2C – RISK ANALYSIS RESULTS

RAID aims at the definition of threats against the implementation of a European Framework Architecture and against the implementation of ITS systems in general. This annex complements the results of the threats collection presented in chapter 6.

1 THE SCENARIO BASED APPROACH

The 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 multi-modal 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.

The current version of the database includes 32 different kinds of *detailed scenarios* identified as different combinations of the values for the four elements described above.

The values of the scenario elements were slightly interpreted in order to reduce the variability of some parameters without loosing the selected level of detail. The original values of the ″time horizon″ element were reduced to three with the following interpretation:
"Long term scenario" when the time horizon is beyond 2010;
– "Medium term scenario" when the time horizon is between 2002 and 2010;
– "Short term scenario" when the time horizon is before 2002;

The 32 detailed scenarios included in the database are listed in the following picture and described using a tree-structured representation.

The resulting diagram can be used as a tool to "navigate" from the definition of a selected scenario to the code of the corresponding detailed scenario, eventually this can be used as the key to extract the related highly rated risks from the RAID database.

The meaning of the abbreviations used in the tree diagram are as follow:

Time horizon element
– **Long, Medium, Short:** as described in the paragraph above.

Public-Private Co-operation
– **Mix:** public and private sectors find a co-operative way of introducing ITS
– **Priv:** private sector is the driving force of the ITS development

- **Priv+:** private sector is the driving force of the ITS development either alone or in co-operation with the public sector
- **Pub:** public sector is the driving force of the ITS development
- **Any:** the scenario does not depend on which forces drive the ITS development.

Main ITS trends

- **Ctrl:** ITS strategies focused on the provision of Telematics infrastructures to improve the efficiency and the safety of the transport network
- **Dman:** ITS strategies aimed at using Telematics applications for traffic Demand Management
- **Inf:** 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
- **All**: the scenario does not depend on the main trend for the ITS strategy.

Geographical extension

- **Inter, Urb, Rural:** stands for Interurban, urban and rural respectively.

	Time horizon	Pub-Priv Coop.	Main ITS trends	Geo. Extension
2211	LONG	MIX	CTRL	Inter
7211				Everywhere
2221		PRIV	CTRL	Inter
2213	MEDIUM	MIX	CTRL	Inter
7213				Everywhere
3216				Inter+Rural
6316			Ctrl+dman	Urb+Inter
7713			ALL	Everywhere
7523		PRIV	Inf+dman	Everywhere
2243		PUB	CTRL	Inter
7614	SHORT	MIX	Inf+ctrl	Everywhere
7714			ALL	Everywhere
7744		PUB	ALL	Everywhere
6117	Always	MIX	Dman	Urb+Inter
7117				Everywhere
3317			Ctrl+dman	Inter+Rural
7317				Everywhere
7417			INFO	Everywhere
7517			Inf+dman	Everywhere
7617			Inf+ctrl	Everywhere
6717			ALL	Urb+Inter
7717				Everywhere
7227		PRIV	CTRL	Everywhere
7727			ALL	Everywhere
7737		Priv+	ALL	Everywhere
6147		PUB	Dman.	Urb+Inter
7147				Everywhere
2347			Ctrl+dman	Inter
7347				Everywhere
7177		Any	Dman.	Everywhere
7477			INFO	Everywhere
7777			ALL	Everywhere

Picture 2C.1: Mapping of Scenario Codes

The above table might appear too complicated and difficult to handle when approaching the problem of identifying the risks involved in the development of an ITS from a higher level of abstraction.
Different criteria could be used to cluster the detailed scenarios into classes to be used as *basic reference scenarios*. The purpose of having a limited number of basic reference scenarios responds to the need of providing a simplified approach to identify the risks of the RAID database that are related to specific implementation environments even when they are not specified with a great level of detail. The scenario based approach can be used in addition to and/or in conjunction with the other classification keys provided by the RAID database such as ″Services″ and ″Categories″.

One effective way of clustering the scenarios is to distinguish between time related and time independent scenarios. Following this initial classification it is useful to distinguish between the case in which the ITS (or just a specific service) development and **operation** is completely driven by the public sector (e.g. Urban Traffic Control Centres, RDS-TMC in Denmark), and the most common situation in which the private sector is involved in the ITS development and **operation** with (e.g. Mediamobile in Paris, RDS-TMC in the Netherlands, tolling systems in France) or without the intervention of the public sector (e.g. Orchid and Trafficmaster in UK, DDG in Germany).

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”.

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 (urban, interurban and rural) although the distinction might turn to be necessary by the end of phase 2 if the recommended mitigation strategies are different for different geographical extensions. At the current stage it can be observed that most of the time, identified risks are general and are applicable to every geographical extension.

The analysis above allows the definition of 10 “basic reference scenarios” (i.e. 5 time related and 5 time independent).

It is up to the user of the RAID database to choose whether to browse through the list of risks by referring to the main basic scenarios or by referring to those more detailed as needed. A structured representation of the basic reference scenarios is provided in the following tables with the mapping of the detailed scenarios previously listed.

Time related

Basic scenario	Description		Detailed Scenarios
S1	Long term		2211, 2221, 7211
S2.1	Medium term	Public only	2243
S2.2	″	Private involved	2213, 3216, 6316, 7213, 7523, 7713
S3.1	Short term	Public only	7744
S3.2	″	Private involved	7614, 7714

Table 2C.1: Time Related Scenario Groups

Time independent

Basic scenario	Description		Detailed Scenarios
S4.1	Private involved	Dman	3317, 6117, 6717, 7117, 7177, 7317 7517, 7727, 7737
S4.2	″	Control	3317, 6717, 7227, 7317, 7617, 7717 7727, 7737, 7777
S4.3	″	Information	6717, 7417, 7477, 7517, 7617, 7717 7727, 7737
S5.1	Public only	Dman	2347, 6147, 7147, 7347
S5.2	″	Control	2347, 7347

Table 2C.2: Time Independent Scenario Groups

As a consequence to the higher level of abstraction used in this case, the proposed grouping of detailed scenarios overlaps. In practical terms it means that the same risks belongs to more than one basic reference scenario. In other words, each basic reference scenario offers a different point of view of the identified risks.

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 and S3.1. 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 data base. The consultation phases that will follow the issue 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.

1.2 Example of use of the basic scenarios

In this section a simple example of the way the basic scenario could be combined is given, in order to effectively use the information included in the RAID database once the actual ITS implementation scenario is defined.

Let’s assume that the municipality of a European city intend to study the feasibility of building up a consortium with selected private companies with the aim of installing and operating an advanced telematic system for the dynamic control of the traffic in the city centre. Beside the technical specifications and evaluation of costs, the municipality will be interested in evaluating what actions have to be envisaged in order to limit the possibility of delays and/or failures of either the development of the ITS system or its successful operation and expansion.

The municipality should then start to look at risks and recommended mitigation strategies classified for the S4.2 scenario (i.e. ”private sector involved in the development of ITS mainly for control purposes”). Within the list those items related to the services of interest can be selected and analysed. The risks of this scenarios can then be merged with those belonging to the S3.2 and S2.2 scenarios (i.e. ”Short term” and ”Medium term” time horizons respectively) to complete the analysis looking ahead up to the year 2010.

If a future evolution of the system integrating demand management facility is foreseen the municipality could complete the analysis by looking at the risks and mitigation strategies included in the scenario S4.1 (i.e. ”Private sector involved in the development of the ITS mainly for demand management purposes”).

Additional useful information can be gathered by looking more in depth at the details included in the above mentioned scenarios; for instance the municipality may understand from there, what problems encountered by the private partners of the consortium are likely to occur, and then plan actions in order to smooth them.

2 PRESENTATION OF THE THREATS GROUPED PER STRATEGY SCENARIO

In the following section, a presentation of the risks and their consequences associated to each selected basic scenario is given.

TIME RELATED

BASIC SCENARIO S1: Long term Time Horizon

Strategy Scenario	Threats
2211 (mix public and private, mainly control objectives, interurban area)	• The cost to equip and maintain sensors and transponders used for vehicle lane keeping in the highway infrastructure will be very high. • Equipment for use by lateral collision avoidance systems will be impossible to design or locate in the highway infrastructure so that they cannot be damaged by accidents, or vandalism.
7211 (mix public and private, mainly control objectives)	• It will prove impossible to develop lateral collision avoidance systems that have a level of hazard that is low enough to be acceptable by vehicle drivers. • Not enough vehicles are equipped with the same lateral collision avoidance capability so that collisions between equipped vehicles do occur.
2221 (mainly privately driven, mainly control objectives, interurban area)	• The cost to equip and maintain sensors and transponders used for vehicle lane keeping in the highway infrastructure will be very high.

Table 2C.3: Threats under the Basic Scenario S1

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

Strategy Scenario	Threats
2243	• Only a small number of vehicles will be equipped with automatic operation functionality.

Table 2C.4: Threats under the Basic Scenario S2.1

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

Strategy Scenario	Threats
7523 (information and demand management objectives)	• Static information (e.g. road infrastructure details) used by systems that provide ITS services is not regularly updated and becomes obsolete.
7713	• The KAREN Framework Architecture is found to be unable to accommodate new transport management policies and ITS services devised for Europe.
6316 (control and demand management objectives, urban and interurban area)	• The forecast of the arrival of emergency vehicles at traffic signals will not be accurate due to their unpredictable interaction with other road users.
3216 (control objectives, rural and interurban area)	• There is no payback in deploying ITS services for commercial vehicles on secondary transport axes.
7213 (control objectives)	• The development of longitudinal collision avoidance functionality with 100% reliability will prove to be impossible or too costly. • Not enough vehicles are equipped with the same longitudinal collision avoidance capability so that collisions between equipped vehicles do occur. • The deployment of system acting in place of the driver will be impossible due to existing traffic regulations
2213 (control objectives, interurban area)	• Only a small number of vehicles will be equipped with automatic operation functionality. • A common standard will not be achieved for communication between the automatic control functions in vehicles that are part

	of platoons. • In will not be possible to develop sensors and transponders to provide accurate vehicle positioning information under all operating conditions. • The development of vehicle control systems that have 100% reliability will prove to be impossible or too costly. • It may prove impossible or too costly to develop roadside or in-vehicle units that can exchange all the required data with vehicles that are passing at high speeds, e.g. in excess of 60mph/96kph.

Table 2C.5: Threats under the Basic Scenario S2.2

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

Strategy Scenario	Threats
7744	• There will not be a common policy across the EU regarding the degree and form of protection that is to be provided to vulnerable road users.

Table 2C.6: Threats under the Basic Scenario S3.1

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

Strategy Scenario	Threats
7614 (Information and control objectives)	• There is no compatibility between data transmission formats used by the large variety of electronic surveillance systems currently in use.
7714	• The KAREN Framework Architecture does not include all current transport policies and ITS services implemented in Europe. • Standardisation within Europe of interfaces to on-board vehicle systems does not materialise in the short term.

Table 2C.7: Threats under the Basic Scenario S3.2

TIME INDEPENDENT

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

Strategy Scenario	Threats
6117 (Urban and interurban area)	• Park and Ride sites have insufficient in capacity, poor security, or are not located in the right quantity nor in the most appropriate location to meet demand.
7117	• The cost and complexity of providing accurate on-line strategy development tools will inhibit the use of this method as an alternative to off-line modelling. • It will prove to be too difficult to predict where and when incidents will occur so that the strategies can be devised in advance. • The variety and number of factors that must be combined to create a viable demand management strategy may require very complex System functionality. • Sensors to accurately detect the numbers of travellers using different transport modes will be unavailable. • Development of sensors to reliably determine Public Transport vehicle passenger loading may prove difficult for those with more than one or a wide entry/exit.

3317 (control and demand management objectives, interurban and rural area)	• The automatic detection of dirty or damaged static highway signs will be difficult because of the lack of reliable and cost effective sensors. • The maintenance of the infrastructure used by travellers will be difficult because of the lack of reliable and cost effective sensors to detect when repair is necessary. • There will be insufficient probe vehicles to make it possible to establish the optimum timing and location of road works in inter-urban and rural areas.
7317 (control and demand management objectives)	• Distance measurement and labelling of roads differs from country to country within Europe. • Development of sensors that can reliably and accurately count the number of vehicle occupants under all operating conditions will be impossible. • The reliable detection of different sub-types of vehicle will not be possible with any degree of accuracy. • A reliable technique will not be found for measuring the emissions of all vehicles under all operating conditions. • It may be difficult to devise a method for the control of travellers (as opposed to vehicles) in a way that enables accurate and reliable images of violators to be obtained. • There are many systems currently deployed that provide electronic transactions without any standardisation of their interfaces and methods of charging. • There is no application of any standards for smart cards and the interfaces with in-vehicle systems across Europe preventing the implementation of a common pan-European system
7517 (information and demand management objectives)	• Static information (e.g. road infrastructure details) used by systems that provide ITS services is not regularly updated and becomes obsolete. • Existing legislation in respect of privacy and data protection is not complete enough to cover the data collected by systems providing ITS services. • Travellers have concerns about the misuse of information collected by ITS services such as origin-destination matrices, travel speeds, vehicle occupancy, etc. • Companies or authorities may not want to make data that they have produced available to other ITS services.
6717 (urban and interurban area)	• Park and Ride sites have insufficient in capacity, poor security, or are not located in the right quantity nor in the most appropriate location to meet demand.
7727 (mainly control objectives)	• 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.
7737	• Political changes to a National or Local Government agency that is partnering the private sector in the provision of ITS services leads to decisions that threatens the financial survival of the partners from the private sector. • There is a disparity between the aims and objectives of the public and private sectors that neither understands.
7177 (mainly demand management objectives)	• The management of public transport services is poor.

7477 (mainly information objectives)	• There are insufficient information sources to make sufficient data available for the service to be provided.
7777	• Lack of a sufficient number of skilled workers will hamper Manufacturers and Service Providers in the development, deployment and/or operation of new systems providing ITS services that are based on the KAREN Framework Architecture.

Table 2C.8: Threats under the Basic Scenario S4.1

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

Strategy Scenario	Threats
3317 (including demand management objectives, interurban and rural area)	• The automatic detection of dirty or damaged static highway signs will be difficult because of the lack of reliable and cost effective sensors. • The maintenance of the infrastructure used by travellers will be difficult because of the lack of reliable and cost effective sensors to detect when repair is necessary.
7317 (including demand management objectives)	• Distance measurement and labelling of roads differs from country to country within Europe. • Development of sensors that can reliably and accurately count the number of vehicle occupants under all operating conditions will be impossible. • The reliable detection of different sub-types of vehicle will not be possible with any degree of accuracy. • A reliable technique will not be found for measuring the emissions of all vehicles under all operating conditions. • It may be difficult to devise a method for the control of travellers (as opposed to vehicles) in a way that enables accurate and reliable images of violators to be obtained. • There are many systems currently deployed that provide electronic transactions without any standardisation of their interfaces and methods of charging. • There is no application of any standards for smart cards and the interfaces with in-vehicle systems across Europe preventing the implementation of a common pan-European system
7617 (including information objectives)	• Poorly designed in-vehicle systems and information can affect driver behaviour. • The infrastructure to collect information is not optimal because the private sector will not be allowed to install monitoring equipment on public roads.
6717 (including demand management and information objectives, urban and interurban area)	• Park and Ride sites have insufficient in capacity, poor security, or are not located in the right quantity nor in the most appropriate location to meet demand.
7717	• The information available from some systems providing ITS services is of poor quality because the data on which the information is based is also of poor quality. • No organisation exists within Europe to measure the quality of the information available from systems providing ITS services. • Some national and private funding may not be sufficient to cover the costs of implementing and operating ITS services that can be provided using systems developed from the KAREN Framework Architecture. • Certain gaps in certification procedures and missing information how the products are used by the drivers are existing. • Some of the existing systems that provide ITS services cannot migrate to become compatible with newer systems developed from the KAREN Framework Architecture because the required changes are too difficult and/or too costly. • Manufacturers want to sell their own systems and establish their own semi-standards to protect their share of the markets. • ITS services are not available in some parts of Europe because suitable wireless technologies are not available. • Different areas in Europe use different incompatible data communications mechanisms particularly for links between the roadside and the vehicle.

	• There is a continued lack of general advertising devoted to the facilities and benefits provided by ITS services. • The infrastructure installed as part of systems providing ITS services rapidly becomes obsolescent due to the fast pace of technology development that enables the services to be provided in different ways. • The regulations for dealing with the consequences resulting from the failure of systems providing ITS services are not well defined. • Despite efforts in some countries, 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 the parties. • 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. • Due to the subsidiary principle, the EU is not able to release recommendations obliging Member States to make use of certain systems or to promote or support certain ITS services. • Safety related data, or data containing personal information, may be corrupted. • Failure to approve and implement European standards in the appropriate time window may mean that any standards that are created do not take account of European needs. • Various data formats are used in various systems that need to communicate as part of several ITS services. • A common location referencing standard will not be available for use by systems. • The cost of providing comprehensive network monitoring will mean that parts of the network are devoid of sensors. • The provision of route guidance that takes account of current traffic conditions will be inaccurate due to lack of suitable vehicle detection on all parts of all routes. • It will be difficult for emerging traffic information services to rely on a unique telecommunication bearer, due to the technological development in telecom in Europe. • The presentation of the information to the user will differ from one country to another, or from one city to another, so that it will not be easily understandable for foreign or not local travellers
7227	• Drivers might fully thrust the proper operation of automatic vehicle control systems disregarding the possibility of the necessity of manual interference. • The functionality of advanced driver assistance systems is highly complex. • It will not prove possible to produce a cost effective vision enhancement systems that can be fitted to all vehicles for use by all physical sizes of driver. • 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.
7737 (including demand management and information objectives)	• Political changes to a National or Local Government agency that is partnering the private sector in the provision of ITS services leads to decisions that threatens the financial survival of the partners from the private sector. • There is a disparity between the aims and objectives of the public and private sectors that neither understands.
2347 (including demand management objectives, interurban	• The automatic detection of dirty or damaged static highway signs will be difficult because of the lack of reliable and cost

area)	effective sensors. • The maintenance of the infrastructure used by travellers will be difficult because of the lack of reliable and cost effective sensors to detect when repair is necessary.
7347 (including demand management objectives)	• Distance measurement and labelling of roads differs from country to country within Europe. • There will be inconsistencies in the way in which traffic regulations are enforced within the different EU States. • It will not be possible to control the start, location and duration of road works, especially when they are carried out by organisations not connected with traffic and travel management. • Each country within the European Union has a different policy covering charging for road usage.

Table 2C.9: Threats under the Basic Scenario S4.2

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

Strategy Scenario	Threats
7417	• Data provided by some organisations may not be used by some Service Providers because it is not available free of charge, or the charge cannot be recovered from the use of the ITS service(s). • There are not enough information sources to make sufficient data available for ITS services to be provided. • End users cannot cope with the facilities provided by some ITS services. • The cost of equipment to obtain pre-trip information and the cost of the information itself will be perceived by travellers to be too high. • This system will have to manage huge amounts of data from all Europe making a data processing hierarchy difficult to establish. • It will not prove possible to create and provide the very complex communications mechanism needed to link data sources across Europe and within some Countries. • It will prove impossible to develop safety readiness systems that have a level of hazard that is low enough to be acceptable by vehicle drivers. • There will be no common standard for the type of safety readiness systems fitted to vehicles.
7517 (including demand management objectives)	• Static information (e.g. road infrastructure details) used by systems that provide ITS services is not regularly updated and becomes obsolete. • Existing legislation in respect of privacy and data protection is not complete enough to cover the data collected by systems providing ITS services. • Travellers have concerns about the misuse of information collected by ITS services such as origin-destination matrices, travel speeds, vehicle occupancy, etc. • Companies or authorities may not want to make data that they have produced available to other ITS services.
7617 (including control objectives)	• Poorly designed in-vehicle systems and information can affect driver behaviour. • The infrastructure to collect information is not optimal because the private sector will not be allowed to install monitoring equipment on public roads.
6717	• Park and Ride sites have insufficient in capacity, poor security, or are not located in the right quantity nor in the most appropriate location to meet demand.
7717	• The information available from some systems providing ITS services is of poor quality because the data on which the information is based is also of poor quality. • No organisation exists within Europe to measure the quality of the information available from systems providing ITS services. • Some national and private funding may not be sufficient to cover the costs of implementing and operating ITS services that can be provided using systems developed from the KAREN Framework Architecture. • Some of the existing systems that provide ITS services cannot migrate to become compatible with newer systems developed from the KAREN Framework Architecture because the required changes are too difficult and/or too costly. • Manufacturers want to sell their own systems and establish their own semi-standards to protect their share of the markets. • ITS services are not available in some parts of Europe because suitable wireless technologies are not available.

	• Different areas in Europe use different incompatible data communications mechanisms particularly for links between the roadside and the vehicle. • There is a continued lack of general advertising devoted to the facilities and benefits provided by ITS services. • The infrastructure installed as part of systems providing ITS services rapidly becomes obsolescent due to the fast pace of technology development that enables the services to be provided in different ways. • The regulations for dealing with the consequences resulting from the failure of systems providing ITS services are not well defined. • Despite efforts in some countries, 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 the parties. • 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. • Due to the subsidiary principle, the EU is not able to release recommendations obliging Member States to make use of certain systems or to promote or support certain ITS services. • Safety related data, or data containing personal information, may be corrupted. • Failure to approve and implement European standards in the appropriate time window may mean that any standards that are created do not take account of European needs. • Various data formats are used in various systems that need to communicate as part of several ITS services. • A common location referencing standard will not be available for use by systems. • The cost of providing comprehensive network monitoring will mean that parts of the network are devoid of sensors. • The provision of route guidance that takes account of current traffic conditions will be inaccurate due to lack of suitable vehicle detection on all parts of all routes. • It will be difficult for emerging traffic information services to rely on a unique telecommunication bearer, due to the technological development in telecom in Europe. • The presentation of the information to the user will differ from one country to another, or from one city to another, so that it will not be easily understandable for foreign or not local travellers
7727	• 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.
7737	• Political changes to a National or Local Government agency that is partnering the private sector in the provision of ITS services leads to decisions that threatens the financial survival of the partners from the private sector. • There is a disparity between the aims and objectives of the public and private sectors that neither understands.

Table 2C.10: Threats under the Basic Scenario S4.3

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

Strategy Scenario	Threats
6147 (urban and interurban area)	• End users will not accept pricing for road usage if the level of other road related taxation remains high.
7147	• Despite the availability of ITS services, everyone will still make their commuting or leisure journeys at the same time of day and day of week. • The cost and complexity of providing accurate on-line strategy development tools will inhibit the use of this method as an alternative to off-line modelling. • It will prove to be too difficult to predict where and when incidents will occur so that the strategies can be devised in advance. • The cost of providing comprehensive network monitoring will mean that parts of the network are devoid of sensors. • When deployed the Systems that contain the demand management functionality will be the responsibility of different organisations. • Organisations that do not actively participate can cause significant flaws in demand management strategies because their uncoordinated actions may be disruptive.
2347 (including control objectives, interurban area)	• The automatic detection of dirty or damaged static highway signs will be difficult because of the lack of reliable and cost effective sensors. • The maintenance of the infrastructure used by travellers will be difficult because of the lack of reliable and cost effective sensors to detect when repair is necessary.
7347 (including control objectives)	• Distance measurement and labelling of roads differs from country to country within Europe. • There will be inconsistencies in the way in which traffic regulations are enforced within the different EU States. • It will not be possible to control the start, location and duration of road works, especially when they are carried out by organisations not connected with traffic and travel management. • Each country within the European Union has a different policy covering charging for road usage.

Table 2C.11: Threats under the Basic Scenario S5.1

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

Strategy Scenario	Threats
2347 (including demand management objectives, interurban area)	• The automatic detection of dirty or damaged static highway signs will be difficult because of the lack of reliable and cost effective sensors. • The maintenance of the infrastructure used by travellers will be difficult because of the lack of reliable and cost effective sensors to detect when repair is necessary.
7347 (including demand management objectives)	• Distance measurement and labelling of roads differs from country to country within Europe. • There will be inconsistencies in the way in which traffic regulations are enforced within the different EU States. • It will not be possible to control the start, location and duration of road works, especially when they are carried out by organisations not connected with traffic and travel management. • Each country within the European Union has a different policy covering charging for road usage.

Table 2C.12: Threats under the Basic Scenario S5.2

3. Presentation of the highly rated threats grouped per category

Category	Strategy Risk Number
Communication	0.2.1, 0.2.2, 2.2.1, 8.2.1

Category	Strategy Risk Number
Cost Benefit	0.3.4, 1.3.1, 8.3.1, 9.3.1, 15.3.1, 15.3.1

Category	Strategy Risk Number
Deployment & Operation	0.4.1, 0.4.2, 0.4.3, 0.4.4, 0.4.5, 0.4.6, 11.4.1, 11.4.2, 13.4.1, 13.4.2, 14.4.1, 15.4.1

Category	Strategy Risk Number
Framework Architecture	0.1.1, 0.1.2

Category	Strategy Risk Number
Funding Provision	0.5.2

Category	Strategy Risk Number
ITS Infrastructure	0.6.1

Category	Strategy Risk Number
Legacy	0.7.1, 0.7.2, 10.7.2, 29.7.1

Category	Strategy Risk Number
Organisation and institutional issue	0.15.2, 0.15.3, 0.15.4, 0.15.5, 2.15.1

Category	Strategy Risk Number
Politics	0.8.1

Category	Strategy Risk Number
Privacy	0.9.1, 0.9.2

Category	Strategy Risk Number
Safety	0.10.1, 0.10.2, 13.10.1, 13.10.2, 16.10.1

Category	Strategy Risk Number
Stakeholder Acceptance	0.11.1, 0.11.4, 27.11.1, 27.11.2

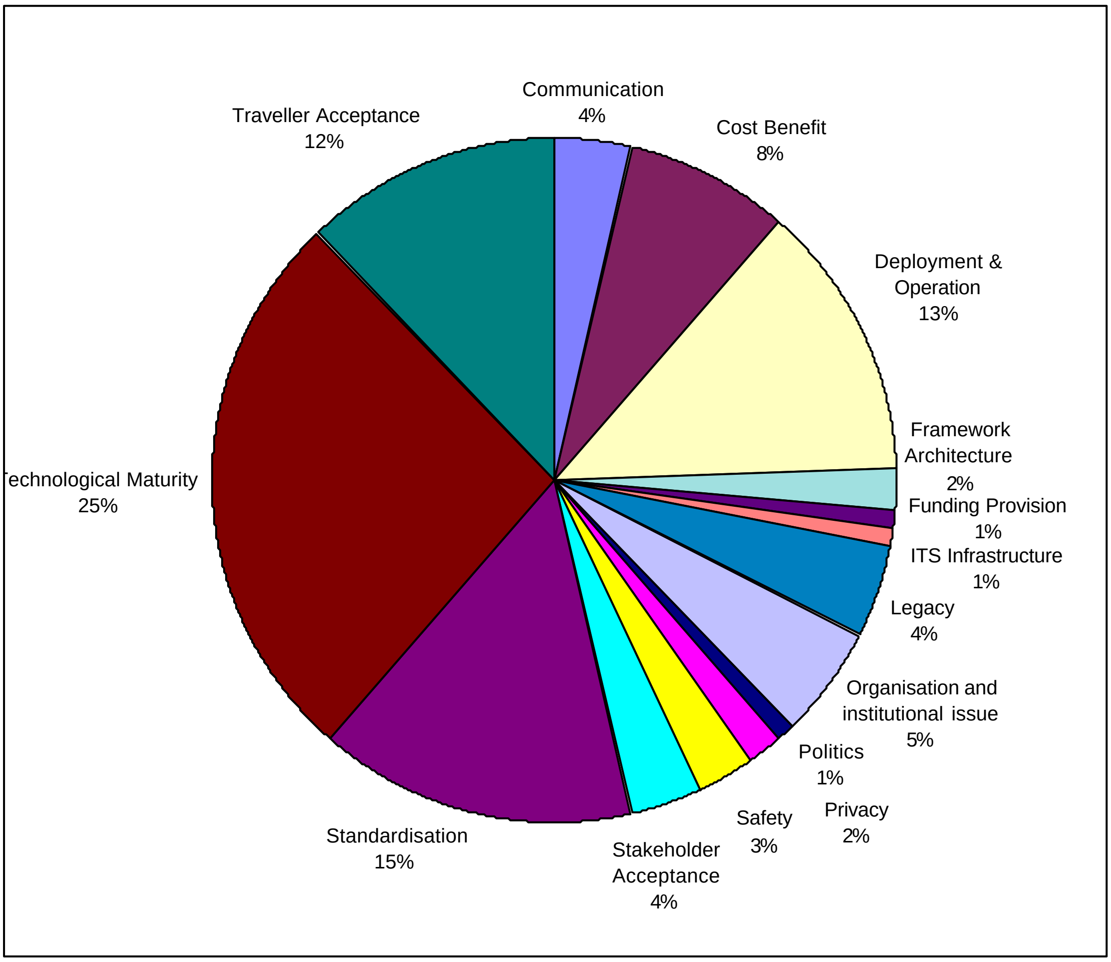
Category	Strategy Risk Number
Standardisation	0.12.1, 0.12.2, 0.12.3, 1.12.1, 1.12.2, 9.12.1, 9.12.2, 13.12.1, 16.12.1, 29.12.1, 29.12.2, 30.12.1, 31.12.1, 32.12.1

Category	Strategy Risk Number
Technological Maturity	8.13.3, 8.13.5, 9.13.2, 9.13.4, 10.13.1, 10.13.2, 10.13.3, 10.13.4, 11.13.1, 11.13.2, 12.13.1, 13.13.2, 13.13.3, 13.13.4, 14.13.1, 15.13.1

Category	Strategy Risk Number
Traveller Acceptance	0.14.2, 0.14.3, 0.14.5, 1.14.1, 9.14.1, 14.14.1, 15.14.1, 22.14.1, 23.14.1, 24.14.2

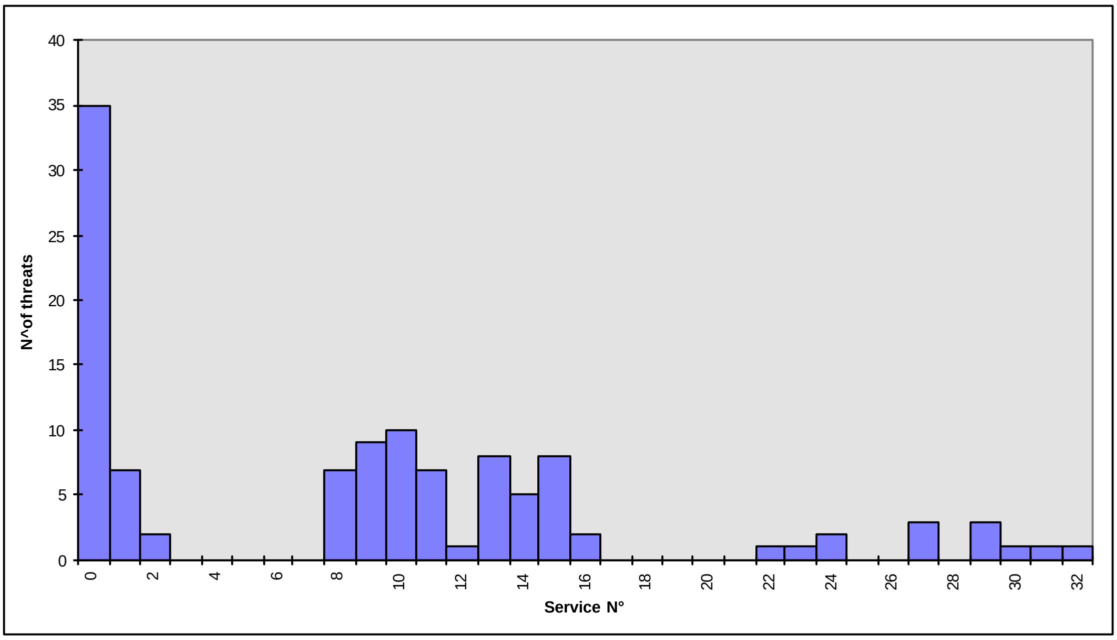
4. STATISTICALLY EDITED RESULTS

This section contains the statistical evaluation of the threats identified by RAID. The distribution of the threats among the risk categories is shown in picture A below.



Picture 2C.2: Distribution of threats according to their Category

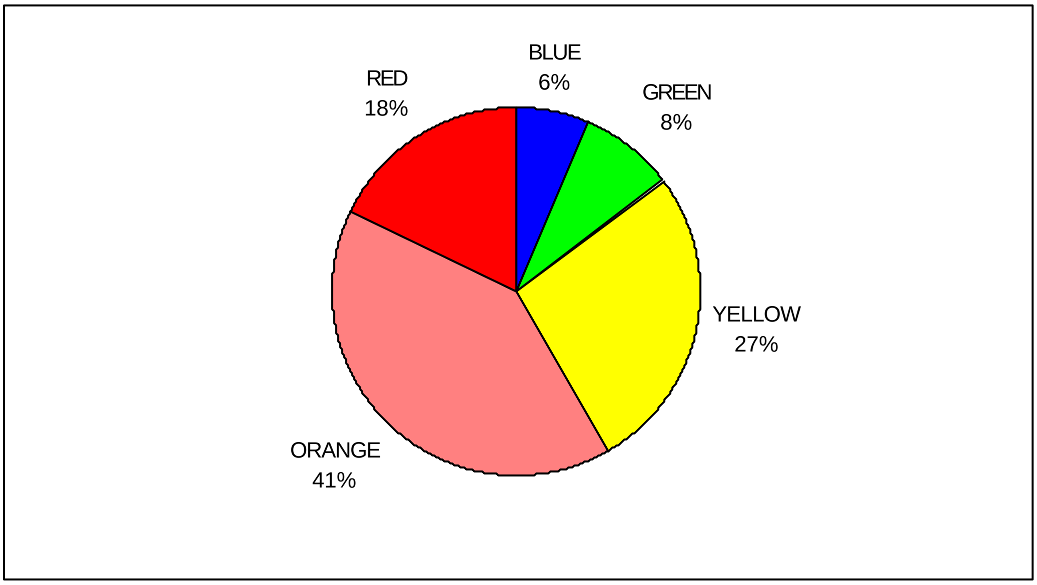
Many threats relate to technology. This could give the wrong impression that a focus of efforts on technology would be sufficient to support ITS system development and deployment. Political support for new R&D, especially in the field on vehicle advanced systems has to be promoted. Stakeholders and end-users have to be informed about potential benefits of ITS by objective information.



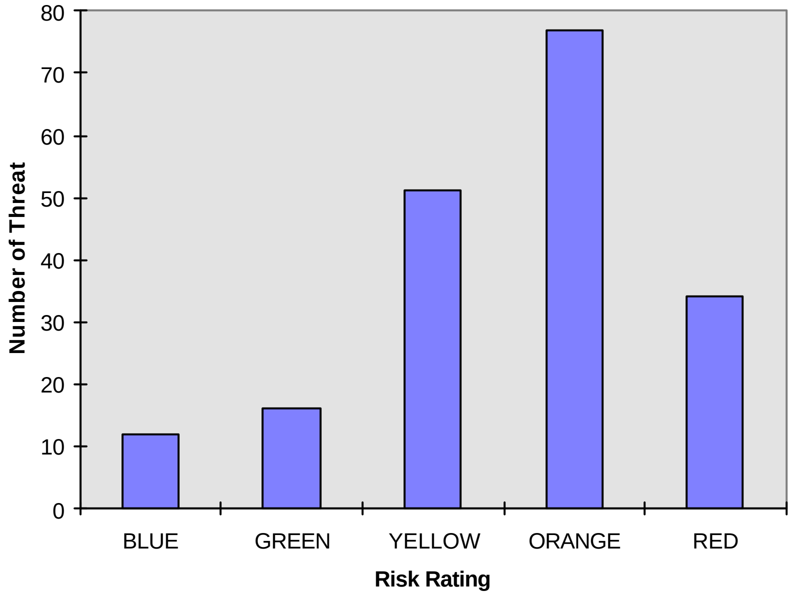
Picture 2C.3: Distribution of threats according to their Services (please refer to Annex 2A for a complete list of services)

It can be seen that the general service holds by far the most threats. Some services do not hold threats because those threats are already covered in service '0' (the general service). This means that many common threats are endangering the implementation of very different services.

The next two pictures show the distribution of the threats according to the rating given by the Risk Rating Scheme.



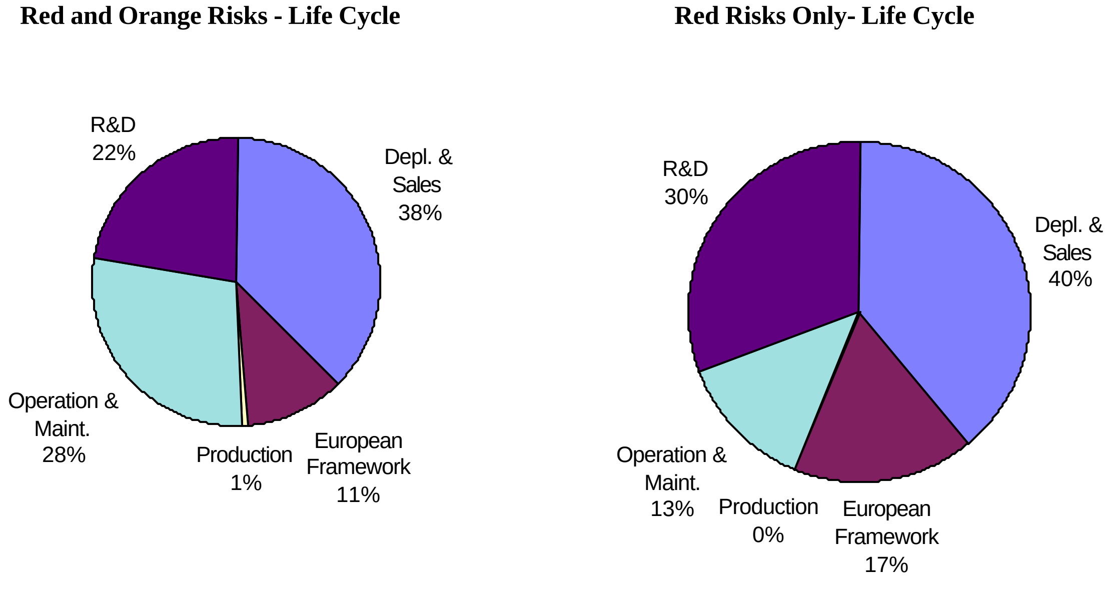
Picture 2C.4: Distribution of threats according to their rating (percentage)



Picture 2C.5: Distribution of threats according to their rating (amount)

The distribution of the threats is according to the Gaussian curve transposed a little bit to the higher risks. This reflects that the team followed a cautious approach in rating the threats. Thus, it is obviously possible to leave out blue, green and yellow threats from the process of developing mitigation strategies.

The next picture shows the distribution according to the Life Cycle status using the definitions described in Annex 2A.

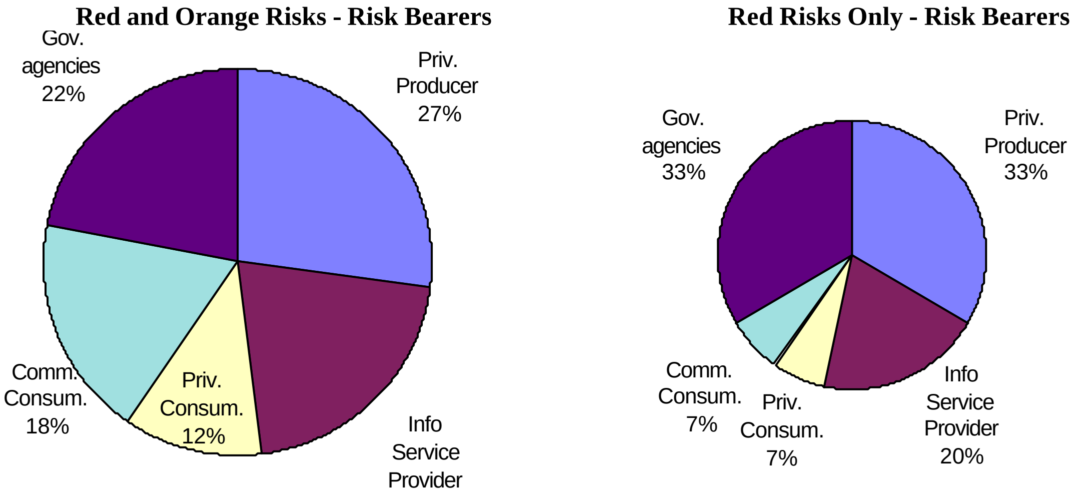


Picture 2C.6: Distribution of threats according to their Life Cycle Stage

It can be seen that not many threats were allocated to the Framework Architecture Life Cycle stage. Only one threat (i.e. ‘It will not prove possible to produce a cost effective vision enhancement system that can be fitted to all vehicles for use by all physical sizes of drivers.'), which is orange, was associated with the production life cycle stage. This threat is specifically related to one special application. Therefore, it can be concluded that production is not a field with major threats in the development of ITS systems.

A majority of threats appears in the Deployment & Sales stage. Well founded promotion to apply ITS and financial aids to install ITS where public interests are met by ITS could help to overcome this.

The next picture gives the distribution of threats according to the risk bearers (for definitions see Annex 2A**)**.



Picture 2C.7: Distribution of threats according to the Risk Bearers

Private Producers and Government are important Risk Bearers. Regarding the importance of the risks it becomes clear that the authorities role is a very important one. Almost one third of the red risks are bared by Government Bodies. Concerted actions of Private Producers and Governments should be considered in order to establish efficient mitigation measures.