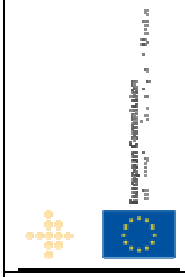
Cooperative Vehicle-Infrastructure Systems

D.CVIS.6.1 Non-technical validation elements

SubProject No.	**SP.1.3**	**SubProject Title**	**DEPN**
Workpackage No.	**WP 6**	**Workpackage Title**	**Validation**
Task No.	**NA**	**Task Title**	**NA**
Author(s)		**Thijs de Graaff**	
Dissemination level PU/PP/RE/CO		**PU**	
File Name		**DEL_CVIS_6.1_Nontech_Validation_Elements_v 1.0.doc**	
Due date		**30 August 2007**	
Delivery date		**24 August 2007**	

Abstract	An exercise was carried out to identify issues related to non technical validation elements (NTVE's) expressing the deployability of CVIS. This work has been done using the intermediate results available from the various topics in the DEPN

	Project supported by European Union DG INFSO IST-2004-2.4.12 eSafety – Cooperative systems for road transport
Project reference	FP6-2004-IST-4-027293-IP
IP Manager	Paul Kompfner, ERTICO – ITS Europe Tel: +32 2 400 0700, E-mail: cvis@mail.ertico.com

	sub-project.

Control sheet

Version history			
Version	**Date**	**Main author**	**Summary of changes**
0.1	7-May-07	M.P. de Graaff	Initial
0.2	29-May-07	M.P. de Graaff	T8 contribution added
0.2pk	6-Jun-07	P Kompfner	PK comments
0.3tdg	4-Jul-07	M.P. de Graaff	Comments processed; NTVE's numbered
0.3	17-Jul-07	M.P. de Graaff	Text clarity improved
	Name		**Date**
Prepared	Thijs de Graaff		7-May-07
Reviewed	Mariana Andrade		24 August 2007
Authorized	Mariana Andrade		24 August 2007

Circulation	
Recipient	**Date of submission**

Table of Contents

Abbreviations and Definitions

Abbreviation	Definition
ADAS	Advanced Driver Assistance Systems
CVIS	Co-operative Vehicle Infrastructure Systems
DEPN	CVIS Deployment Enablers subproject
IP	Integrated Project
ITS	Intelligent Transport Systems
NTVE	Non-Technical Validation Element
QoS	Quality of Service
TCO	Total Cost of Ownership
OEM	Original Equipment Manufacturer (meaning automotive manufacturers)

Executive Summary

The DEPN subproject of the CVIS integrated project (IP) is treating (in seven separate "topic groups") some of the most significant non-technical issues for the development and deployment of cooperative vehicle-infrastructure systems. As part of the DEPN activities this early deliverable reports on an exercise to identify non-technical validation elements to be treated in the CVIS project validation process, mainly based on field trials at six test sites.

By their nature non-technical validation elements (NTVE's) may not be evident or explicit. Besides, quite a few emerge from the environment (systems, organizations, regulations, policies, etc.) within which CVIS will operate in the future, and it is difficult to define them. The task for the various topic groups in DEPN was to envision the future CVIS world and identify the non-technical issues likely to arise in that world.

Translation of non-technical issues into unambiguous, simple requirements and related criteria appears to be impracticable. Validation of specific, and often technical CVIS outcomes against an inventory of non-technical issues is likely to take the form inspection of meeting notes of interviews or discussion forums, with the validation elements as discussion topics.

This work is based on the interim results from the technical development activities in the various CVIS sub-projects.

1. Introduction

The CVIS project is developing a hardware and software reference platform to enable vehicle-to-vehicle and vehicle-to-infrastructure communication, and application software for a number of example test cases. The system design is based on user needs and system requirements already derived early in the project term. The hardware and software will be tested in six test sites across Europe.

The validation process is focused on the test site results. These will be mainly directed at the technical and functional evaluation of the system, but will include as far as possible an assessment of the effects of the various applications on, and benefits for users. While some of these impacts will be "technical", i.e. time, cost or energy savings, others will be more or less unquantifiable – but potentially very significant for future deployment.

As the validation process follows a bottom-up approach, the requirements do not necessarily indicate how to approach the validation of non-technical issues. Many of these issues concern a future CVIS world and are not really suitable for validation in the CVIS project lifetime.

This future CVIS world is best understood from a business rather than a technical viewpoint. The context is one of business partners having incentives and intentions, using business models, interacting using business information and with all the constraints normally occurring in a real world situation.

As an early task of DEPN, an early exercise was carried out to identify issues related to non technical validation elements (NTVE's) expressing the deployability of CVIS. This work has been done using the intermediate results available from the various topics in the DEPN project.

2. The procedure followed in the compilation process

The compilation of non-technical issues into an inventory for validation has followed the individual topics of DEPN:

T2 – Openness and interoperability

T3 – Safe, secure and fault-tolerant design

T4 – Utility, usability and user acceptance

T5 – Costs, benefits and business models

T6 – Risk and liability

T7 – CVIS and policy

T8 – Deployment maps

Experts of the various DEPN topics have brought in issues according to their own expertise. Naturally, general CVIS requirements will be reflected in their contributions. During this compilation process various perspectives were used, like End User, Authority and OEM. The issues that have been identified are expressed as a requirement. In this way they should input to and help guide the validation process, but are not intended as a rigorous addition to the validation methodology. The work needed to arrive at clear validation actions, like interpretation of the individual NTVE toward the different CVIS subprojects and specifying the validation criteria that go with it, is considered to be a task for WP6 when making the Validation Plan.

3. CVIS Non-technical validation elements

3.1. T2 – Openness and interoperability

the high and low level architectural design of CVIS must be such that:

a. An end user can trust that CVIS will appear to be a performing system over the years, functioning as a extendable package of solutions for his ITS needs.
b. An end user can expect from CVIS to provide a service environment that allows the incorporation of extra services from any organisation that supports CVIS.
c. An end user can use and access simultaneously multiple relevant services.
d. An end user can add new services to the environment without disturbing the existing services.
e. To support its policy making an authority can expect the CVIS system and the future development to stay "lean-and-mean", so that new policies can easily be implemented.
f. The CVIS system should be flexible enough to support policies of the various authorities in any country in Europe.
g. CVIS should be interoperable with legacy systems, safeguarding long-term investments.
h. The implementation of policies and regulations will be interoperable between different member states of the EU adhering to the CVIS concept.
i. The overall CVIS infrastructure leaves an open and flexible way for information to be exchanged between stakeholders (typically being 'hosts')
j. CVIS will offer a good outlet for an OEM's products and with a good price/performance ratio.
k. CVIS helps an OEM to retain its competitive edge.
l. CVIS gives an OEM better market opportunities.
m. CVIS offers handy, well documented and understandable interfaces.
n. An OEM or service organisation can freely choose between own development and buying 3rd party system components when developing CVIS based services.
o. CVIS offers an easy organisational operation to an OEM.
p. An OEM will be capable of offering custom-made parts in addition to a CVIS compliant product.
q. An OEM will be able to connect to the CVIS system easily and in a user-friendly way.
r. An OEM will not be obliged to obey requirements enforced by its competitors.
s. When developing CVIS components, an OEM will be free to use its own trusted field of development and the language it uses in that domain.
t. When an OEM obtains CVIS components from other vendors, these will work directly (plug-and-play).

3.2. T3 – Safe, secure and fault-tolerant design

the design must be deliberately and demonstrably such that an end-user can trust CVIS in safeguarding:

a. the performance of the enabling technical platform in relation to the performance as required by the various services;
b. the accuracy and precision of positioning data;
c. the integrity of any measured data;
d. its privacy;

e. the integrity of the data as exchanged with other end-users;
f. the trustworthiness of other end-users it is cooperating with by obliging any such end-user to identify, authenticate and authorize themselves;
g. the responsibilities of other end-users by making it hard not to say impossible to repudiate the outcome of a cooperation transaction, e.g. an information exchange at a toll booth;
h. that any cooperative activity not be disrupted by intruders;
i. the continuity of both the enabling technical platform and the services by being able to withstand a complete service (application) interruption and invoke a subsequent recovery in the event of failure of physical components;
j. the durability of both the enabling technical platform and the services by being able to withstand a partial or gradual degradation in service that would occur in the event of failure of some of the physical components of the distributed system;
k. the recovery of both the enabling technical platform and the services by being able to recover from a complete service interruption with no additional manual effort;
l. the consistency of both the enabling technical platform and the services by being able to realize the same results given the same data and processing criteria in any case.

3.3. T4 – Utility, usability and user acceptance

a. The end user can use all relevant information in an easy and logical way. No difficult instructions shall be needed. The interface should thereby not depend on the car type. (Clear human machine interface)
b. the design must be such that when using CVIS the user will not be distracted from the main driving task in such way that dangerous situations might occur. (Situational awareness)
c. the design must be such that when CVIS is not working properly or there is no information available users must be informed about this (high integrity of the system to improve trust in the system)
d. it should have been taken care of in the architecture that during the transition phase towards a full scale CVIS system the end user should already see the benefits of the system (Acceptance)
e. an investigation must have been carried out whether CVIS systems will increase a driver's workload

3.4. T5 – Costs, benefits and business models

a. The CVIS system should produce benefits for congestion, throughput and emissions with respect to the present situation even in the case that people are stimulated to use their car more often. An reasoning and/or fact finding must have been done in this respect.
b. an investigation must have been made what the current spending of stakeholders is on similar systems, e.g. road side equipment
c. a discussion must have been held what could be the quick-wins with CVIS
d. an investigation must have been made whether the stakeholders are prepared to pay for the CVIS equipment
e. an investigation must have been made whether CVIS has the potential to become an environment in which commercial services are being operated

f. an investigation must have been made what price the driver is prepared to pay for CVIS services
g. an estimation must have been made what the total cost of CVIS would be if implemented in large scale across Europe
h. an investigation must have been done as to what business models should be applied to put CVIS onto the market
i. a discussion must have been held which tangible commercial benefits the stakeholders will have when implementing CVIS, and whether it will be measurable anyway
j. an estimation must have been made what the pay-back period for CVIS will be
k. an investigation must have been done what the initial cost for CVIS and the yearly maintenance cost will be. This should be measured according to the TCO (Total Cost of Ownership) model.
l. an investigation must have been made what the (price) trends are in the technology and how CVIS can benefit from them
m. a discussion must have been held what the additional commercial benefits are when CVIS is incorporated with other systems (tolling, navigation, eCall,…)

3.5. T6 – Risk and liability

a. an investigation must have been done which laws or standards (European or National) affecting CVIS are likely to be adopted in the near or long term, and how far these would relate to CVIS functions /architecture
b. an investigation must have been done which the legal and political fields are that influence (and/or could influence) CVIS customers, and whether they have been analysed
c. a concensus must exist and be documented about to what extent CVIS might be exposed to criticisms of consumers' associations
d. a discussion must have been held whether political or legislative tendencies could be used as advantages for CVIS
e. a discussion must have been held whether insurance companies could play a key role in promoting the use of CVIS technology, how they might react in case of CVIS technical malfunctions, and what might be their impact on CVIS functions / architecture / business model
f. the different standards / requirements across EU Member States must have been analyzed for relevance to CVIS technical issues
g. an inventory must have been created of external risks and threats to the safe deployment of CVIS systems and application projects, with mitigation strategies for the most significant risks
h. it must be clear how these risks are monitored and by whom during the course of the project
i. it must have been documented that the liability exposure of CVIS actors in the CVIS deployment and operational service chain has been researched and mapped according to National (e.g. English) law using selected Use Cases as scenarios
j. it must have been listed what the reaction has been of those CVIS Actors in relation to the liability exposure under a co-operative system, such as CVIS, as opposed to their current liability exposure - whether in respect of, for example, ADAS or as regards the way they normally conduct business
k. it must be clear how the legal liability mapping has been structured during the project phase and how the results have been taken into consideration by the technical sub-

projects to ensure that each Actor only carries legal liability for what he can actually control technically

l. there must be a list available of measures that might be put in place to limit the legal liabilities of CVIS Actors which have been identified as a consequence of this research
m. it must have been made clear how these measures could be made applicable to and accessible by the range of different Actors involved in CVIS
n. there must be a list available of findings in respect of the legal exposure of parties who certificate or otherwise attest to the compliance and efficacy of CVIS products/components and services and those who rely on their attestation
o. it should be clear how the insurability of the CVIS system and the Actors who are involved in its deployment is dealt with
p. it must be clear how a failure of the CVIS system, in whole or in part, will be dealt with and what financial solutions could be put in place to effect such restoration
q. there must be a list available of the legal issues that have been considered
r. sufficient confidence should have been provided that liability insurance for involvement in co-operative systems could be developed, if it is not currently available
s. safeguards must have been considered to prevent or minimise legal disputes as between different Actors within the CVIS system or if claims are made against the system by end users

3.6. T7 – CVIS and policy

- The following issues must have been discussed about effects of deploying CVIS:
  a. increase/decrease the risk of accidents
  b. change of the profile of accidents (e.g. create fewer but more serious accidents)
  c. change of the end users' perception of safety (e.g. encourage risk compensation)
  d. creation of additional hazards (e.g. driver distraction)
  e. attraction of the attention of malign groups or individuals, i.e. can someone gain from disrupting or distorting the operation
  f. clarity about responsibility for system security
  g. the consequences of lapses in security
  h. undermining of existing policy initiatives
  i. influence on cost-effectiveness of delivering existing and future policy initiatives
  j. capacity to extend the performance/target of a policy initiative
  k. capacity to resolve a conflict between policies (e.g. safety and environment)
  l. contribution in enabling local, national and international policy to be delivered more coherently
  m. creation of more winners than losers
  n. improvement of mobility
  o. contribution to a more open and competitive market
- The following issues must have been discussed about viability of CVIS:
  p. sufficient support from other market sectors, e.g. communications, ICT
  q. requirements for additional licensing or type approval
  r. support in its architecture for a clear division of liability

3.7. T8 – Deployment maps

a. The deployment of CVIS must likely be aligned with the apparent general changes in market perspectives for ICT. E.g. the following should have been considered:
   - Personal communication → new communication models

- ICT services → ICT capabilities for the emerging needs and process innovation
- Multimedia services → content through the broadband network
- Universal service → Telephony over IP
- IP interconnection between Operators for voice, data, video
- Network Provider/ Service Provider separation

b. CVIS has to support services responding to changes in transport market demand. E.g. topics should have been addressed like:
   - Evolution of the economical and regulatory framework
   - CO_2 and global warming
   - Infrastructure charging
   - Oil prices
   - European competitiveness

c. The availability of CVIS services should be sufficient and meeting the standards in the area of interest. In this respect discussions should have been taken place about e.g.:
   - Open interfaces
   - Third party applications
   - Services provisioning
   - Service adaptation
   - Service design

d. CVIS must take into account the evolution of opportunities of ICT. In this respect discussions should have been taken place about e.g.:
   - Speed, Access, high/distributed storage capability
   - All IP network platforms with QoS guarantee
   - Adoption of IT technologies - Service Oriented Architecture

e. The various deployment options must have been considered pertaining to local versus global aspects of CVIS, e.g.:
   - Automotive industry addresses a global market but deployment will also include local perspectives tied to local infrastructure, actors and processes

f. The balance of private and public CVIS services must be acceptable. Accordingly discussions should have been taken place about e.g.:
   - Deployment of commercial services related to publicly operated services utilizing same service delivery architecture

4. Conclusions and recommendations

A compilation of non-technical validation issues have been given from a deployment perspective and from a viewpoint of various stakeholders in the CVIS world. How to validate that those issues risen have been properly addressed within CVIS will be part of D-CVIS-6.2, the CVIS Validation Plan.

By their nature non-technical validation elements (NTVE) may be difficult to relate to (technical) performance criteria, and even more to quantify those criteria. Consider for example the non-technical validation element "*An end user can trust CVIS in safeguarding the accuracy and precision of positioning data*", formulated from the perspective of safe, secure and fault-tolerant design. Quantifying 'end user trust' in an objective way is not straightforward. Even more, different SPs will probably have different interpretations of 'trust'. Having noticed that we recommend the following.

Non-technical validation elements listed may occur more than one and they even may conflict with each other. This is not en error but is brought about by different interests of the various stakeholders, and reflect as such real life interest conflicts. To pass the validation well documented trade offs should have been made in case of such conflicts by the related CVIS subprojects. We recommend that in such case an inspection of the (sub)projects documents must be done.

When making the Validation Plan basically every NTVE should be considered by every subproject (including the CAG for validation on IP level whenever relevant) and decide on its relevance. If found relevant, the *interpretation* of the NTVE should be documented prior to the validation itself and also the validation criteria and procedure should be specified. Validation of NTVE's should be done based on criteria that should be as sharp as possible.

During validation (in case of 'soft' criteria) it must at least be clear and traceable in the documentation of the respective subprojects, be it meeting notes, architectural designs or any other (formal) document, how the relevant NTVE's have been addressed, and whether this is sufficient according to the applicable validation criteria. In difficult cases it might be considered to be sufficient if a traceable, understandable rationale can be found in the subprojects documentation, proving that the NTVE has indeed been addressed.

Annex(es)

[None]