical and defined as such.

Fourth and Last Step ²Elements of Scenario a Posteriori²

Finally, scenarios are revisited when the risk analysis is completed through describing the recommended mitigation strategies. This is due to the fact that the "relevance" of the risk and consequently the actions that should be taken, as well as who should take the responsibility of overcoming the risk, often depends on the scenario.



Picture 4.1: Illustration of RAID Scenario Approach

4.3 Differences between countries

Beside the scenarios described above it is also necessary to analyse the particular context present in the different EU member states. The main reason for this kind of analysis is based on the fact that while in the private sector international co-operation and business rules have been established for a long time, the situation is quite different when public authorities are involved as institutional and organisational aspects are different from one country to another. Also the different level of development of infrastructures, already existing ITS products and services as well as the involvement in European activities have to be considered.

The direct implication of these observations is that recommended mitigation strategies have to be adapted to the characteristics, priorities and already established structures present in the different EU countries. National and local authorities are often identified as the key actors that have the capability to intervene and favour the deployment of ITS. In order to show the 'practicality' of the recommendations provided by RAID, their description need to be completed considering the experience in Public-Private-Partnership and project financing initiatives existing in the different countries, organisations already active for promoting ITS, as well as plans already established for ITS deployment.

This information have been initially collected through existing reports:

- the WELL-TIMED Study [11]

- the TELTEN 2 report [13]

and has been updated by discussing the details of the RAID work with public authorities of different EU countries: France, Germany, Italy, the Netherlands, Sweden and UK. The proposed mitigation strategies included in the second report have been used as a basis for discussion in order to better focus on the objectives of the study and to allow to better target the possible actions to be undertaken by the concerned actors.

In the following subsections an overview of commonalties and of the currently ITS related activities and organisations existing in the member states is reported. Detailed references to relevant country specific characteristics are included in sections seven as part of the analysis of the single mitigation strategies.

4.3.1 Commonalties

In all European countries, public authorities are in charge of traffic management, even if they can delegate them to a public or private operator (toll motorway for example). Traffic monitoring is then in majority in the hands of public sector, even if some countries have allowed implementation of data collection devices by private sector and have established general rules (UK, Germany, Austria) or discussed it on a case by case basis (Flanders, the Netherlands)

This situation explains that ITS services based on the provision of road data are in majority under the control of public authorities. Access to public data is ruled by a legal framework in some countries (UK, France, Norway) but in general it is treated through specific contracts. All countries have now taken initiative to facilitate this access. [13, Volume 4C, table C

Concerning the regulatory framework, the TELTEN2 report [13], reveals that in most of the Member States, the existing legislation allow for ITS services deployment. The main obstacles seem those of ITS services using in-vehicle devices and of the advanced driver assistance domain. [13, Volume 4C, table C5].

4.3.2 ITS deployment plans

For speeding up the ITS deployment, some countries have established ITS deployment plan for the public sector:

4.3.2.1 Italy

In 1995, the Italian Ministry of Public Works officially presented the first national plan for road transport Telematics described in the document "Telematica e Sistemi di Comunicazione Avanzata Applicati alle Reti Stradali - Primo Piano Nazionale (1996-2002)".

The first National Plan posed as a first target to be achieved by 1998 the introduction of the RDS-TMC technology with the coverage of the North Italian sections of the Trans-European Road Network. The National Plan played a key role in the dissemination of the knowledge of new technologies and in the definition of a European context for their implementation. It also contributed to the solution of problems at infrastructure level by creating a reference architecture for data exchange and favouring the monitoring and the control of the road network. The RDS-TMC service has been developed and put into operation by solving basic organisational obstacles.

The Second National plan was compiled by the Ministry of Public Work at the end of the year 1998 to upgrade the first National Plan and to extend the horizon up to the year 2004.

The second National Plan was developed following two main guidelines:

- To move from Advanced Transport Telematics (ATT) to Intelligent Transport Systems (ITS). The latter representing the combination of information, communication and technologies in integrated systems aimed at improving efficiency and safety of transport for a better and more comfortable mobility and with a reduced environmental impact.

- Improvement of the level of service provided on the Italian roads by means of information and other services for travellers. Information is considered as basic factor for both road safety and mobility management.

The basis for the definition of a national architecture compliant with the European framework architecture is being elaborated by a working group nominated by the ministry of public works.

The second National Plan focuses on the long term planning for the introduction of the new technologies, the co-ordination between the actors involved and the harmonisation of the development of new technologies by defining the following main objectives:

- To create an homogenous infrastructure throughout the interurban and motorways national network compatible with the rest of Europe.

- To define an organisational architecture allowing the integration of all ITS applications

- To define the needed interfaces with the urban environment

- To involve in the process the industries and the service providers

- To involve all other modes of transport to multimodality.

In addition to this specific plan, the Ministry for Transport is currently defining the new national plan for transport in which it will be included a specific section on the role of Transport Telematics. The publication of the document is expected within the year 1999.

4.3.2.2 France

In France the Ministry of Equipment (METL) has drawn up a similar plan. The SDER (Schéma Directeur d'Exploitation de la Route), follows the TELTEN guidelines and indicates main priorities (services, geographical coverage, etc.) for traffic management and traffic information. Priority has been given to the deployment of RDS/TMC and new traffic management systems or extension of existing ones on peripheral arteries of big cities (Paris/SIRIUS, Lyon/CORALY, Lille/ALLEGRO, Bordeaux/ALIENOR, Toulouse/ERATO, Marseilles/STRADIVARIUS, Strasbourg/GUTHEMBERG and others). A study is currently conducted by the METL for planning the implementation of ITS services on TERN according to TELTEN recommendations. In addition, the METL is preparing actions in order to develop a national ITS architecture, which will be compatible with the KAREN Framework Architecture.

4.3.2.3 Germany

In Germany, the Federal Government has developed a clear policy between public and private activities Basic information services related to road operation are the responsibility of public sector, while new value added services are to be provided by the private sector. In some urban areas, and states traffic information networks are under implementation on a public/private partnership basis. (in WELL-TIMED study, Main Report [11].

4.3.2.4 The Netherlands

In the Netherlands, the next version of the interurban traffic control architecture was expected to be released in February 99. The architecture titled "Architectuur voor Verkheers Beheersing" (AVB) is led and financed by the Dutch MoT, which is leading the KAREN project. It will then contribute to the European framework. The architecture in development is based on five regional traffic control centres and one national centre, which will be under the control of the police. It has been designed to meet present and future needs such as floating car data, roadside and in-vehicle information systems, dynamic local and regional traffic control strategies, dynamic infrastructure (e.g. tidal flow systems), automatic vehicle control, road pricing, pre-trip information, and the co-ordination of motorway management with neighbouring countries

4.3.2.5 United Kingdom

UK has not established an ITS plan but has already defined rules for implementing the different ITS services: UK introduced first in Europe legislation for the licensing of driver information systems in 1989. This Act allowed the fast development of private initiative for traffic information: Traffic*master*™ was the first commercial ITS service implemented and other commercial services are now under deployment. It is worth mentioning that in the UK, Automobile Clubs have a long tradition of "service providers" in co-operation with transport authorities and Police. They have reached agreements with Traffic*master*™ to share information. At present, the Highway Agency (in charge of

the trunk network in England) has launched the Traffic Control Centre project aiming at implementing strategic traffic management by delegating the operation to the private sector, which will be authorised in addition to providing additional value added services to the individual user. The Highway Agency has yet produced its own "business plan" for preparing ITS deployment.

4.3.2.6 Sweden

In August 1998 the Swedish National Road Administration gave Cap Gemini Travel & Transport the commission to start a Swedish system architecture project for ITS. The project is expected to consider the ongoing international work and especially the KAREN project. The Swedish project is to run until July 2000.

The aim of the project is to enable an efficient exchange of information between the organisations that supply and/or use information within the road traffic system. One purpose of the project is to suggest a solution to the problem of information exchange between the different actors involved. The solution shall be defined in the areas of responsibility, content, function and distribution. The other purpose of the project is to develop a working methodology for designing system-architectures within the ITS-area. A step-by- step methodology that can be used and developed through "best practice".

The project is divided into seven parts. Six of them are chronological and the seventh is the method development that will go on during the whole period. It starts with a focus on the services. The assumption is that a system always exists for its customers. Every ITS service is to be developed and evaluated from a customer perspective.

It is assumed that since ITS is often complicated, one way of simplifying is to start with the services defined as most important and develop them: to simplify by going from general to special only when necessary to gain value to a customer.

To evaluate and make priority between services is a difficult task. The project has developed an embryo of a method for this. The method is partly based on weighting the effects of the service in relation to the Swedish transport policy values of minimising death and injury, minimising burden on environment, facilitating accessibility to all members of the society and efficiency. The other part is letting a fixed set of representatives for customers, authorities and operators do their weighting. Adding the two parts gives the final priority.

The method includes mainly four dimensions. Those are:

- customer orientation - the work is based on the defined needs of the customers
- process oriented - the flow of information is described in added-value chains
- relations -the project aims at making clear how relations and responsibilities are interfacing and how they can be generalised
- time - the project aims to analyse the demands on information and distribution from the perspective of how a service relates to time

The method has been tried in a minor test phase. Several different operators like police, emergency services, public transport operators, commercial services and commercial hardware have been interviewed. The processes and the customer needs they take part in developing are being drawn. The service priority phase is going on right now. The method has shown itself useful and the project will continue according to the plans.

4.3.3 ITS organisations

Besides the European level, with the existence of ERTICO, initiatives are taken by several key actors in order to form organisations with the objective of promoting ITS deployment.

4.3.3.1 United Kingdom

Such groups are among others ITS Focus in UK: ITS Focus is a non-profit association of organisations concerned by ITS, including today 107 members (industry, public authorities, academics, police, consultants, etc.) Its main aims are "to ensure that ITS becomes an integral part of transport policy and to help the UK to become a major centre for ITS activities". It has set up a series of task forces and interest groups on specific topics (one on architecture).

4.3.3.2 France

Though, not so much formalised, in France some groups of common interest parties are acting in the field of ITS. "ERTICO France" was a first tentative to relay ERTICO, but its interest was quite limited due to its partnership: French members of ERTICO.

Another organisation, ATEC (Association pour les Transports, l'Environnement et la Circulation) which is a non-profit association has set up several committees constituted of members from public and private sector on ITS topics: new ITS services, ITS evaluation, use of DSRC, environment and ITS, safety and ITS. The objective of these committees is to establish position papers (even reflecting divergences) and influence decision-makers.

4.3.3.3 Italy

In March 1999 the new association TTS ITALIA (Telematics for Transport and Safety) will be formally created. The members of the association include national stakeholders in the field of transport Telematics: ministries, local authorities, private industries, user associations, service providers.

Main activities of the association are:

- Support the development of the new technologies, applications, architectures necessary for the establishment of an open market of ITS systems
- Provide technical and organisational support to members for related activities such as involvement in European projects, access to public funding, etc.
- Provide the liaison between the members, the standardisation bodies and the national and local initiatives.
- Favour research and development activities by co-ordinating the activities for obtaining European and national funds for projects.
- Perform dissemination and education activities in the field of ITS.

4.3.3.4 Germany

In Germany, a Federal Forum on Transport Telematics was established in 1995 to act as an enabling institution for the rapid development of ITS [11]. Participation in this high level group chaired by the Federal Minister of Transport, is from automotive industry, electronics industry, authorities, association of cities, etc. The objective is to jointly promote the implementation of ITS within an integrated transport context.

5. METHODOLOGY USED

This section explains how the information handled by RAID has been captured. The procedure used directly follows the RAID three phases. This is why there is one sub-section per phase.

The information to be captured by RAID is related to:

- The Risks that can impact the deployment of a Transport Telematics European Framework Architecture,
- The mitigation strategies that allow lowering the Risk effect, according to possible deployment scenarios.

Describing the information to be captured is to define those attributes and structures that allow the Risks to be recorded and analysed in their ITS context. It is also to ensure that any information is captured in a homogeneous way and that it is possible to specify a Risk with its main characteristics. Finally it is to ensure that the Risks can be managed correctly during their definition process. A list of the attributes under which Risks were captured is provided in Annex 2A and includes a detailed description of each attribute. The remainder of this chapter describes the procedure used.

5.1 Step by Step Procedure for Phase 1

The procedure used by the RAID team to compile the Risk database during Phase 1 is a four-step procedure followed by all partners, partly with alternating responsibilities (e.g. in the review periods, to assure a high degree of objectivity).

The first step ″Setting-up the Scene″ aimed at organising the Risk information definition. A service-based approach was chosen, hence the database Excel-table was organised accordingly.

The second step ″Identifying the Risks″ aimed at collecting the raw information. Each partner had to define Risks for a precise set of services. It was deliberately decided to allocate more than one partner to a given service in order to ensure a better cross-fertilisation of ideas..

The third step ″Consolidating and Reformulating the Risks″ aimed to merge and categorise the Risks. The fourth step ″Defining Scenarios and Allocating Risks onto Scenarios″ aimed to identify the scenario list to be considered for RAID and finally to allocate the risks onto those scenarios.

One difficulty of the procedure was to guarantee that the rating would be relevant, bearing in mind that only qualitative information can be provided. In order to achieve this important criteria the RAID team adopted a DELPHI[1] technique approach [7] and tailored it to its own needs. The DELPHI approach was used to guarantee the objectivity of the Risks. It requires that the experts participating in the development of the Risks alternately review the results produced by their colleagues.

1 The DELPHI procedure was created at the RAND CORPORATION in the 1960's as a means to extract opinions from experts. It is intended to gain advantages of a committee of experts (combining amounts of knowledge) while overcoming their disadvantages (e.g. subjectivity) and thus reaching a forceful agreement

The set of reviews making out the kernel of the DELPHI approach were performed at different stages:

- at the end of the ″Identifying the Risks″ step where each partner was allocated exclusive services in order to achieve coherency within each service,
- during the ″Consolidating and Reformulating the Risks″ step in order to achieve coherency through the data and specifically to identify threats that could become ″General″ ones,
- at the end in order to polish the wording, the attributes values, and the production of the missing information. This last review was performed by a limited set of partners.

5.1.1 Setting-up the Scene

This step aimed at organising the Risk information and procedure definition. It consisted of a brain storming session where a procedure and a Risk structure was challenged against the first identified Risks themselves. The objective of the brain storming was to verify that the procedure and structure under definition could be used. It identified when the different attributes of the structure could be filled in during the process and defined the way in which different sources of information will be merged and traced back to their originator. The list of services selected as reference for the definition of the clustering of Risks was then chosen and the structure of the database was completed, as it is described in detail in the annex. At the end of this step a procedure and a structure were finalised.

A numbering system was adopted in order to ensure that there is a unique and unambiguous number for each threat.

5.1.2 Identifying the Risks

The step “Identifying the risks” aimed at compiling the first version of the database. The sequence of actions was the following:

- Identify and provide threat description

  Each partner described the threats with the following attributes:
  - Service Number
  - Service Description
  - Threat Number
  - Threat description
  - Consequences of the Threat

  Then all the available information was merged together.

- Define threat rating

  In order to enforce coherency at the service level each service was allocated to a different partner. Then the rating was defined through the following attributes:

  - Probability of Occurrence
  - Explanation of the Probability of Occurrence
  - Level of Impact
  - Description of the Level of Impact
  - Risk Rating Scheme

  Finally, all the available information was merged together

5.1.3 Consolidating and Reformulating the Risks

The step "Consolidating and Reformulating the Risks" aimed at reviewing the threats, merging and categorising them, and finally filling in the missing attributes. The sequence of actions was the following:

- Merge at the service level

Within each service the redundant threats were identified and those threats that belonged to service "0" were identified. A traceability column was added internally in order to keep track of the author of the merging and suppression.

- Define the Category values

All the available information was merged and a consensus was made among the team members in order to identify the category values.

- Merge at the threat analysis level and revise the rating

The responsibility for all services was transferred to a working group who had the objective to reword the threats, identify and correct any redundancy, and to identify those threats that belong to service "0". It also had the responsibility to revise the rating of the threats and finally to fill in the following attributes:

  - Category
  - Geographical Extension (Geo. Ext.)
  - Life cycle
  - Risk Bearers (stakeholders)

5.1.4 Defining Scenario and Allocating Risks onto Scenario

The step " Defining Scenario and Allocating Risks onto Scenario " aimed at identifying a possible scenario list, then to indicate which risk were belonging to each scenario. The sequence of actions was the following:

- Define the Scenario list values

The appropriate scenario list was established.

- Identify the scenario influence

The scenario influence was only sought for risks rated ORANGE or RED. For each of such threats the relevant Scenario Number was introduced.

5.2 Phase 2 Step by step procedure

The final aim of Phase 2 is the recommendation of the mitigation strategies that will reduce the risks to the deployment process. A second objective of this phase is to consolidate the analysis of the scenarios started in Phase 1. This was achieved by linking the mitigation strategies (and their categories) to the appropriate scenarios. The procedure used by the RAID team to compile the second phase of the project is a four-step procedure followed by all partners.

The first step “First definition of mitigation strategies” aimed at defining the first version of the mitigation strategies to avoid and or control the risks defined in the first phase of RAID.

The second step is the "First review of the mitigation strategies" aimed at the review of the contents of the information provided in the table both from a syntax and a semantic point of view. Furthermore, it aimed at determining the strategies that needed to be merged and at categorising them. This step was deliberately performed by other experts than those who worked on the first step.

The third step "Second revision of mitigation strategies and analysis of the strategies" aimed at the final review of the previous step and the analysis of the categorisation of the strategies that it defined.

The fourth step "External Experts feed-back" aimed at identifying, through formalised interviews with a limited set of ITS experts, whether all ISO services were correctly covered, whether or not the mitigation strategies were complete and improvements to be included in the database. This consultation activity has to be considered as preliminary since a second consultation is to be performed during the Phase 3 of the study.

In the following sub-sections, the four steps will be illustrated successively.

5.2.1 First definition of mitigation strategies

The first step in Phase 2 of the RAID project addressed the formulation of strategies to deal with the risks defined in the first phase of the project. This first step comprised the following identification activities:

- Strategy action

For each of the RED and ORANGE risks that were formulated in the first phase of the project one or more strategies were defined that could be deployed in order to deal with these risks. Only risks with these ratings were considered, as they are the most significant and likely to have greatest impact. Through the RAID team members different points of view and thus sources of information and concerns have been considered for defining the first version of the mitigation strategies. Those points of view cover Research, Industry, System Architecture, Telecommunications and Transport Telematics.

After the strategies where defined by the 'strategy definition' team, all strategies were subject to various internal reviews and discussions. This resulted in additional strategies and changes to strategies that were already formulated.

- Strategy action by whom

Together with the mitigation strategies, also the organisations that should implement the strategies were defined. In this second phase of the RAID-project it was not always possible to precisely indicate which actor was really involved in a strategy action and with which level of responsibility. This is due to the lack of knowledge within the RAID team on this organisational matter in Europe at any level (European, National, Regional, or Local). For instance, the role of the European Commission could be to initiate the strategy when other organisations would implement it. This question of roles has been deferred to the third phase of the RAID-project by means of consulting external people able to help in completing the information.

- Strategy action type

When devising the mitigation strategies, it was found that they could be classified into one of two types. These are strategies for risk avoidance and strategies for risk control. A specific strategy is of the type 'risk avoidance' when implementation of this strategy would prevent the risk occurring. When

the effects of the risk could be controlled by implementation of a specific strategy, i.e. the effects of this risk will become more manageable, but the risk would still occur, this strategy is considered to be of the type 'risk control'.

- Scenario (in fact Scenario Number)

Each scenario identified during Phase 1 was put in perspective of the mitigation strategies and completed or corrected when required. All attributes mentioned in this section, i.e. Strategy action, Strategy action by whom, Strategy action type and Sc*enario* Number are added and included in the table that was formulated in the first phase of the RAID-project.

5.2.2 First review of the mitigation strategies

The objectives of the second step were twofold. The first objective was the review of the contents of the information provided both from a syntax and a semantic point of view. The second objective was to determine the strategies that need to be merged and classified in groups. This step is deliberately performed by other experts than the ones in the first step.

The first action taken was the review of the strategies. This included a review of the wording of the mitigation strategies, the assigned organisation to take the action, the action type and the scenario number. The sequence of the actions on the syntax was the following:

I. On the basis of this review, several strategies have been reworded and merged. As there appeared to be a large number of formulated mitigation strategies, it was decided to categorise them into a limited number of groups, called action categories. This would enable strategies with a common theme to be grouped together, and provided the possibility of creating a smaller number of more general but all-inclusive strategies.

II. Four new columns were added to the risk table - one for the category of each Action. Each mitigation strategy was then allocated to the most appropriate action category. On the basis of this categorisation, combined with the scenario for each risk, an analysis of the mitigation strategies is performed in the next step of phase 2 described in the following subsection.

5.2.3 Second revision of mitigation strategies and analysis of the strategies

In the final step of this phase, two main actions were performed. First, the second revision of the mitigation strategies focused on the involved organisations, the action type and the scenarios. Thereupon, an analysis of the mitigation strategies was accomplished. The analysis of the results of the previous step was performed in three parts. First, the strategies and the involved organisations for each action type were checked; second, the analysis was performed by scenario; and third the results were analysed by actor.

Finally the results of the strategy analysis were used to produce a small number of high level strategies. These will be used by Phase 3 in its presentations to stakeholders and others.

5.2.4 External Experts Feed-Back

Despite the good coverage of the domain by the experts' team, it appeared that some of the areas were less considered. The risks identified and mitigation strategies proposed required then to be validated by external experts of the related area. This consultation initially planned for the third phase was then initiated as part of the phase 2.

For achieving this consultation a questionnaire was elaborated and used as guidelines during face to face interviews. Some members of the team were asked to approach key stakeholders focusing the attention on their area of competence. The objective was to complete the following items:

- Identification of missing risks
- Identification of missing mitigation strategies
- Review of selected entries of the database
- Identification of priority areas
- Review of the 'overall' mitigation strategies included in the first issue of this report

Stakeholders approached in this preliminary consultation phase included: car manufacturers, public authorities, public transport operators, service providers, FFM operators and automobile associations. People contacted were experts in their field and agreed to have an informal conversation on the subject on a personal basis then without formally providing the position of the company represented.

5.2.5 Final consolidation

Phase 3, already initiated during phase 2, consisted in a consolidation of the mitigation strategies analysed during phase 2 by continuing the consultation of the key ITS actors in Europe: European Commission, public authorities, transport operators, infrastructure owners, service providers, manufacturers, users which are included in the KAREN "Permanent Consultation Group". Particular attention was given to areas where the most critical risks have been identified and where mitigation strategies appear controversial during the first consultation. In addition, in Phase 3, differences between countries are highlighted when relevant.

It is important to mention that the methodology used for this consolidation process was based on a voluntary basis from the persons interviewed: representatives of the RAID consortium were not carrying an official mandate. For the sake of efficiency and celerity, no agreed "mechanism" was set up between the Commission, the RAID consortium and the parties involved to make these consultations "official". The answers of the persons interviewed reflect then their own opinion and judgement and cannot be considered as those of the company/organisation they belong to. But it is important to highlight that, "not constrained by any pressure", these opinions are those of experts well aware or the subject treated and have then much value than more official statement at this stage of the process. It is then not possible to give a nominative list of the persons and organisations interviewed in this report. The following table gives the distribution of the interviews according to nationality and type of organisation.

Country / Type of Organisation	B	D	EU[2]	F	I	NL	S	UK	Total
European-type organisation			**2**						**2**
Freight Operator			**1**						**1**
Information Service Provider		**1**	**1**	**1**	**1**			**1**	**5**
Local Authority				**1**	**1**				**2**
Industry		**2**	**1**	**1**	**1**		**1**		**6**
National Government,		**1**		**1**	**1**	**1**		**1**	**5**
Public Transport Operator	**1**								**1**
Total	**1**	**4**	**5**	**4**	**4**	**1**	**1**	**2**	**22**

[2] Europe : organisations at European level

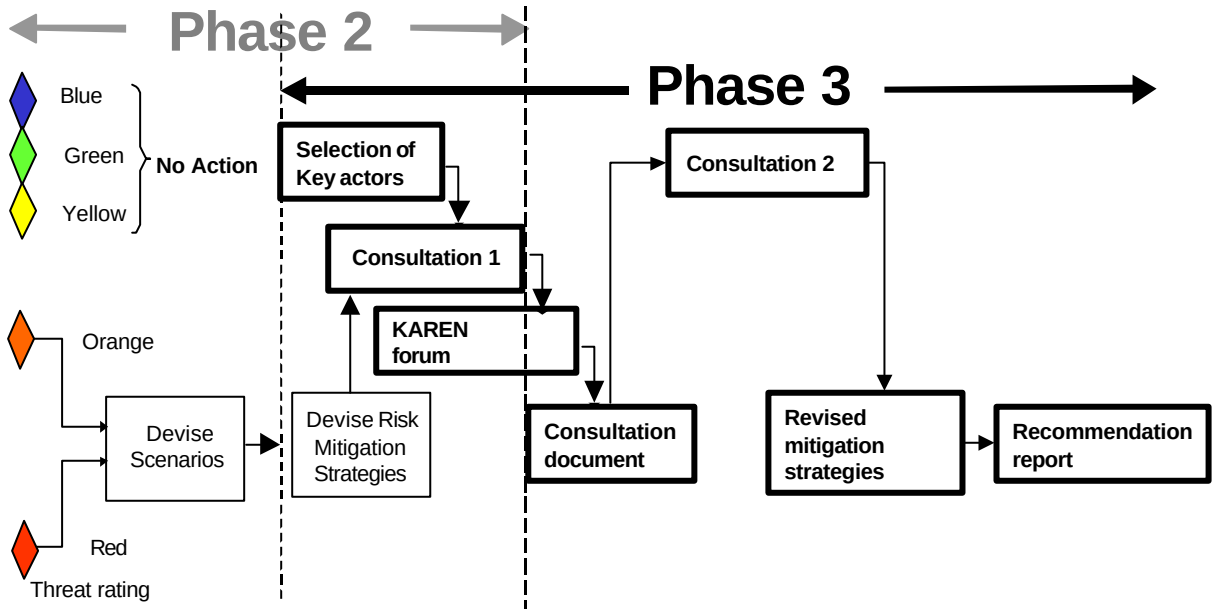
Table 5.1: organisations and countries of consulted stakeholders

Phase 3 consisted in the following steps:

- presentation of the RAID project and the results obtained so far at the first KAREN Forum (Amsterdam, 10/12/98)
- elaboration of a "consultation document"; based on the second report and highlighting the main mitigation strategies proposed
- continuation of visits and interviews of key actors
- refinement of the mitigation strategies
- production of the recommendation report

Once the consultation phase completed, this report has been produced in close co-operation with the Commission. It summarises all the work performed during the study, gives an outline of the analysis performed supporting the recommendations for actions needed by the Commission and proposes an action plan for implementing the main strategies identified including a dissemination plan of the recommendations. The report is also available on CD-ROM and on www2.echo.lu/telematics.

The process described above can be illustrated by the following diagram



Picture 5.2: RAID Phase 3 Work Plan

6. RISK ANALYSIS

Threat analysis plays a key role in the implementation of ITS. Early definition of the situations that have the potential for impeding the implementation of ITS is a critical element to the success of their implementation. The approach adopted in RAID differs somewhat from the usual business case method that could be use for deploying a specific product or systems. Much attention must be given to legal, institutional and organisational issues. RAID is aiming at identifying a consistent set of threats but new ones are believed to appear as the ITS market further develop.

This analysis consists of three parts. The first one presents a general analysis of the threats, the second depicts the threats according to their category and the third one contains an analysis according to strategy scenario. Only threats rated as "RED" or "ORANGE" have been included in this analysis.

6.1 General Analysis of the Threats

Legal, institutional and organisational issues must be considered in a large extent if a greater deployment of ITS is to be achieved. These issues that could hinder deployment of ITS are related to different aspects. Product liability is an important one as some ITS systems could have an impact on safety as inappropriate information can affect the behaviour of users. The lack of co-operation between public and private organisations at national or European level is also an important threat leading to an absence of data sharing or incompatible systems for data exchange. For instance, the project INFOTEN (Telematics Applications Programme) which aims at developing multimodal information systems has highlighted the difficulty to develop common strategies for the access of information and to develop homogenous formats for in formation exchange. Most of the organisations (public or private) insisted to keep their proprietary interfaces to safeguard their investments. For private sector in transport, information is also seen as a commercial tool for attracting customers: a good example is given by airline and railways companies that have created their own systems for serving the travel agencies and reinforcing their competition (e.g., AMADEUS[3], GALILEO[4], SABRE[5]). Another important threat relates to the lack of proper European regulation to protect traveller's privacy or to support common enforcement mechanisms. Actually, there is no consistent enforcement regulation throughout Europe: each country is using is own evidence system for enforcement and an evidence collected in a country cannot be necessarily used in another country for prosecution.

On the technical side, the threats relates to the feasibility and acceptance of new technology used by a system but also the interoperability of different systems, already implemented (legacy systems) or about to be implemented. Lack of harmonisation, not to say standards, causes delays in the deployment of systems. It also appears that high maintenance costs and rapid obsolescence of infrastructures can endanger ITS deployment. For example KAREN must take into account the legacy issues if it wants to sell its results to the European stakeholders while this problem was not so important in USA where a more green-field approach could be used. At last, some threats highlighted the fact that some modelling tools are still lacking especially for demand and incident management.

On the financial side, an important threat comes from a lack of funds to support the ITS deployment and from a poor pay-back of certain ITS systems, sometimes due to their specific geographic

[3] AMADEUS is a central Global Travel Distribution System own by Air France, Continental, Iberia and Lufthansa

[4] GALILEO is a competing system created by Brtitish Airways, Alitalia, KLM, Swissair, Olympic Airways,United Airlines.

[5] SABRE is a third competing system created by US Companies

coverage, making the market not attractive for investors. It is also clear that absence of co-operation between owners of ITS systems may lead to a spread of investments in independent systems without exploiting the high potential synergy offered by Telematics solutions. For example, to avoid this situation of spread of investments, TEGARON and MANNESMANN Autocom, two competitors in Germany for the provision of ITS services, funded together a common infrastructure for the collection of data. Their competition is done at the customer service level. A similar strategy has been used in Japan where Industry and Public sector have developed a common infrastructure for data collection, processing and distribution (VICS): the competition is in this case limited at the individual equipment level (variety of on-board systems).

Social issues are important to consider as users (either public authorities, public or private operators or private end-users) will only invest in and use ITS if they are fully informed about ITS benefits and if they have realised they will gain sufficient advantages out of it. This supposes that quality of service is high and affordable. For instance, in UK a private service has been developed that aims to provide a more effective control for fleet owners through knowledge of precise vehicle location and condition and increases security. This leads to improved business performance and customer satisfaction that can justify their investments in the system. Another threat is due to the absence of skilled staff to develop and use ITS, especially at the regional and local authority level.

Finally, the KAREN Framework Architecture itself may fail its purpose in practise, especially if the promotion and presentation of results is done in an inappropriate manner. Stakeholder may refuse to use it as they cannot see the benefits of such an approach that may be considered as too “theoretical” or they find it too expensive to adopt. Industries can also perceive it as too constraining and obstructing new developments. This concern was already raised at the first KAREN Permanent Consultation Group where a public authority representative gave the warning that KAREN should not end-up in a theoretical exercise with minor or no relations to real conditions.

6.2 Summary of the Threats according to their Category

Each threat is allocated to one of the categories defined by the RAID Project. Hence the analysis of the contents refers to these categories. For a full description of the threats and their consequences as well as other information about them, see annex 2.

- In the **Framework Architecture** category the main concern is that KAREN results may not cover all existing transport policies and that they may not be possible to integrate new transport management policies or ITS systems. This may result in a decrease of acceptance of the Framework and/or may not be useful for the intended purpose in the future. Some countries are developing a complementary approach to KAREN for a national architecture (France, the Netherlands, Sweden, etc.) while others are not: this might result in incompatible solutions on the architecture level and this may increase the differences between countries concerning the speed of ITS deployment.

- The main threats found in the **Communication** category originate from a lack of coverage of communication methods with a possible outcome that some ITS services may not be available in some geographical areas. It also appears that a number of differing communications technologies and standards may be used across Europe to transfer data between the vehicles and the roadside. The organisation of the communication network is also important: FM radios can be public or private. The data resources available on FM carriers have different status according to national regulations: they can be a property of the broadcaster that can be utilised only for certain purpose or they can be considered as additional “communication resources” that can be let or sold to third parties.

- **Cost Benefit** is an important aspect of ITS deployment. There is a concern about the general under-utilisation of ITS due to lack of finance to support its deployment or due to the lack of awareness of the public.

- Under the category **Deployment & Operation,** the most important threats come from the lack of high-quality and comprehensive data (including data coming from probe vehicles). As in the current situation, data sources are mostly under the control of public authorities, competition between operators is not based on the quality of data provided to the public. At this initial stage of ITS deployment, a solution could be to include quality indicators in the provision of information. This would ensure that quality value services are provided, hence allowing the market to develop. Once the market developed, alternative data sources can be used by the service providers as a mean to increase the quality and scope of the service provided. Another important aspect may be the lack of skilled workers to develop and maintain ITS systems.

- In the **Funding Provision** category, the main threat is that national and private funds may not be sufficient to cover the implementation of all services covered by the KAREN Framework Architecture. Funds that are available from the European sources should be used to encourage national and private organisations to invest and fill the gaps.

- The main threat in the **ITS Infrastructure** category is that high maintenance costs of the required infrastructure may prevent the introduction of new ITS technologies. This will be because the initial capital investment cannot be recovered. Hence the maintenance costs may use up an important part of the available investment sum for ITS. Another threat is linked to the rapid way in which infrastructures become obsolete; as the technologies supporting ITS systems (e.g. in the field of telecommunications) evolve quickly.

- Problems linked to **Legacy** are important. Investments have been made in existing systems and migrating to new system solutions is not always possible. A rigid regulation could also lead to the rejection or postponement of new ITS systems.

- Several serious threats were found for the category **Organisation and Institutional issues**. They may result in a situation, in which the ITS businesses do not develop in the desired manner and that the quality of service is poor in some areas. This can be due to improper private-public partnership, lack of collaboration between member states, lack of common European regulation and an unwillingness for data sharing between public and private organisations. To complement this, the threat was identified in the **Politics** category that important changes in the political context of a region or country can sometimes lead to the suppression of the political support to ITS deployment initiatives.

- Threats in the **Privacy** category raised concerns about the use of data collected by ITS systems. The Commission has issued a directive on data protection in October 98. Member States are bound by the objectives of this directive but have a certain freedom for the adoption of national regulations or the evolution of the existing regulations. Even with the existence of laws, travellers may be concerned about the misuse of personal data (e.g. tracking of the movements of travellers) and thus be reluctant to use some of the ITS systems.

- In the category of **Safety**, threats related to the use of non safety-compliant systems are highlighted. Improper human machine interface is one of the important issues. Safety decrease is not acceptable and dedicated safety analysis has to be conducted for all systems, not only those that directly influence vehicles. It should be noted that driver behaviour changes by the availability of certain systems, either giving them a false sense of safety, making them dependent on the system or overloading them with too many complicated systems and too much information.

Another threat deals with the difficulty to have immediate detection of incidents and to know where incidents can occur, reducing the effect of strategies devised to reduce their consequences.

- In the **Stakeholder Acceptance** category several severe threats were defined. The lack of co-operation between stakeholders and their poor acceptance of some ITS solutions due to safety and financial aspects are among the most important. Co-operation and understanding between all the partners involved is required to achieve the goals of ITS. A failure of this communication, on any level, could result in ITS not being as beneficial and widely used as predicted.

- The **Standardisation** category includes a high number of threats. Their general point is that European harmonisation seems not only necessary for technical but also for non-technical issues such as common operational rules, harmonisation of human-machine interfaces and administration. Possible results, if such a harmonisation is not achieved, would be a loss of market shares for European industry, a delay of the deployment of ITS systems, the delay or prevention of the implementation of some of the Framework Architecture's functions and the interruption of already deployed services. Compatibility of ITS systems is one important issue at stake.

- The category of **Technological Maturity** provides the largest number of threats. The main threats are that the technology needed by the services related to automatic vehicle operations will not be available, will be too expensive, or will have insufficient reliability, at least in the short term. It also appears that viable demand and incident management tools rely on complex technology that does not exist and may be very costly to develop.

- **Traveller Acceptance** is also an important category and holds several critical threats. High quality services must be given at no or reasonable costs and be easily accessible by travellers, especially those using public transport. Continuity of service must also be ensured and travellers must be able to use all the information that is available throughout their trips. The public needs to be informed through advertising of the ITS services that are available and of the benefits that they can provide.

The complete list of threats grouped by category is given in Annex 2C.

6.3 Scenario Based

6.3.1 Scenario definition

A scenario definition is used to cluster and classify risks included in the database according to the environment in which they are relevant and for which the recommended mitigation strategies are suitable. The scenarios are built on four types of elements:

- Time horizon

The risk can be time related (long, medium or short term) or time independent.

- Public-Private Co-operation

ITS (or just a specific service) development can be completely driven by the public sector or by the private sector alone or by a mix of both.

- Main ITS trends

In some cases it is also useful to distinguish between the possible main trends for ITS development that are modelled in RAID by means of the scenario element called „Main ITS trends". Those include:

  - ITS strategies focused on the provision of Telematics infrastructures to improve the efficiency and the safety of the transport network (Control);
  - ITS strategies aimed at using Telematics applications for traffic Demand Management (Demand Management);
  - ITS strategy focused on the use of Telematics for disseminating real-time multimodal and multimedia information to both end-users and operators/authorities/police (Information);
  - A combination of the three above.

- Geographical extension

At this high level of analysis, when looking at ITS deployment risks it does not seem relevant to distinguish between the three different geographical extensions. Therefore, this element is left out in the analysis.

As a conclusion of the RAID analysis, 10 „basic reference scenarios" were defined; five time related and five time independent scenarios. Those are described in the following tables. The full process leading to these reference scenarios is presented in Annex 2C.

By looking at the number of threats of the RAID database mapped to each basic reference scenario, it appears that only one threat is associated to scenarios S2.1 (Medium Term perspective for the public sector only driving the development of ITS) and S3.1 (Short Term perspective for public sector only driving the development of ITS*)*. Of course it does not mean that these two scenarios represent two ideal "risk free" environments for ITS development. On the contrary it highlights areas where there is a lack of information and potential for improvements in the database. The consultation phases, that will follow the issue of this first version of the database, will have to be focused on these two areas in order to complete them with a more comprehensive view of the possible ITS deployment constraints.

6.3.2 Analysis of the time related threats

BASIC SCENARIO S1: Long term Time Horizon

The main focus of the threats, mapped in the long-term scenario is on the ability to implement and maintain technological advancements at a standard high enough to meet the public's requirements. The threats involve a new piece of equipment and the problems involved in its use or acceptance by the public. The consequences of the threats are a decreased driver safety or reluctance by the public to use the new equipment technology. This is a general threat occurring at the introduction of any kind of new technology which can not be avoided but the design of the new technologies has to respect this threat so that dangerous consequences are avoided.

BASIC SCENARIO S2.1: Medium Term perspective for the public sector only driving the development of ITS

The medium term threat involves the public's acceptance of automatic operation functionality. The low-penetration of interdependent systems may decrease their potentials, leading to low acceptance of the system by the public.

BASIC SCENARIO S2.2: Medium Term perspective with the private sector involved in the ITS development

The threats focus on the restrictions, in both expense and implementation, of new technologies and their acceptance and use by the public. There is a possibility that the public has too high expectations of the systems or overestimates its effects. They also outline some issues dealing with the widespread use of ITS technology both in a geographical sense as well as according to the types of vehicles involved. The overall consequences are that the expected benefits of the systems may not be achieved which may lead to uncertainty in the use of the system or a decrease in driver safety. It is important to be aware of the development stage of new technologies so that implementation is not done pre-maturely causing problems in the systems. This could lead to a decrease in the safety or effectiveness perception of the users and finally to the not fully or optimal development of the system.

BASIC SCENARIO S3.1: Short Term perspective for public sector only driving the development of ITS

The scenario includes only one threat which relates to the possibility of inconsistency of policies within the European Union Member countries which will lead to a hindrance of the ITS services.

BASIC SCENARIO S3.2: Short Term perspective with the private sector involved in the ITS development

The threats identified in this scenario are related to the current information systems used in the European Union member countries. They highlight that the current data compatibility is unknown and the possibility of short-term standardisation of the different systems is also questionable. Therefore an inconsistency across Europe may exist and integrating these systems, making them interoperable, may not be possible in the short term.

6.3.3 Analysis of the time independent threats

BASIC SCENARIO S4.1: Private sector involved in the ITS development mainly for demand management purposes

The threats included in the scenario mostly deal with data collection constraints, lack of appropriate sensors or their inability to collect the appropriate data, and the maintenance of the infrastructure. These concerns may lead to data collection schemes that are unreliable and not cost effective. Another issue is that the lack of data collection legislation as well as individual traveller's concerns regarding data collection may hamper the standardisation of the data collection and traffic management systems. It is also recognised that co-operation is required within the EU as well as between public and private partners.

BASIC SCENARIO S4.2: Private sector involved in ITS development mainly for Control purposes

A large portion of the threats included in this section deal with lack of consistency and co-operation in many facets: across borders within the European Union, between private and public parties, and between old and new systems and their implementation. Regulations and specific interests vary within all of these relationships impeding the use of ITS systems. Lack of quality data as well as its monitoring is tied in with lack of available reliable and cost effective sensors. It can be expected that the market for this will be influenced by larger demand of data collection modules and that thereby the consequences of threats will be minimised. Basic research results of recent programs show the possibility for dedicated detection equipment. The research activities should concentrate on the technological maturity.

BASIC SCENARIO S4.3: Private sector involved in the ITS development mainly for real-time information provision

These threats involve the inability to provide appropriate ITS information due to cost constraints, lack of information sources or an undesirable end user reaction. They also highlight a fear of not meeting European needs due to lack of co-operation between involved parties, insufficient output data quality, lack of common data formats or location coding structures or simply due to the complexity of standardising and integrating such a system. It can be pointed out that homogeneous technological solutions are needed and that the access of information should be eased in a strategic sense.

BASIC SCENARIO S5.1: Public sector only driving the ITS development mainly for demand management purposes

These threats concern the acceptance of new systems by the public and the lack of desired effect of ITS. The maintenance of required infrastructure and the cost and complexity of implementing systems, both locally and throughout the European Union, are also addressed. Additionally it has to be pointed out that among the European regions a consensus on strategies for demand management has not yet been achieved. Therefore the consequences of the threats of the application of ITS have to be set into this strategic context.

BASIC SCENARIO S5.2: Public sector only driving the ITS development mainly for traffic control purposes

The majority of the threats in this scenario concern the lack of consistency throughout the European Union in regard to regulation enforcement, road labelling and road fee collection. Lack of a standardised system could lead to confusion of the user or a lack of further development due to its limited acceptance. There is a strong need for the information to be distributed in a homogeneous or compatible manner because it will be unacceptable and confusing to drivers making long, multi-national journeys to need to apply several different systems or to be confronted with different representations of information or different measures.

The complete list of threats grouped by strategy scenario is given in Annex 2C. The reader can also find in this annex the statistical evaluation of the threats identified by RAID.

7. MITIGATION STRATEGIES

As described previously, having defined the Risks, the next aim of the Study has been the definition of Mitigation Strategies. These are designed to counteract the impacts of the threats defined by the work in Phase 1. The work in Phase 2 has produced strategies for threats that have been rated RED and ORANGE by the work in Phase 1. These threats are shown in Annex 2C and the corresponding detailed strategies are reported in this section.

This section provides a synthesis of the mitigation strategies by identifying a few key high level strategies and their main actors. They have been produced as a result of a more detailed analysis of the strategies. This analysis was carried out by reviewing and consolidating a first version of the strategies through a consultation process initiated in Phase 2. This process has been continued in the Phase 3 of the study to transform the draft mitigation strategies into "recommendations".

Threat Category	**Overall Mitigation Strategies** (subsection number)											
	7.1	**7.2**	**7.3**	**7.4**	**7.5**	**7.6**	**7.7**	**7.8**	**7.9**	**7.10**	**7.11**	**7.12**
Framework Architecture	**X**											
Communication		X	X								**X**	
Cost Benefit				**X**								
Deployment & Operation		X	X		X			X	X		X	
Funding Provision				X							X	X
ITS Infrastructure								X				**X**
Legacy	**X**											
Organisation and Institutional Issues			**X**		**X**				**X**			
Politics			X	**X**	X							
Privacy										**X**		
Safety		X				**X**		X			X	
Stakeholder Acceptance				X	X				X			
Standardisation		**X**										
Technological. Maturity						**X**	**X**	**X**				
Traveller Acceptance			X	X		X	X					

Figure 7.1 Relationship of Overall Strategies to Threat Categories

In most cases each overall strategy covers more than one threat category and involves more than one of the actors identified. The way in which the categories are covered by the strategies is shown in the above table (shaded cells indicates the main categories addressed by the strategies).

Each high level strategy identifies main actor actors that need to be involved in their implementation. However it is possible that some or all of the remaining actors will also be involved in strategy implementation in some way or other. The main actors to whom the recommended overall strategies are primarily addressed comprise a European Authority, Public Authorities, Private Industry and the KAREN Project.

In the following sections, each overall strategy description is accompanied by the overall risks specifically addressed. The strategy is briefly presented with its main components and **key actors** in bold and then developed taking into consideration the national particularities if relevant and the potential key actors involved. A commentary paragraph aiming at clarifying the characteristics of the strategy is then added.

7.1 Support of Transport Policies and development of new information Society products and services

Risks: The KAREN Framework Architecture will not include the facilities needed to support all current European road transport policies and the ITS services that are currently emerging from public and private sectors, particularly information services. It will also not be capable of accommodating facilities needed to provide products and services that will be developed in the future.

Mitigation Strategy:

- In KAREN deployment plan: **KAREN** Framework Architecture to include existing systems and propose cost effective migrations schemes.
- National architectures to relay KAREN : initiatives to be taken by **National** or **Local authorities or ITS national organisations** encouraged by **European Authorities**.
- Create an expert group in charge of maintaining the Framework Architecture and take into account the evolution of user needs (**European Commission with Standardisation bodies**).

The KAREN Framework Architecture must endeavour to include facilities provided by currently deployed systems, including existing commercial services if they are able to evolve towards European interoperable services. Where this is not practically possible, the Architecture must clearly show in its deployment plan how it is possible to make systems compatible. The migration strategies that are proposed to achieve compatibility must be easy and cost-effective to implement.

The KAREN Framework Architecture provides a reference for developing ITS systems architecture. It has been made clear that for taking into account national transport policies that may differ from a country to another and legacy systems, it is very helpful if national architectures are developed in order to complement the KAREN approach.

In this process KAREN and the deployment of the KAREN Framework Architecture play a fundamental role as most of the national initiatives aim at defining the national architecture for ITS. It is important that they are compliant with the European Framework Architecture and reversibly that the European Framework Architecture is continuously updated to take into accounts the peculiarities specified at the national level.

Such initiatives have been launched in several countries, directly by Ministries in charge of Transport sector (The Netherlands, France and Sweden) or by groups of organisations directly concerned: mirror group of KAREN in Italy, working group from ITS Focus in UK.

During the interviews conducted as part of Phase 3, it was generally admitted that the KAREN results will be useable only if such national initiatives are developing. Then, a support from EC or other authorities for initiating such actions at the national level should be encouraged. This could be by financial support or other type of support as benefits will be shared between national and European levels.

The continuous evolution of user needs, the rapid development of new services and the likely evolution of European transport policies necessitates that the KAREN framework architecture is verified from time to time and up-dated in order to cope with these evolutions. To achieve this objective, an expert group, including members from public sector, industry, users should be created. It will be in charge of

discussing and proposing modifications and changes needed to keep the framework architecture up-to-date.

Comments: This strategy principally addresses the threats that are in the **Framework Architecture** and **Legacy** categories. The KAREN Framework Architecture will be based upon the KAREN User Needs that the Project will produce. The Architecture will include functionality to meet these User Needs which will include requirements relating to existing transport policies in the European Member States. Where appropriate this functionality will be based on that which has already been created for existing systems - often called "legacy" systems. What is and is not appropriate will depend upon the relationship between the ITS services offered by the existing systems and the KAREN User Needs. KAREN will produce suggestions for migration strategies to enable the migration of those existing systems that do not conform to the KAREN Architecture. It will need to be emphasised in the KAREN deliverable that the migration process does not necessarily mean "replacement". It may include "enhancement", or "upgrade" either of which may be cheaper or more cost effective solutions. Thus for example an existing system my only require the addition of an extra interface to enable it to communicate with other (possibly new) systems that conform to the KAREN Architecture.

7.2 Standards, technical and non technical harmonisation

Risks: Failure to approve and implement standards that apply to Europe, in the appropriate time window, may mean that any standards that are created do not take full account of European needs. It will then be more difficult to obtain systems to provide ITS services from suppliers that do not have Europe as one of their business areas. And there is a risk that ITS services will not be accessible everywhere with the same device for European travellers. Though not requiring formal standards, some ITS services need a certain level of harmonisation at technical or non technical levels (procedural, contractual, legal) in order to facilitate the market development.

Mitigation Strategy:

- Establish a strategic plan: **European Commission** to act, based on findings from M 270, phase 1[6] and other inputs.
- Encourage actions for quick harmonisation at the appropriate level in order to ensure interoperability: set-up task forces, working groups **under umbrella organisations** with the support of the **European Commission**. Priority items : , enforcement, after-theft systems and electronic fee collection.
- Develop harmonisation of key features of ITS services when beneficial for users acceptance, market penetration and global benefits : expert groups based on the results of current R&D projects (**European Commission**).
- **European Commission** to support actively formal standards only if and when there is a common European benefit: in this case use of the Unique Acceptance procedure[7] and/or supporting actions (e.g.: ISIS programme).
- Develop migration paths (specific projects from **industry, operators**, concerted actions launched by the **European Commission**) for offering temporary interoperable solutions.
- Develop mutual recognition of conformance checking mechanisms undertaken at national level for key standards necessary for ensuring compatibility and interoperability of key systems**. (European Commission with Standardisation bodies**)
- Prepare the revision of the current standardisation procedures (**European Commission**).

Participation in European and International standards activities must be reinforced and particularly better organised in a strategic way. This active participation must cover non-technical areas such as the quality of data and ITS services, operational rules and administrative plans.

[6] M270 : mandate forwarded by EC to the European standardisation bodies, with the objective in phase 1, of evaluating the global situation on RTTT (Road Transport and Traffic Telematics) standardisation. Phase 2 is the elaboration of a revised work programme.

[7] Unique Acceptance procedure: Procedure that can be applied to any type of document in order to achieve rapid approval of an EN (European Standard) or HD (Harmonisation Document), if it is reasonable to suppose that the document is acceptable at the European level (in CEN/CENELEC Internal Regulations, Art 4.6 Edition 1994-03)

Developments of standard are required where appropriate: support of EC should focus on the standards where the best collective benefits can be expected. It is then necessary to compare the efforts for EU harmonisation to the real collective benefits. Standards development procedures are generally considered as time consuming and slow. Where priorities have been identified, the standardisation process should be accelerated. Several means have been identified for this purpose: the unique acceptance procedure, specific mandates given to CEN or specific projects such as those undertaken in the ISIS programme.

There is a consensus among consulted stakeholders that standardisation process is too complex and not really necessary in all domains. In that context the Vienna agreement[8] appears to be more an obstacle than a facilitator for solving the problems in a short-term horizon. The main reason is that for some key topics the debates have to be brought at ISO level, involving more experts and leading in general to more competing issues. It is then recommended to encourage when appropriate creation of fora where interest parties can try to reach an agreement in a limited time frame (examples of WAP and GATS fora).

The former recommendations can be put into operation within the existing standardisation procedures. Another way, likely to be more difficult to implement quickly, should be to revise the current CEN procedures and adopt a simplified and more responsive mechanism. The following topics have been identified in a first approach as requiring EC intervention. This intervention could be of different nature according to the topic:

- Concerning in-vehicle HMI, there is a need for clear guidelines that should be established at the European level. This need is clearly expressed by automotive industry and equipment suppliers. UK has already issued a code of practice but its real usage seems questionable. After the issue of the European Statement of Principles on Human machine Interface for In-Vehicle Information and Communication Systems [15] a task force has worked under the auspices of European Commission (CONVERGE project) and produced a report [16] in order to expand each of the principle and so facilitate their implementation. This work needs to receive acceptance from automotive industry and equipment suppliers..

- The continuation of standardisation for data exchange at international level when appropriate is required but national systems have to be taken into consideration. Extension to cover multimodal information is necessary.

- After theft systems are in development in many countries. Standardisation and interoperability are crucial there: by definition, their efficiency relies on the interoperability and coverage within the whole Europe.

- Enforcement of regulations is also a topic where harmonisation of procedures is necessary. Today the lack of mutual recognition of evidences concerning traffic law infringements between countries

[8] Agreement between ISO and CEN in order to avoid duplication of effort : for each WG area, one of the corresponding WGs (ISO or CEN) has been given the leading role. When CEN has been given this role, the ISO convenor is European and the CEN/WG is open to non-European experts. When ISO has been given the leading role, European experts participate as CEN members are also ISO members. Work items that are not common to the two workplans are pursued within the original organsiations.

jeopardises the efficiency of new ITS services like dynamic speed control, electronic fee collection, ... This work has started within the VERA[9] project and should continue.

- In the domain of Electronic Fee Collection, though not a priority for some countries, many efforts and actions have been undertaken at the European level and should continue: current R&D projects are producing recommendations aiming at ensuring interoperability of EFC systems and related applications such as enforcement, classification, etc. CARDME concerted action is working for designing migration paths towards a common European EFC, taking into account existing systems and besides national implementation such as TIS in France, some Euro-regional projects have started implementation of cross border services

These priorities are suggestions that need to be validated. A strategic plan involving EC, standardisation bodies and European organisations needs to be established and then, several types of actions should be undertaken according to priorities:

- forming task forces, working groups, for clarifying quicker the various positions in new domains that have to be investigated, for examining de-facto standards and prepare the work that will serve as inputs to the standardisation process

- developing more quickly standards where necessary using the Unique Acceptance procedure when feasible and pursuing some accompanying actions (e.g. pursuing DG 3 actions : ISIS program[10])

In parallel, develop migration paths from existing systems to European interoperable systems (e.g.: CARDME for EFC domain) with the objective of offering temporary partial interoperable solutions allowing payback of legacy systems. This is one of the major expected result from KAREN project: the framework architecture will be designed according to existing systems and their potential migration.

Comments: This strategy mainly addresses threats in the **Standardisation** category. However it also will have a minor impact on threats in the **Communication**, **Deployment & Operation** and **Safety** categories. The "reinforcement" required by the strategy can be achieved by providing sponsorship of activities to create, review and harmonise standards. Strong emphasis must be placed on HMI because its harmonisation will make it easier for travellers to make use of and gain the maximum benefit from ITS. It is also important that for in-vehicle HMI key features are harmonised for the sake of safety and a better understanding by users : nobody can imagine that taking account of aestheticism considerations warning messages should appear in green on the on-board display…This work is being carried by an ISO Working Group, in which there is European participation to try and ensure that any resulting standards are to the benefit of European users and industry. However at the moment this work is concentrated on the in-vehicle interfaces and the need to look at other interfaces such as those for traveller information must be explored. A report has been issued in July 98 by ADAC, the German automobile-club, presenting recommendations for ensuring interoperability of the infrastructure on the TERN-Network. Similar work could be undertaken, focusing on ITS applications,

[9] VERA (Video Enforcement for Road Authorities) : 4th FP project which aims at examine harmonised approaches to the enforcement of traffic laws and to promote the acceptance of video records as evidence in court

[10] ISIS is a specific program launched by DG3, aiming at speeding up the standardisation process by financing dedicated projects on targeted topics. Two projects are currently dealing with ITS.

involving the same actors as user representatives and industry. It may need to be carried out as a CEN activity our out of the standardisation process in order to be more effective, as there may be little scope for its application elsewhere in the World.

In other areas such as data exchange, there is some activity, both within Europe and internationally. These activities need to be followed-up in order to address urgent problems such as exchanges between urban and interurban and multimodal. They also need to be extended to cover the quality of data and related criteria (see data exchange section 7.3.).

In many countries, traffic management systems are in place and exchange of information between parties in operation (France, UK, Germany, etc.). National standards are existing and facilitate these national deployments.. However, exchanges between neighbouring countries with high level of cross border traffic are still limited though needed. In addition, exchanges between cities and interurban networks are a major concern in most of the countries.

For digital maps, and location referencing, there is no clear need from the infrastructure operator point of view as conversion tables can be used easily.

In this field of standardisation, it is worth to mention that CEN 278 has undertaken a specific action (mandate M270) which is to prepare reorientation of the priorities for European standardisation. The first phase, “evaluation of the global situation” will be achieved in May 99. A second phase will lead to define a strategic plan for standardisation activities.

7.3 Data Exchange

Risks: There is no commitment or willingness on the part of EU Member States to use Telematics to exchange data about cross-border traffic rather than traditional data exchange systems. This will reduce the amount of data available for use by some ITS services and jeopardise the efficiency and benefits arising from their deployment.

Mitigation Strategy:

- Extension of the MoU on data exchange in order to incorporate rules for the format of data and the quality criteria indicators for the data sources. (**Member States** and organisations who have currently signed the DATEX MoU to support this activity with the help of DATEX-GO task force)

- Set-up a specific body (with data administrator role) in charge of defining and maintaining the description of the data formats and the data quality indicators and of keeping the reference European data base and providing assistance. (**Member States and European Commission**)

Recommendations must be produced to actively encourage the use of a contractual framework to make sure that data exchanges are taking place between neighbouring countries. The data exchanged must be of high quality and able to provide continuity of ITS services across national borders within the Community for travellers using all modes of transport.

Examples and models should be provided in order to help organisations that would like to enter in the data exchange network. Models could be developed at various levels, (European, National and local levels) according to the characteristics of the service. Following the examples currently in use for specific applications (e.g. RDS-TMC), those organisations which would like to join the data exchange network should be required to accept and sign a Memorandum of Understanding. Such a Memorandum of Understanding, as a minimum, defines a set of rules for the format of data, the quality criteria for the data exchanged and offered and the "data administrator" in charge of maintaining the description of the data formats and quality criteria according to the evolution of standards. This administrator may also maintain the basic data necessary for the data exchange (e.g. European level location coding database). Updates and upgrades of the database would be provided regularly to all the members of the data exchange network. In other words, by adopting this scheme, new organisations that would like to join the data exchange network will receive support from the administrator.. The all process could be included as a specific part of the organisational level in the KAREN Framework Architecture.

Roaming rules as well as right and obligations of the members offering the same kind of service should be established at the level of "memorandum of understanding" as the capability of offering continuity of the services is a key requirement for existence of a data exchange network. These rules should be compliant with subsidiary principles in order to be largely accepted.

Comments: This strategy primarily addresses threats in the **Organisational and Institutional Issues** category. However it also covers the threats in the **Communications**, **Deployment & Operations**, **Politics** and **Traveller Acceptance** categories. A contractual framework could be established using the DATEX Memorandum of Understanding (MoU) or a similar instrument. This type of MoU would bind those signing to use a communications specification (e.g. DATEX-Net) when exchanging traffic and travel data or information. Those signing would also have to conform to certain requirements covering access, file transfer, management of background information, message management, plus a defined set of rights and obligations. But it is worth mentioning that this MoU does

not imply that any kind of criteria concerning the service offered to the final user have to be imposed : this should be eventually let to the bilateral agreements, in order for example to ensure compliance with specific transport policies. It is important that the service provider keeps a large degree of freedom for the definition of the service, in order to encourage competition. An example of actual deployment is given in Europe by the CORVETTE project that is an interregional bilateral and multilateral implementation project. It is sponsored by the European Commission as part of the TEN-T Programme. Starting from the summer 1996 and lasting for three years CORVETTE has provided the co-ordination platform for the harmonisation of Road Transport Telematics services through the Alps involving Italy, Germany, Austria and Switzerland. Partners involved focused their effort on the enhancement of traffic monitoring and data collection and on the implementation of the international data exchange network between TIC/TCC (DATEX). During the same period the INFOTEN project (TAP research project sponsored by DGXIII) has demonstrated the technical and organisational feasibility of cross-border multimodal information service. It is likely that it will be deployed by the next phases of CORVETTE. Other pilot projects are developing the same data exchange agreements: SERTI, CENTRICO, VIKING, ARTS, etc.)

7.4 Promotion of ITS and education

Risks: There is a continued lack of general advertising devoted to the facilities and benefits provided by ITS services. This means that ITS services fail to deliver the expected benefits because travellers do not know of their existence or understand what they can provide or because authorities, infrastructure operators, etc. do not know all the potentialities offered by ITS services.

Mitigation Strategy:

- **European Commission** to prepare communication strategies on ITS
- Organisations such as **ERTICO, POLIS, UITP, ACEA** at European level, **ITS organisations** at national level to reinforce promotion of ITS benefits and particularly prepare basic material for promotional actions: European ITS handbook for example.
- **Automobile associations, insurance companies** to relay the information to their members (magazines, reports, tests of products, etc.)
- Use of public events as window for ITS technologies (**National authorities and EC**)
- Development of ITS courses in education programs. (**National education authorities**)
- Development of ITS courses for retraining of professional people **(All actors**)

ERTICO and POLIS, at the European level, and similar organisations, at a national level, should co-operate with the **European Authorities** in a concerted promotion of the benefits and limitations of ITS. The aim should be to increase the demand for this type of system and ITS services, thus reducing their deployment and operational costs. The benefits should be summarised as providing more efficient and cheaper road transport that will reduce pollution and in some cases save lives.

For implementing this strategy, it seems necessary to differentiate between at least, three targets: final users, intermediate users of ITS and Political level

✓ Final users :

For marketable ITS products it is to the industrial/service operators to sell their products. However there could be collective actions from the industries in the same sector. For not easily marketable products (most of benefits are collective, e.g. safety, efficiency), promotion should be encouraged by public sector or associative sector, or indirect beneficiaries. .

- in countries where Automobile associations are powerful and have an ancient traditional activity for informing their members, (Northern countries) promotion of ITS is already made through subscribers magazines, mailings, etc.

- in countries where Automobile associations are less present (Latin countries in particular), same promotion activities can be undertaken by insurance companies that are now developing lot of services for drivers.

On priority topics, incentives could be given at the European level for developing this promotion at national level. Basic material should be available at the European level, which could be adapted by national communication support. Harmonisation is not necessary, even not desirable as communication

relies mostly on cultural background in the different countries. However, addressing common topics at the same time in different countries, during holidays for example should reinforce the impact of the national promotion measures. In any case it is important to have the support of communication consultant (ITS promotion appear very frequently to be nowadays prepared by non-professionals).

Other ideas can be developed such as promoting ITS events among the public. Dedicating some time during the World congress or other ITS congresses to public sessions with media should be examined (this is already done for Exhibition but seems to have limited impact due to the lack of public promotion). Public events where ITS are implemented for facilitating transport could be used as a window for ITS promotion: Olympic Games in Nagano, World Skiing Championship in Sestriere, ARENA project in NL, etc.

✓ For intermediate users, there is a clear necessity to develop :

- guidelines, toolbox for implementation demonstrating the potential benefits (good example provided by ITS Pioneer)

- case studies reports (proof by example).

- European ITS handbook: Japan has produced such a document and PIARC[11] (C16 Committee) has produced an ITS handbook for less developed countries and economies in transition.

But these tools remain inefficient if not translated and adapted to national, local levels: most of local transport and traffic managers are not English speakers and are not even familiar with the "ITS jargon". This activity is to be undertaken at the national level by authorities and ITS groups/organisations. European authorities could propose a mechanism and support some R&TD projects in the support action domain of the 5th FP.

✓ Political level: at this level, there is a long tradition of lobbying by automobile associations. They represent in fact numbers of electors and can make pressure on the political power. In other countries, where these association are less present the ITS dedicated groups can play this role, but not representing electors, they are by definition less powerful.

In promotion activities for ITS, KAREN results play an important role as the Framework Architecture should be a support for the deployment and development of ITS services. Consequently it is recommended that KAREN recommends a dissemination programme capable of providing high quality means for dissemination to make European stakeholders aware and updated about KAREN results.

Promotion of ITS can also be achieved through the education and training programs. Several countries have started specific training courses on ITS. These initiatives should be encouraged in other countries and exchange of students between countries could activate the ITS technique penetration in Europe.

Retraining of professional people is also a major issue due to the fast evolution of techniques. Training sessions are already organised at national level by private or public organisations. Programs at European levels have also been organised by supporting specific ad-hoc projects. It is worth mentioning that US have organised a specific program on ITS architecture with regular courses. This program appears successful in terms of attendees and similar initiative could be organised in Europe.

[11] Permanent International Asssociation of Road Congress

Comments: In some European countries (e.g. The Netherlands, U.K., France, Italy) national ITS initiatives have started with different purposes but all including promotion and harmonisation of ITS applications throughout their country

In general, most promotional effort for the moment is targeting top professional users. More must be done to inform public authorities at local level. This can be done for instance through education programmes proposed by national authorities or national ITS organisations (e.g. ITS Netherlands, ITS France, etc.).

Concerning the promotion of ITS among non-professional users, more broadcast programmes advertising or informing on ITS should be used. For instance ITS could be presented during popular science programme or be featured in television series (use ITS-equipped vehicles when showing police, fire, ambulance...). Even for marketable products, common actions between industrials could be undertaken (an example is given by milk products in France that are promoted by a union of milk producers with collective advertising, in this case sponsorship is likely to be obtained in the mean time by authorities). To achieve this, there is definitely a need to use communication experts to bridge the gap between the ITS community and the television world to ensure that ITS applications are featured in the programs. Promotion should also be done during events such as motor shows or through national or specific press such as journals of national motoring clubs. In this case, national automobile clubs and national car manufacturers associations should play a role.

In addition to promotion and education activities aimed at re-training professionals, also the introduction of the ITS subject in the formal training (i.e. university) should be favoured. The example should be taken from the training courses that are already organised in some countries:

Italy: From the year 1998 in the engineering faculty at the "Politecnico di Torino" there is a new sector for Ph.D. students in "Information Technology applied to the Transport sector". The new sector is a joint initiative of the Polytechnic of Torino and Genova.

In France a Master Degree section has been created in ITS and in UK, University de Leeds in association with other universities is developing ITS courses.

7.5 Public Private Partnerships and organisational aspects

Risks: The allocation of roles and responsibilities for the provision of ITS services is the subject of competition by (National and Local) Government agencies, or is simply misunderstood by some or all those involved. This means that providing ITS services becomes a hazardous area of business particularly for the private sector. Some of the actors may be reluctant to introduce permanently the new technology having the feeling of loosing a part of their responsibility.

Mitigation Strategy:

- **European Commission** to set-up task-force/working group for preparing: *"a code of practise for ITS services on traffic management and control including model agreements with service providers" and model contract clauses on data content and accuracy in discussion with the data suppliers and information content provider*
- Enlarge the WELL-TIME study to all relevant ITS services that can be developed through public private partnership : **European Commission**
- Encourage **National** and **Local authorities** in the development of Public Private partnership schemes by demonstrating the achievable benefits.
- Encourage **National** and **Local Authorities** to reorganise their own services in order to benefit from the introduction of new private ITS services

In each European country, the role of Public Authorities and the Private Sector vary enormously. There is a need for Public Authorities to be made aware that involving the private sector in the provision of ITS services can produce benefits. These include risk sharing plus a reduction in the financial burden that Authorities have to bear. Public Authorities should be encouraged to create strong Public-Private Partnerships between themselves and the Private Sector. If needed they should also facilitate the creation of partnerships that only involve members of the Private Sector. In every case the precise roles of each of the partners must be clearly defined and agreed before any partnership is created. In any case, existing business models in other types of activities can be transferred easily to the ITS domain. Adaptation to national rules is necessary in some case. Most important aspects have already been developed in the WELL-TIMED study [11]. Among others, it appears important that:

- *"a code of practise for ITS services on traffic management and control issues should be drawn up (including model agreements with service providers)"*
- *model contract clauses on data content and accuracy should be drawn up in discussion with the data suppliers and information content provider*

However, models for Public/private partnerships should not be limited to "traffic or travel information" services. A more global approach should be undertaken in order to encompass other ITS services like:

- emergency systems
- after-theft and personal security systems
- freight and fleet management

- traffic management

- electronic fee collection

Another important aspects is related to the organisation of the public sector itself. A lesson learnt from the French test site of the In-response project is that the implementation of new facilities for detecting and managing the incident has as main consequence a necessary modification of the current procedures and of the share of tasks between Road operator, Police and Emergency services. Some of the actors have expressed their worries about that and may be reluctant to introduce permanently the new technology having the feeling of loosing a part of their responsibility. The only way to solve this kind of problem is then to:

- Convince the concerned organisations of the rationale of changing the procedures

- Convince authorities to change the rules and/or attributions of the various entities if necessary.

To do so, it is extremely important to have a clear view of the benefits gained and to promote them very actively.

Another example is given with the introduction of Mayday systems based on GSM. The generalisation of a unique emergency phone number (112) necessitates that suitable procedures are implemented in order that in case of emergency the concerned emergency service is activated (problem of location, zone of competence, …..). In addition, systems based on data transmission (call activated by shock sensor for example), necessitate the alert is transmitted without delay to the related public service (police, fire-brigade, …).

For meeting these requirements, public authorities should be encouraged to implement suitable procedures, or even reorganise their services in order to benefit them selves from the new services.

Comments: This strategy primarily addresses the threats in the **Organisational and Institutional Issues** category. However it will also have an impact to a lesser extent on the threats in the **Deployment & Operation**, **Politics** and **Stakeholder Acceptance** categories. The culture, promotion and use of Public-Private Partnerships (PPP's) and the involvement of the Private Sector in ITS activities varies widely across Europe. For example in the UK there is a strong driver to establish PPP's as a means of generating alternative forms of funding, sharing of risk and the provision of better (performance related) services. The generating of alternative funding may involve the use of new or novel methods such as commercial advertising. Whatever method is used it should offer the prospect of innovative procurement methods and sophisticated forms of capital recovery, for example by tolls, fees and different forms of automatic payments. Another advantage of PPP's is that they provide long term commitment. This will encourage the participation of the Private Sector because they can see that there will be a realistic period in which to recover the cost of developing the often-new products and services. However the provision of ITS services entirely by members of the Private Sector should not be ignored, and if necessary should be encouraged by Public Authorities. In this domain, it is important to underline some national particularities:

Some countries have already developed public/private partnership since long time, but on different basis. France developed the "delegation de service public" (delegated management) in the 19th century. The idea is to delegate by contract the provision of basic services (water supply, road infrastructure, etc.) to private companies. It is not privatisation as the facilities remain property of the public domain, but the service is managed on a private basis and is subject to market competition. Since this time, similar forms of delegations have been introduced in other countries.

In the domain of traffic management, this delegation is more recent: it started with toll motorways in Italy, Spain, Portugal, France and Greece where some motorways are built, financed and operated by private consortia (some by public owned companies). Other forms were developed like in UK (DBFO projects) where motorways are built by the private sector that receives annual payment according to traffic and some performance indicators. There is no toll for the driver (shadow toll principle). This type of contract has been extended for maintenance activities on trunk network in UK. The recent TCC project (England) is based on the same principles. The 5T project in Torino which was designed for the management of the transport in the city is built on similar principles and at the end of the contract between the city council and the consortium, the systems will become property of the City council and the Mass transit operator according to a predefined scheme The operating costs saving calculated for the ATM company in Torino and the payback period for the system[12] is a very good example of the benefits of the correct approach for integration and PPP.

The liberalisation of Telecom in Europe has introduced a development of new services. Private telecom operators express interest in the provision of new services linked to travel, but in fact we observe that concerning travel and traffic information, the provision of this service is still in majority in the hands of public authorities. No delegation management exists in this domain alone, proof that it is not ranked at a high priority by public authorities. However initiatives have been taken by automobile clubs in countries where they are well established in order to improve the service for the drivers.

Great hopes have been placed in the interest of the private sector in this domain and UK has introduced in 89 a law[13] for enabling this development.

Traffic*master*™ has developed its services with its own means and there is now plan for extending to Germany with other industrial partners.

Public private partnership for information provision have been developed in Scotland (SCOTIA), but there is no evidence of its success. Similar schemes are under deployment in Germany (Nuremberg, Bayern info, etc.), France (Médiamobile).

Some lessons learnt from these projects are that:

- travel and traffic information as an independent value added service seems difficult to bring payback to private investors.
- Existing models reveal that to be attractive several services should be combined (individual as emergency assistance, collective as traffic management) with in some cases the transfer of public money from public operation to payment of a service to the private sector.
- Where road infrastructure is operated by private operators, with tolls the development of the ITS services could be facilitated.

Private telecom operators have invested a lot in the basic infrastructure for communications and are competing by offering new added-value services. But in fact it seems that for the time being, they not placing on top priority traffic and travel information services: the profitability is very critical on the market size while penetration seems to be slow. A broadening of the ITS services that are offered is necessary to reach the critical size.

---

[12] In the QUARTET Plus project (TR1044) it was reported for the 5T system a payback period of 922 days by considering the operating cost savings only and 131 days if benefits for individual users (i.e. travel time) are included.

[13] Road Traffic (Driver Licensing and Information Systems) Act 1989. regulating the conditions for an operator to operate a driver infroamtion system in relation to public roads in Great Britain.

7.6 Advanced Driver Assistance

Risks: It will not be possible to develop advanced driver assistance systems that can achieve absolute reliability (100%), be suitable to all types of driver, provide safe operation under all circumstances, and communicate reliably with both all other similarly equipped vehicles and the road infrastructure. On the other hand drivers might thrust fully to the proper operation of advanced driver assistance systems not being at any time aware of the necessity of manual interference which will result in driving less attentive and will increase reaction times in case of system malfunctions and irregular driving conditions. The functionality of advanced driver assistance systems is highly complex, which implies that the majority of the drivers does not understand its operation and thereby might not be able to recognise conditions under which a human interference is required quickly which could arise safety critical conditions. Therefore these systems will not be attractive to drivers who might purchase them and to manufacturers. Thus the deployment of ITS services involving automatic vehicle operation will not be successful.

Mitigation Strategy:

*Note : most of the strategies rely on the current work undertaken by EU's TAP project RESPONSE, and by the task force on legal aspects created by EU's TAP projects AC-ASSIST, UDC and CHAUFFEUR. Results that allow to have a clear view of the situation in each country is expected very soon (**European Commission**). However, the following strategies can already be proposed :*

- Consider revision of existing directives in order to take into account the introduction of "interventional systems" in the car: European working group with national representatives. (**European Commission)**
- Encourage and finance large scale tests in order to evaluate all possible impacts **(European Commission, Automotive Industry** with support from **authorities, automobile associations and insurance companies**)

Advanced driver assistance systems should be widely implemented in Europe as they can provide more efficient and safer road use. Such systems must be sufficiently reliable; at least it has to be avoided that systems are deployed which cannot detect malfunctions and erroneous conditions quickly enough to alert the driver sufficiently of such conditions. In any case profound education and training of the drivers is required and the design of the systems has to take into account the skills of the "least informed user". The operation of automatic vehicle control systems has to be compatible to long-term used skills in order to retain instinctive and correct driver interference thus ensuring safe operation also under degraded mode and under all possible circumstances. This topic is not only a manufacturer or a market problem, as systems will change dramatically the driving task and driver's behaviour. Then resources must be provided to assist with the subsequent operation of large scale test trials : in this field there is a need for long term tests under real-life conditions in order to evaluate all the possible impacts. When this has been completed, resources must also be provided to develop strategies for the installation of any required infrastructure and provide regulations to ensure common standards of safe operation. They must also work with Road Users' associations and/or Insurance Companies to promote awareness amongst drivers of the existence and use of these systems (see section on Promotion of ITS benefits)

For some systems, difficulties appear so important that it is likely that the national legislators will require a type of "super-licence" for drivers being authorised to drive vehicles equipped with safety critical advanced vehicle control systems. This idea does not seem really acceptable and is in

contradiction with the targeted objectives: there is a risk of restraining the market development of such products. For most systems, a reinforcement of drivers' current training will be sufficient. The automotive vendors and equipment retailers should be as well trained to inform and instruct the drivers of newly equipped cars. In order to assist drivers to understand what the systems can do, a differentiation needs to be made between those systems that provide warnings to drivers and those that actually exert some control over the vehicle.

The RESPONSE project is scheduled to produce additional input to these topics that can be used to form the basis of an action plan to be developed.

An action plan should be developed in this area in order to address, step by step the difficulties:

- first address the problem of "additional warning functions" (the existing type approval rules seem sufficient).
- Secondly address the problem of "reactive systems" (i.e. systems modifying the actuators functioning): the existing type approval does not seem sufficient and should be completed.
- Thirdly address the problem of "interventional systems" (which can overrule the drivers' actions), which necessitates more R&D and long term evaluation.

This action plan has to be set-up with the concerned parties: automotive industry, regulation European and national bodies.

Comments: This strategy mainly addresses threats in the **Safety** and **Technological Maturity** categories. It also will have a minor impact on the threats in the **Traveller Acceptance** category. The deployment of advanced driver systems tends to be erratic. This is because they are not easy to fit into existing vehicles and therefore have to wait until manufacturers can produce new models. They are also not seen as being totally safe and reliable in operation. There needs to be a concerted and co-ordinated methodology for test deployment programme so that the technological feasibility, safety of operation and extreme reliability of these systems can be proved. Existing guidelines for testing procedures should be then extended in order to encompass the new systems. In particular, advanced driver assistance systems based on artificial intelligence, fuzzy logic, … cannot be tested for each situation they may encounter, as mechanical systems can. New procedures must be then established.

In addition, this last difficulty raise the problem of liability issues : to what extent the limitation of liability products may evolve if necessary with on top of that the different legal philosophies among different states (case-oriented vs law oriented jurisdiction).

. An important work has been achieved within a task force created by 3 R&D projects: AC-ASSIST, UDC and CHAUFFEUR. A report on Legal Aspects has been produced [14] and identifies the major issues. However, concerning compliance with traffic regulations, liabilities of the driver and the keeper of the vehicle, product liability it is focused on German and Italian laws. A widening of this approach is already undertaken thanks to the RESPONSE project.

However, it has to be taken into account that a need has already been expressed for an extension of the EC recommendation for the certification of new vehicles equipped with systems able to control the vehicle (Extension of the 70/156/EEC directive, relevant only for M1 vehicles, i.e. vehicles designed for the carriage of passengers and comprising no more than 8 seats in addition to the driver's seat).

7.7 Demand Management

Risks: The variety and number of factors that must be combined to create a viable demand management strategy may require very complex technology. Suppliers will be reluctant to develop such technology because of the high cost. Authorities and Service Providers may also be reluctant to implement these strategies because of adverse traveller reaction.

Mitigation Strategy:

- Encourage development of modelling tools : R&D funding **(European Commission and National Authorities**)

The definition and implementation of demand management technology must be actively promoted at different geographical levels (city, regional, national or European) including all relevant transport modes. This technology should be capable of proposing and implementing strategies to manage travel demand to enable different transport policies to be pursued. Support for this work must come through the development of sophisticated modelling tools. These must enable real data to be used to explore the different ways in which demand can be managed across all transport modes in a way that produces benefits and is acceptable to travellers.

Comments: This strategy mainly addresses threats in the **Technological Maturity** category, but will also have an impact on those in the **Traveller Acceptance** category. So far there is no demand management system available in Europe that is capable of optimising demand levels across different modes of surface transport. What systems do exist are mainly concerned with providing ad-hoc advice in the case of incidents and are dependent on the personal view of those (operators or broadcasters) giving the advice. There are many examples of this across Europe, providing advice via such things as radio broadcasts, teletext, the Internet and VMS. Demand management systems could provide benefits where it is possible to switch travellers between private cars and various forms of public transport. Generally this will probably not be in real time, except when incidents occur in which case the effect of different forms of travel advice could be investigated. In general however these systems could be used to forecast the effects of different transport measures, for example changing car park prices, imposing tolls, etc.

National particularities:

Demand management strategies should be adapted to the various situations (national, local context), type of traffic (commuters, holiday migrations, etc.). They are first based on transport policy and involve a lot of different aspects.

Due to its position allowing transit from Northern Europe to Southern Europe, France implemented in 76 the first large scale management operation for holiday traffic (termed BISON FUTE, from the name of a “clever Indian” used for advertising purpose and giving the idea of guiding the motorists on the best route at the right moment).

First strategies were implemented with basic forecast tools based on surveys and communication to the users was at the beginning very simple. After years, the traffic modelling was improved in order to better take into account the user behaviour. In the meantime, the communication became more sophisticated in order to meet better the drivers’ requirements. Lessons learnt from this experience (still in operation after more than 20 years) reveal that in this domain traffic modelling and strategies have to be tuned after real implementation (learning process).

Similar experiences exist in other contexts and particularly for commuting traffic (Netherlands, Germany...) with strategies for transferring traffic from individual transport to public transport. It appears that these strategies are effective only when they can evolve in order to be permanently adapted to the user behaviour.

This confirms the need for more R&D aiming at the development of modelling of strategies and users behaviour.

7.8 Incident Management

Risks: It will be too difficult to predict where incidents will occur, reducing the effect of strategies developed in advance. When they do occur their immediate detection may not be possible because it will be too expensive to provide sensors throughout the road network. The high complexity and cost of developing on-line modelling tools will force network managers to use off-line tools or rely on unskilled operator action. This will mean that the strategies that they developed and implemented will be less effective.

Mitigation Strategy:

- Support of R&D for development of on-line modelling tools (**European Commission** and **National Authorities**)

The development of incident management strategies must be actively promoted to minimise disruption and reduce the time it takes for those involved in incident to receive assistance. Sophisticated on-line modelling tools must be developed that enable the reliance on comprehensive network monitoring, the use of off-line tools and operator intervention to be reduced. These tools must also enable a variety of different scenarios for incident locations and response actions to be explored according to the existing organisations that may differ from one country to another

Comments: This strategy is designed to mainly impact the threats in the **Technological Maturity** category. However it will also affect threats in the **Deployment & Operation**, **ITS Infrastructure** and **Safety** categories. In some places across Europe, what are called incident management systems are starting to be deployed. Whilst the detection of incidents is becoming increasingly more sophisticated and reliable, there is still a problem with the provision of adequate sensors in the ITS infrastructure. The creation and implementation of strategies is still largely a manual operation and hence the skills and experience of operators. Work needs to be done to make strategy implementation more automatic and to provide tools for the on-line development of strategies. Automatic implementation would probably need to be based on the use of artificial intelligence and in the first implementations may provide advice to operators. The on-line development of strategies would use models and simulators, based on such things as the road network structure, plus current and historic traffic data. One benefit of both these developments is that they can combat the unpredictable nature of incident occurrence that makes most pre-defined strategies not applicable. Innovative incident and congestion management systems of this type were demonstrated in the cities of Turin in Italy and Toulouse in France as part of QUARTET Plus initiative (a TAP project sponsored by DGXIII). The two systems are both based on the "town supervisor" concept and showed very positive results by using two different approaches. In Turin an approach involving a conventional system based on advanced modelling was used whilst in Toulouse an approach using artificial intelligence techniques was applied. Both these approaches are being implemented in other European cities.

7.9 Data Sharing

Risks: Service Providers, Transport Operators and Public Authorities will refuse to share data with one another and with the Public Authorities. Data use will be confined to those responsible for its collection. This will restrict the growth of ITS services and fragment the market for ITS products. This will as well reduce the possibilities for travellers to use alternative modes of transport, and will make difficult for authorities to promote multimodality.

Mitigation Strategy:

- The co-operation and exchange of data between service providers, authorities and transport operators must be favoured and encouraged for the mutual benefit, thus removing the culture of data being the exclusive property of the collector. **National Authorities** and **Local Authorities** to define clear policy concerning data access to private organisations, establish sustainable rules and continue to develop legal framework for facilitating co-operation with private sector.
- Reference models (e.g. Interchange agreement) to be developed along the lines of the common practise in the emerging DATEX network with extension to other services than only traffic management and information. (**European Commission and National and Local Authorities**)
- Support R&D activities in the field of provision of travellers assistance services to allow easy and efficient switch of transport mode for travellers and freight (**European Commission and National Authorities**)

The idea that sharing data will increase the size of the market for ITS related products and systems, as well as the patronage of ITS services must be promoted within the Service Providers and Transport Operators. This may require that steps are taken to put in place legal requirements to make data available from some organisations such as the Police. However the general exchange of data between providers should be encouraged so that more comprehensive range of ITS products can be provided to more travellers. It particular, within these ITS services, multimodal information services are of interest both for the individual traveller and for the transport authority; but multimodal information services are the most critical as they can only be implemented if the different transport operators agrees to share their data. This exchange of data can also be encouraged by providing a sophisticated legal framework concerning this new industrial field.

While the structure based on the memorandum of understanding (see 7.3) is needed to rule those constraints that are common to all the members of the data-exchange network, at the lower level another mechanism is needed to rule the relationship between couples of organisations exchanging or sharing data; typically this is to be decided on a case by case basis. It would be recommended to develop further and establish reference models developed along the lines of the common practise in the emerging DATEX network. Among other things (e.g. communication protocol to be used) the rules for data exchange, limits of responsibility and permitted use of data are defined in an “interchange agreement” signed between two organisations which decide to share data. If a third party wants also to develop a service using these data, it is required to sign an “interchange agreement” with the two. The interchange agreement should also be the mechanism that establishes the relationship between the services offered by the involved organisations and defines what are the allowed duplication, overlapping and liaisons of information and degree of freedom in the decision of the strategies to be used for value added services (e.g. in a multimodal routing service the best route for each mode can be decided by the operators of each modes or by the service provider).

The data exchange network should be extended from the TERN to the TEN and complemented including multimodal information. The extension of the data exchange network have also to take into account the organisational issues related to the need for co-operation, data sharing, and sharing of responsibility between different operators normally operating independently for different mode of transport. [17]

Attractive travellers assistance services have already been demonstrated by using GSM based communications (i.e. SMS on mobile phones, Personal Traveller Assistant), capable to follow step by step the traveller for an efficient and reliable support in the trip optimisation in conjunction with integrated payment facilities. R&D should be encouraged in this field because the provision of a high level of comfort is one of the key elements to attract users toward different travelling approach.

Comments: The main impact of this strategy will be on the threats in the **Organisation and Institutional Issues** category. There will also be an impact on the threats in the **Deployment & Operation** and **Stakeholder Acceptance** categories.

The culture of data being the exclusive property of the collector has to be removed. However this should not cause Service Providers and Network Operators to suffer. It should be seen as a way of making more information available to more travellers via a variety of mechanisms. For example if traffic flow data was made available by private data collection companies to network control centres, the private companies could be given access to guidance information normally only shown on VMS. The result would be that the network control centres would have more data on which to base their traffic information. In addition the private companies would be able to offer guidance in addition to information about traffic levels.

National particularities:

Some countries have developed since long time the share of data between administrations themselves or between administrations and non-profit organisations such as automobile-clubs. Some examples:

- ✓ in France, traffic data are collected by police, Gendarmerie and Department of Transport services. They are put together in traffic information centres that are ruled by the three Ministries. A protocol established in 80 and updated in 89 rules the operating principles
- ✓ in UK, AA[14] and RAC[15] have since long time collaborated with the police, Highway agencies, and counties for exchanging traffic information.
- ✓ In the Netherlands, Germany, the same operating principles have been put in place.
- ✓ In Italy the same approach allowed motorway companies, police, automobile associations, ministry of public works and national television and radio broadcaster to build a new centre for gathering traffic information, initially needed for the provision of the RDS-TMC service.

[14] Automobile Association, U.K. based association of drivers

[15] Royal Automobile Club, U.K. based association of drivers

New regulations have been introduced in some countries concerning the provision of public data: in France directive of the Prime Minister for enabling access to public data (access to raw data must be provided free, while process, formatting, transmission can be charged). In UK the access of data is also facilitated for driver information system operators, once they have been licensed by the Secretary of State. In addition a MoU has been established between the police and five organisations in order to organise these exchanges: according to the area, only one of the organisation is responsible for collecting the information from the police and transmitting them to the four others. In Germany, traffic data are passed freely onto private organisations.

Other member States are developing similar facilities ([13, Volume 4c, table C2)]

7.10 Privacy and Data Protection

Risks: Existing legislation concerning privacy and data protection either does not completely cover the data collected by systems providing ITS services or is not properly complied with. Travellers will be reluctant to use these services because the information that they contain could be misused, thereby compromising their privacy.

Mitigation Strategy:

- Promotion of the existing measures taken for guaranteeing the privacy**: European Authorities, National Authorities, ITS Organisations, Automobile Associations and Privacy and Consumer Protection Organisations**.
- Inclusion in the launch of a new ITS service, and in the documentation of suitable information about how privacy is taken into consideration : **Information Service Providers**

The idea that safeguarding of the personal privacy of travellers using ITS is essential must be actively promoted amongst Service Providers and Network Operators. If necessary this promotion should be supported by legal measures to ensure that minimum data protection standards are observed, as well as providing travellers with legal safeguards against cases of data misuse. The measures that have to be made to ensure a maximum level of privacy for travellers must also be clarified. In parallel with these activities, the social awareness and acceptance of the need to identify movements must be actively promoted amongst travellers.

Comments: This strategy is only aimed at the threats in the **Privacy** category. In the past services such as road pricing have not been adopted because of the fear that travellers' movements will not have the privacy they currently enjoy. However the climate of public opinion is changing - witness the widespread use of mobile telephones where the location of each handset is needed to make sure that "roaming" can take place. In the ITS area data such as that gathered for use in origin-destination matrices may contain data that shows specific traveller movements. There needs to be a greater effort to show travellers that their details can be protected and privacy ensured. Thus the provisions of existing data protection legislation need to be studied and enhanced if needed. One step would be to ban the active use of traveller data for things such as marketing of ITS products.

National particularities:

In fact there is now a EU directive in force since Oct 98 concerning protection of private data. National legislation is then likely to be adapted in the near future. It seems that from the legal point of view the protection of privacy will be then at the same level in all European countries.

The problem seems to be in the understanding of the law and the confidence that the drivers could have in authorities, public organisations or private organisations for respecting the rules. One example:

- in UK, up to know there is in general no controversy by the drivers who have infringed a traffic regulation (traffic lights, speed, etc.) and are identified by automatic systems.
- In France, the use of automatic systems (photos) and of radar has been contested for long years and this contest is relayed by some media. This phenomena is particularly amplified when comes to the public revelations about situations, without any relation with ITS, where privacy has not been respected (several cases in the recent past).

This leads in fact to the problem of public acceptance of ITS systems for which promotion should be conducted. (see 7.4).

7.11 Vehicle Communications

Risks: Across Europe a number of differing communications technologies and standards will be used to transfer data between vehicles and the roadside. There will also be different areas of geographic coverage due to the type of technologies being used by the various Service Providers. This will mean that ITS services will not be available uniformly across Europe thus fragmenting the market and making it too costly to provide the services.

Mitigation Strategy:

- Encourage the deployment of systems having reached a sufficient level of maturity, (e.g. RDS/TMC, DSRC, etc.). Plan carefully the evolution towards emerging technologies in order not to kill the first coming ITS services, particularly by promoting transitory solutions. **KAREN** Framework Architecture to facilitate the implementation of such solutions, priorities to be established by the **European Authorities in concertation with National Authorities.**
- Develop European framework for ensuring interoperability of ITS services **(European Commission).**
- **National** and **Local Authorities** and **Information Service Providers** to establish concerted plans to prepare smooth evolution toward new technologies and adopt transitory solutions if necessary.

Steps must be taken to ensure that road users can move from one geographic area of Europe to another without loosing access to any ITS services. To achieve this **Private Industry** must develop ITS products that use technologies that enable services to more easily cover all geographic areas. In addition resources must be provided through research initiatives (sponsored by European and Public Authorities) to enable Private Industry to carryout R&D and support standardisation of the interfaces between vehicles, with the road infrastructure and with the driver. This work must make sure that the interfaces enable in-vehicle equipment to be updated as system and vehicle technology evolves with time, and make it possible for more comprehensive system self-testing and fault diagnosis.

Comments: An important aspect is roaming agreements between Network providers and between information service providers. The first should provide to ITS service providers a standard unified protocol that allows ITS service providers to continuously monitor the quality of communication and should agree on seamless roaming for all wireless services. This needs to be discussed in appropriate fora (e.g. GSM-MoU). Also if the telephone is used in other networks than the home network (Roaming) it can be extremely important (e.g. for emergency situations) that a network service provider supporting both voice connection and SMS can be selected. Network providers should support and forward Calling Line Identification to allow simple means of end-to-end authentication for different services.

The same approach should be used by the information service providers to provide the “roaming” of the service. Different service providers should establish an agreement so that if the user cannot access to the “home” provider the user can still receive a minimum level of service by accessing to another provider, or alternatively can use another provider as the mean to reach the “home” provider.

National particularities:

Several cases can be given as an example:

- At present, in the domain of EFC, there is an emerging European standard, based on the (5,8 GHz Dedicated Short-Range Communication. Before this standardisation process, Italy and Portugal developed their own standards, on the same frequency but incompatible with the European one. In the meantime, French motorways implemented various different systems. And nowadays: there are currently projects promoting the use of GSM coupled with GPS for EFC. Without willing to cast any doubt upon the interest of this alternative solution, it is clear that the immediate effect will likely be to raise obstacles for interoperability of EFC systems in Europe. The presence of an alternative solution will also weaken the positions in favour of a common European standard. A second and similar example is given by after-theft systems: in some countries, they are using GSM/GPS, while in other they are based on DSRC. There is no doubt that for this application the interoperability is essential (even more than in the first case where intermediate operating procedures can be established to ensure interoperability).

- A third example is given by the introduction of Mayday systems based on GSM network. There should be the guarantee that a subscriber to a service in one country could have the possibility (of course with the extension of his subscription) to use the system with the same level of service in another country. There could be several possibilities: if there is a similar service operating, contractual agreement should be arranged between operators for ensuring the roaming facilities. If there is not, the possibility of a minimum service should be examined.

Without contesting the interest of competition, actions should be taken at European level in order to give guidelines, after having assessed the various scenarios: socio-economic evaluation of the different solutions should be undertaken, in order to allow authorities to take appropriate measures if necessary..

7.12 ITS Infrastructure

Risks: The infrastructure installed to support ITS products rapidly becomes obsolete due to the fast pace of technology development that enables the services to be provided in different ways. Service Providers and Network Operators will not participate in the provision of ITS services as they will be unable to recover the initial capital investment in the infrastructure before it becomes obsolete.

Mitigation Strategy:

- Exploit **KAREN** results for designing optimised and evolutive communication infrastructure, able to support several ITS applications. (**ITS system designers/developers**)
- Develop public-private and private-private partnership for the sharing of common and generically available communication infrastructures. Promotion developed by **National and/or European Authorities** (see 7.5)

Private Industry must develop ways of making it easier to deploy the infrastructures needed to support ITS services. This can be achieved in several ways including a reduction of their capital and operating costs, and the sharing of the infrastructure resources with other services, some of which may not be ITS related. The work of Private Industry on the sharing or infrastructure resources must be enhanced through the active promotion by European Authorities of its benefits and cost savings. In order to minimise the risks, it is also recommended that authorities made public clear plans about their ITS policy and maintain for a sufficient time lapse the same strategy.

On the strict traffic management level, some interesting approaches have been developed for a better share of common resources between several applications. Adopted and tested in different sites in Europe the solution is based on the installation of on-road equipment that enables sensors, beacons and information displays for locally grouped applications to share the same communication network while minimising the duplication of hard-wiring. This solution allows for considerable savings in both installation and operation costs, by installing proper outstations on strategic locations on the transport network and connecting as many devices as possible to each of these outstations. Each outstation then provides the management of a shared communication link to the control centre or to other outstations. Thus outstations act as nodes of a shared communication network were messages/data are transmitted between devices and control centres regardless the application they belong to.

This approach demonstrated its efficiency in both urban and interurban environment and should be encouraged for all new applications.

The same approach described above demonstrated additional benefits by adopting as outstation "intelligent" units capable of the performing different task locally and autonomously. In this cases, in the literature; the units are defined as Multifunctional Outstations and might allow a low-level integration of application by offering the platform for data exchange and processing (e.g. co-operative traffic state estimation and control at the local level).

One example of implementation of this approach is given by the 5T system in Turin in which multifunctional outstations are a fundamental component of the integrated architecture. In this case the multifunctional outstations are primarily an Urban Traffic Control component which can be integrated with various types of area control and implementations.

In the case of the 5T system it was calculated that by using the multifunctional outstations, the number of communication links needed was reduced to less than 20% of those that would be required by the

alternative solution of connecting single function outstations to the centres. In terms of the costs for purchasing and installing the outstations at the roadside, it is estimated that they can be recovered by savings on transmission charges over a payback period of one year.

These issues have a clear link with the issues raise above (see sections 7.3. and 7.9.) about data exchange and data sharing. In order to be able to exploit the advantages of the multifunctional outstation approach it is necessary that integrated applications and systems agrees as a minimum on the used message formats and interfaces with the shared network. The establishment of this approach at the level of European Framework architecture would also push for an open market of compatible multifunctional outstation available "off the shelf".

Authorities and system operators, who are now "cabling" their cities for more demanding applications, will certainly be prone to convert to standard, shared solutions for lowering the implementation and maintenance costs of their systems. They need to see convenient solutions on the European market, capable of offering paths for gradual conversion of their systems, with a convenient set of applicable standards. The on-going developments in urban telecommunication networking and related technologies have to be carefully looked at: the traffic/transport application can, indeed, only piggyback on other large-scale developments.

One important component of the costs of installation and operation of hard-wired communication network for roadside equipment resides in the costs for "cutting" the road surface to install the cabling. Successively the installation the hard-wired communication network represents the weak part of the system as it is exposed to the damages due to road works with consequent additional operating costs. The wire-less technology can offer a solution to these costs mainly nowadays in which digital communications allowing robust data transmission (e.g. GSM and DECT) are available at low cost (and almost null installation costs) and costs for communications are rapidly decreasing.

An alternative solution, which is in development particularly on toll motorway network, is to install high capacity communication infrastructure. This infrastructure can be financed by the infrastructure operator and then let to private operators or financed by private communication operators who pay a right of way and offer spare capacity for the needs of ITS applications. Such agreements should be encouraged (see 7.5)

Other approaches, in some cases implemented or still in the research phase, should be encouraged as they can help in achieving the double objective of the expanding the coverage of the surveyed area and limiting or avoiding the wiring.

The basic idea is to equip vehicles with on board units capable of measuring vehicle journey parameters such as travel time, speed, emissions etc. and communicating uploading them to a centre by means of a radio link or DSRC when driving passed beacons. In urban environments some systems uses already this approach by using public transport fleet vehicles and taxis as source of information. Private vehicles could be also used particularly when already equipped with on-board systems for other reasons (e.g. route guidance, exhaust emission control systems, location system).

On the interurban environment many countries have toll motorways equipped with infrastructures for automatic fee collection and a large number of equipped vehicles, consequently there is the potential for a huge amount of additional traffic data at almost no additional costs by exploiting the existing infrastructures. This requires a clear design of the data collection system in order to respect privacy. It is worth to mention that this allow to cover not only the existing toll motorway network (about 20,000 km in Europe), but also all the network where equipped vehicles are likely to drive.

Another potentially available source of traffic data for interurban environment is given by commercial vehicle fleets as these vehicles are commonly equipped with sophisticated systems and already provided with data communication facilities.

Comments: This strategy is mainly aimed at the threats in the **ITS Infrastructure** category. However it will also have an impact on threats in the **Funding Provision** category. The cost of providing the infrastructures needed to support ITS services must be reduced. Although the rapid advance of technology is producing many new products, the actual type of infrastructure that they use, such as copper cable and fibre optic cable, is not changing. Therefore Manufacturers need to make the upgrade to products using this new technology as cheap as possible. They must also make it possible to take advantage of using the new technology whilst retaining the existing infrastructure. At the same time research and development activities must be aimed at new technology that can make use of the existing infrastructures. Activity is also needed by European Authorities and Governments to promote the sharing of infrastructures by a variety of different services. This should look at services outside ITS, such as entertainment and general data communications.

Part III

GLOSSARY

ACEA
Association des Constructeurs Européens d'Automobiles (European Association of Automotive Manufacturers)

Category
The threat ″Category″ attribute is a means focusing on a limited set of values that allows clustering of threats according to the range of issues with which different ITS stakeholders will need to deal.

DATEX
Pre-standard for traffic data information exchange between traffic information centres and traffic control centres.

DG
Directorate General. A part of the European Commission that has been given particular areas of responsibility. The most relevant ones for the RAID Project are DGXIII (Information Society: Telecommunications, Markets, Technologies - Innovation and Exploitation of Research), which activities include Transport Telematics, and DGVII (Transport).

EFC
Electronic Fee Collection

FA
Framework Architecture

FFM
Freight and Fleet Management

HMI
Human Machine Interface.

KAREN
Keystone Architecture Required for European Networks. It is the project number TR4108 sponsored by the European Commission's Telematics Application Programme that in the period 1998-2000 will produce the European Framework Architecture.

HOV
High Occupancy Vehicle - a private car or van that is carrying more than one occupant, and is therefore able to use lanes in the highway that are specially reserved for such vehicles.

ISO
International Standard Organisation - responsible for devising and implementing standards throughout the World.

ITS
Intelligent Transport System is a system that aims at improving mobility, security and the environment by introducing Telematics within transports.

ITS America
Organisation that aims at promoting the development and usage of ITS through the United States of America. Its membership comprises Government organisations, private industry, consultants and academia.

Mitigation Strategy
A series of actions designed to lower the probability of occurrence of a threat. The actions will have actors to implement them and a scenario under which they are to be implemented.

MoU
Memorandum of Understanding

POLIS
Promoting Operational Links with Integrated Services - is a network of European cities, regions and regional organisations who are working together to solve their common transport and environmental problems through the use of advanced telematics applications. POLIS is an independent international association which is closely linked to the European Association of Metropolitan Cities (Eurocities).

PPP
Public Private Partnerships - a partnership between a Government organisation and a private company that is formed for the purpose of delivering (amongst other things) ITS services. The Government organisation may be from the National or Local Government sectors, or a combination of the two.

RAID
Risk Analysis for ITS Deployment. It is the name given to both the Study on System Architecture TAP97/9 and the team performing it.

Risk
A risk is a characteristic of a situation or action wherein two or more outcomes are possible, the particular outcome that will occur is unknown and at least one of the possibilities is undesired [4]. So, a risk is, at minimum, a two dimensional concept involving (1) the possibility of an adverse outcome and (2) uncertainty over the occurrence, timing, or magnitude of that adverse outcome. If either attribute is absent, then there is no risk.

Scenario
A scenario is a set of circumstances in which a risk might occur and for which a mitigation strategy is recommended.

TAP
Telematics Application Programme. EU Research and Development programme 1994-1998 (part of the EU's 4th Framework Programme).

Threat
A threat is a circumstance or situation that will in some way adversely affect the outcome of a programme of events. The definition of each threat is contained in its description.

TICS
Transport Information and Control Systems. It is the acronym used in the ISO bibliography to refer to the Transport Telematics systems.

TT
Transport Telematics.

UITP
Union Internationale des Transports Publics (International Organisation of Public Transport)

REFERENCES

1. ISO/TC204/WG1, "Transport Information and Control Systems - Reference Model Architecture(s) for the TICS Sector - Part 1: Fundamental TICS Services", Version 3.0, 7/2/1997

2. Project CONVERGE, "Services and functions: where do we stand?", Issue 1.0, November 1996

3. Vlasta Molak, "Fundamentals of Risk Analysis and Risk Management", CRC Press, 1997

4. Covello, V.T. and M.W. Merkhofer, "Risk Assessment Methods, Approaches for assessing health and environmental threats", Plemum Press, New York, 1993

5. Ansell J. and F. Wharton, "Risk: Analysis, Assessment and Management", Wiley, 1992

6. ITS America Architecture URL http://www.itsa.org

7. DELPHI Technique; URL http://www.nasi.hq.faa.gov

8. Dale Cooper & Chris Chapman, „Risk Analysis for Large Project », Wiley, 1987

9. Joseph H. Schmoll (DSMC - Fort Belvoir), "DSMC/Introduction to Defense Acquisition Management", Defense Systems Management College, 1993

10. Benjamin S. Blanchard & Walter J. Fabrycky, "Systems Engineering and Analysis", Prentice Hall, 1990

11. John C. Miles & A. Janet Walker, "The WELL-TIMED Study", EC - DGXIII/C6, April '98

12. Telematics Application for Transport - EC DGXIII-C, URL http://www.trentel.org

13. TELTEN 2 A partnership between the European Commission (DG VII) and ERTICO, May '97

14. Legal and Liability issues of market introduction (Dr Joachim Feldges – PVW&A and al.) October '98.

15. European Statement of Principles on Human Machine Interface for In-Vehicle Information and Communication system EC 5/98 May '98

16. European Statement of Principles on HMI – Expansion of the principles Del 6.1.2. CONVERGE project, 31/12/98

17. INFOTEN (TR 1032); Public-Private Partnership - Issues and Examples (09/98)

18. Becker S., Mihm J., Brauswetter C. "Advanced Vehicle Control Systems _: User Comes First...", 4th World Congress on ITS, Berlin, 1997

19. ComUniti: Comfort and Safety in an User-oriented TERN-Network ensuring interoperability of the Transport Infrastructure. Published by ADAC. Project carried out for the European Road Safety Federation by ADAC, AA, ACI, ÖAMTC and ANWB, with the support of the European Commission; July 1998.