2A – DATABASE DESCRIPTION

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 to lower the Risk effect,
- The possible deployment scenarios and the mitigation strategies that are consequently derived if they were applied.

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.
The list of attributes - Field of information - chosen for describing a Risk is provided in the following table.

Field of information	Explanation
Service Number	As per the Number for each Service in the ISO/TC204 document (from 1 to 32) plus service ″0″.
Service Description	As per the title of each Service in the ISO/TC204 document plus service 0 "General".
Category	Describes the category in which the threat has been identified. They are 14 different categories.
Threat Number	A Threat Number is defined for each threat. It is made up of three digits, the Service Number, the Category Number (labelled from 1 to 14), and the threat identifier itself.
Threat description	Description of the threat.
Consequences of the Threat	Description of the consequences as a result of the threat.
Life cycle	Describes the life cycle stage when the threat might occur.
Risk Bearers (stakeholders)	The group of stakeholders most likely to bear the threat.
Probability of Occurrence	This describes the probability of the occurrence of a threat. There are three levels of occurrence: low, medium and high.
Explanation of the Probability of Occurrence	In this column the Probability of Occurrence has to be justified by giving the reason for the choice
Level of Impact	This described the impact that the threat will have. There are three levels of impact: low, medium and high.
Description of the Level of Impact	In this column the level of Impact has to be justified by giving the reason for the choice.
Risk Rating Scheme	This column describes the Risk Rating resulting from the Risk Rating Scheme.
Strategy Risk Number	Strategy number, expressed as the number of the Risk to which it relates.
Strategy Sequence Number	Strategy number, expressed as a numerical sequence and independent of the Risk related number
Strategy Action (1)	The first Strategy action.
Strategy Action By Whom (1)	A two or three letter code for the organisation that must take the first Strategy action.
Action Category (1)	The category of the first Strategy action.
Strategy Action (2)	The second Strategy action.
Strategy Action By Whom (2)	A two or three letter code for the organisation that must take the second Strategy action.
Action Category (2)	The category of the second Strategy action.
Strategy Action (3)	The third Strategy action.
Strategy Action By Whom (3)	A two or three letter code for the organisation that must take the third Strategy action.
Action Category (3)	The category of the third Strategy action.

Field of information	Explanation
Strategy Action (4)	The fourth Strategy action.
Strategy Action By Whom (4)	A two or three letter code for the organisation that must take the fourth Strategy action.
Action Category (4)	The category of the fourth Strategy action.
Strategy Action Type	The Strategy action type, expressed as a two letter code.
Scenario Number	List of the Scenarios (Numbers) that are related to the threat.

Table 2A.1: Contents of database

A detailed description of each attribute follows.

1 Service number and Service Description

The Risks need to be structured in a easy and logical way. The structure needs to be understood by the ITS specialists.

Different alternate solutions could have been chosen for structuring the risks. The list of services selected as reference for the definition of the Risk clustering is that produced by ISO [1]. In addition to these 32 Services, it was important to add another service, ″General″, or ″Service 0″, that allows to cluster Risks which are not bound to a specific ISO service or that are applicable to all the services.

Thus in the previous table the attribute ″Service Number″ can take values from 0 to 32. The attribute ″Service Description″ is the name of the service as described in [1] for the values from 1 to 32. It uses the name ″General″ for service 0. The ISO List of Services is given in Annex B for information.

2 Category

A service allows Risks to be classified according to the final user point of view. Thus a Risk will be viewed in terms of what a user will get from the system used to provide the service.

A category is for RAID another means to classify a Risk. As noted in section 3.1 a Risk can be technical or non technical. Below this high level of separation, there exists a lower level, the categories. For RAID the categories are identified according to the types of issues with which the different ITS stakeholders need to deal. This is the main criteria for defining them.

A category also enables an ITS general topic, to which a Risk belongs, to be highlighted. The list of categories was finalised once the Risks themselves were identified. The number of Risks associated to a category value gives an indication of its importance. A total of 14 categories have been identified. They are given below together with their meaning.

Category	Category Number	Description
Framework Architecture	1	A Risk belongs to this category when it describes a ITS issue that is not expected to be covered by the Framework Architecture. An Example is ″All existing transport policies are not included in the Framework Architecture″.
Communication	2	A Risk belongs to this category when it describes a data exchange mechanism not widely accepted or deployed. An example is ″Different areas in Europe use different data communication mechanisms″.
Cost & Benefits	3	A Risk belongs to this category when it describes a situation that may affect ITS systems, such as development, implementation or deployment, that does not provide a sufficient return of investment. An example is ″There is no payback in deploying ITS services on secondary transport axes″.
Deployment & Operation	4	A Risk belongs to this category when it describes a situation that will negatively affect ITS system Deployment and Operation. An example is ″Only a small number of vehicles will be equipped with automatic operation functionality.″.
Funding Provision	5	A Risk belongs to this category when it describes a situation that results in a lack of funding in order to support the Framework Architecture deployment. An example is ″Non-ITS interest groups may be powerful enough to limit national funds″.

Category	Category Number	Description
ITS Infrastructure	6	A Risk belongs to this category when it describes the difficulty in funding, developing, deploying or maintaining ITS Infrastructure. An example is ″Installed infrastructure rapidly becomes obsolete″.
Legacy	7	A Risk belongs to this category when it describes a situation that deals with the migration of existing ITS systems under a Framework Architecture. An example is ″There are many systems in existence that support electronic transactions″.
Politics	8	A Risk belongs to this category when it describes a situation related to politics influence on the Framework. An example is ″Due to the subsidiary principle, the EU is not able to release directives obliging Member States to make use of certain systems or to promote or support certain ITS services.″.
Privacy	9	A Risk belongs to this category when it describes a situation which affects individual privacy. An example is ″Existing legislation in respect of privacy and data protection is not complete enough″.
Safety	10	A Risk belongs to this category when it describes ITS services which do not provide an appropriate safety level. An example is ″Poorly designed in-vehicles systems and information can affect driver behaviour″.
Stakeholder Acceptance	11	A Risk belongs to this category when it describes a situation not compliant with a stakeholder interest. An example is ″Industries want to sell their own system and establish their own standard and also protect their market shares″.
Standardisation	12	A Risk belongs to this category when it describes a situation related to a missing or not used standard. An example is ″Failure to approve and implement European standards in the appropriate time window will create an opportunity for non-European companies″.
Technology Maturity	13	A Risk belongs to this category when it describes a situation related to a maturity lack for a required technology. An example is ″Sensors to accurately detect the numbers of travellers using different transport modes will be unavailable″.
Traveller Acceptance	14	A Risk belongs to this category when it describes a situation which can not be accepted by a traveller. An example is ″ITS systems do not take into account the specific needs of impaired people″.
Organisation and Institutional Issues	15	A Risk belongs to this category when it describes a situation related to the cooperation between different actors. An example is ″... the allocation of roles and responsibilities for the provision of ITS services is the subject of competition by Government agencies ...″.

Table 2A.2: Numbering of the categories

Each Category is given a specific number regardless of the service in which it appears..

3 Threat number, Threat description, Consequence of the Threat

A threat is an element of the environment that generates an adverse outcome and it is part of a risk description. It is defined in two parts, one describing the threat itself and one describing the direct consequences of the threat. The first is the attribute ″Threat Description″ and the second is the attribute ″Consequence of the Threat″.

A threat has a unique number made of three (3) digits in the form ″A.B.C″ where:

- A″ is the service number ranging from 0 to 32
- B″ is the category number ranging from 1 to 14
- C″ is threat identifier for the pair ″A.B″.

″A.B.C″ is represented by the attribute ″Threat Number″.
Since a service does not necessarily contain the 14 categories, the numbering of the threats within a service may not always be continuous.

4 Life Cycle

In order to depict the point of time in which the threat may occur the following life cycle stages (with abbreviations) were defined:

Stage	Definition
European Framework (EF)	Covers the period of the implementation of the KAREN Framework Architecture.
Research and Development (R&D)	Covers the period that starts when an idea is conceived through the proof-of-concept to the development of a prototype of a system.
Production (P)	Covers the period during manufacture or construction of a system to provide all or part of an ITS service.
Deployment and Sales (D&S)	Covers the period during which the system is being marketed, sold, and installed.
Operations and Maintenance (O&M)	Covers the period after installation when a system is in operation providing an ITS service and is being routinely maintained and repaired, if necessary.

Table 2A.3: Life cycle stages

5 Risks Bearers (Stakeholders)

The following table gives the threat bearers (with abbreviations) which were defined:

Risk Bearer	Definition
Government agencies (G)	European, National, Regional and Local agencies with primary responsibility of governing, regulating, managing, and funding ITS.
Private Producers (PP)	Manufacturers or builders of ITS related products, financed by the private sector or funded by government agencies, motivated by profit or fee.
ITS Service Providers (ISP)	Providers of ITS services. They cover for example information provider for traveller, booking services, payment. They are either financed by private institutions and motivated by service fee, or contracted by government agencies to provide ITS services for a fee.
Commercial Consumers (CC)	Users of the ITS while playing their business.
Private Consumers (PC)	Users of the ITS for personal purposes.

Table 2A.4: Risk Bearers

6 Probability of Occurrence, Level of Impact and Risk Rating Scheme

As described above the probability of occurrence and the level of impact formed the basis for the threat assessment. The definitions for both are given below.

Probability of Occurrence	Description of the Probability
Low	The Risk is not likely to occur.
Medium	Risk is likely to occur.
High	The Risk is (almost) certain to occur.

Table 2A.5: Probability of Occurrence

Level of Impact	Description

Level of Impact	Description
Low	Insignificant or negligible impact.
Medium	Will result in "significant" disruption of systems based on the KAREN Framework Architecture or to system implementation, increase of costs, degradation of performance or a delay of implementation.
High	Will make the implementation of the systems based on the KAREN Framework Architecture impossible.

Table 2A.6: Level of Impact

From both results depicted on the previous page, the Risk Rating Scheme is derived. This is shown in the table below.

Risk Rating	Probability	Impact
Red	High	High
Orange	High	Medium
	Medium	High
Yellow	High	Low
	Medium	Medium
	Low	High
Green	Medium	Low
	Low	Medium
Blue	Low	Low

Table 2A.7: Risk Rating Scheme

7 Scenario Number

Only the threats rated as severe are considered. By severe it is meant the threats rated ″RED″ or ″ORANGE″. Please see Table I: Risk Rating Scheme for the rating definitions.

A scenario number is made of four digits, ″ABCD″, where ″A″ describes the ″Geographical Scope″, ″B″ the ″Main ITS trends″, ″C″ the ″Public/Private Co-operation, ″D″ the ″Time Horizon″.

Each digit relates to the different possibilities, either elementary or combinations. Each digit is presented in the table as a decimal number (this is, and at most, ranging from 0 to 9). But it relies upon a binary basis representation.

The table that follows gives for each digit A, B, C the possibilities together with the binary and decimal representation. The meaning of the abbreviations used in the table are as follows:

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
- Pub: public sector is the driving force of 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

Geographical Extension

- Inter, Urb, Rural: stands for interurban, urban and rural respectively.
- Time Horizon
- 2002: KAREN framework is issued
- 2005: maturity of the KAREN framework
- 2010: the KAREN framework has to be revised significantly

A	²Geographical Scope²

Possibilities	Binary Representation	Decimal Representation
Rural	001	1
Inter	010	2
Inter + Rural	011	3
Urb	100	4
Urb + Rural	101	5
Urb + Inter	110	6
Urb + Inter + Rural	111	7
B ²Main ITS trends²		
Possibilities	**Binary Representation**	**Decimal Representation**
Dman	001	1
Ctrl	010	2
Ctrl + Dman	011	3
Inf	100	4
Int + Dman	101	5
Inf + Ctrl	110	6
Inf + Ctrl + Dman	111	7
C ²Public / Private Co-operation²		
Possibilities	**Binary Representation**	**Decimal Representation**
Mix	001	1
Priv	010	2
Pub	100	4
D Relates to the ²Time Horizon²		
Possibilities	**Binary Representation**	**Decimal Representation**
2002	100	4
Up to 2005	110	6
2005 Onwards	011	3
2010 Onwards	001	1
All	111	7

Table 2A.8: Scenario Numbering Scheme

Examples of possible Scenario values:

- 7147 = all geographic scopes, ITS deployment for traffic demand management , public funding and all time frames
- 1723 = rural geographic scope, no ITS deployment effects, private funding, and year 2005 onwards time frame
- 6217 = urban and inter-urban geographic scope, ITS deployment for Telematics infrastructure provision, mixed public and private funding and no time frame impacts

8 Strategy Numbering

There are two numbers for each Strategy. They are stored in the "Strategy Risk Number" and "Strategy Sequence Number" fields.

The first number is based on the Risk number. It is built by adding "A" to each Risk number for its first Strategy. The second Strategy adds "B" in place of the "A", and so on if the Risk has more than two Strategies. Examples are: 0.3.2A, 28.13.1A, 28.13.1B, etc.

The second number is an independent number. It starts at "1" for the first Strategy for the first Risk and increases sequentially to "2", "3" and so on for each subsequent Strategy.

9 Components of a Strategy

There are four (4) components to a Strategy:

1. the mitigation action to be carried out by the Strategy;
2. strategy actors which is the list of organisations involved in the action implementation;
3. the action category;
4. the Strategy action type.

The components (mitigation action, bearer, category) are in coupled groups of three (3), i.e. the three components in a group are related to each other. There is a minimum of 1 such group per strategy and a maximum of 4. For each group none of its 3 components is empty.

In the Risk table, each mitigation action is stored as the "Strategy Action" attribute, whilst the strategy actors are stored as the "Strategy Action By Whom" attribute. There may be several strategy actors for one action. The action category is stored as the "Action Category" attribute. Each group of three attributes is identified by a suffix number, e.g. (1), (2), etc.

The strategy actors considered, together with their code, are the following :

Strategy actor	Code
European Commission	EC
National Government	NG
Public Transport Operator	PTO
Local Authority (State, City, Municipality, County, etc.)	LA
ITS Service Provider (Motoring Organisation, Tour Operator, Travel Service Provide, etc.)	ISP
Emergency Service Provider	ESP
Freight Operator (Freight Handling Company, Road Haulage Company, etc.)	FO
Manufacturing Industries	MI
KAREN Project	KP
Road Operators	RO

Table 2A.9: Strategy actors

The action category is a means by which Strategy mitigation actions can be clustered. Ten (10) possible values have been identified :

Action Category Values	Action Category Description
1.	Ensure KAREN Architecture is capable of being evolved
2.	Enforce KAREN Architecture Adoption
3.	Enforce European ITS Deployment
4.	Adopt ITS Systems Common Requirements
5.	Fund Research and Standardisation
6.	Define Secondary Axes Policies
7.	Define Data Control & Exchange Policies
8.	Address Competencies Issues
9.	Promote ITS & Define Pricing
10.	Define ITS Failure Policies

Table 2A.10: Action Category Values

The Strategy action type is stored as the "Strategy Action Type" attribute in the Risk table. There is only one of such an attribute per Strategy which means that for a given Strategy all its mitigation actions have the same type.

The mitigation actions in a Strategy can be one of two types: Risk Control or Risk Avoidance. The first is used where it is required to ensure that the Risk does not happen, or have its impact. The second is used when the Risk cannot be prevented from happening and action is needed to reduce the impact. Two letter codes are used: RC for Risk Control and RA for Risk Avoidance.