

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/27353940>

Testing the untestable: Towards a pro-active safety assessment

Article · January 2008

Source: OAI

CITATIONS

0

READS

70

3 authors:



J.A. Stoop

Delft University of Technology

127 PUBLICATIONS 769 CITATIONS

[SEE PROFILE](#)



J.H. Baggen

Delft University of Technology

18 PUBLICATIONS 17 CITATIONS

[SEE PROFILE](#)



Jaap Vleugel

Delft University of Technology

91 PUBLICATIONS 304 CITATIONS

[SEE PROFILE](#)

Testing the untestable: towards a pro-active safety assessment

John Stoop¹, Jaap Vleugel, John Baggen

Delft University of Technology, Delft, the Netherlands

Abstract: Major infrastructural and transport projects are submitted to a multi-actor design environment, facing strict budget management considerations and contractual restrictions. By their nature, such projects are unique, often without a technological precedent, no operational experience and embedded in their specific social-economical context. Although testing of these components has reached a high level of maturity with respect to standardisation of performance limits and operational procedures, the integral safety performance of such systems is very hard to assess.

Testing such design concepts at an integral performance level is not possible. The variety of testing conditions is almost unlimited, while destruction of the object during testing is out of order. A collapse of the systems during operations is also unacceptable, due to the permanent loss of integrity and social and financial costs involved.

Based on a series of major infrastructure transport accidents, the concept of critical size events is developed. They represent the integral safety performance limits of complex systems, dealing with tunnel fires, derailment and terrorist attacks. In addition, critical events may occur in policy decision making processes. Public faith may be jeopardized during the design and construct phase if such decision making processes are flawed, potentially leading to Parliamentary Inquiries. This contribution elaborates on such decision making processes in the High-Speed Line railway development in the Netherlands.

Keywords: proactive safety assessment, transportation

1. INTRODUCTION

With the advantage of hindsight a picture emerges from the developments on the railways in which on one hand continuing a long tradition in railway design and national policy making has to be brought into balance with on the other hand technological innovation, European harmonisation and interoperability. The Netherlands is one of the countries that had chosen to invest in a new system of signalling safety, eventually to be deployed across Europe. Industrial tests were performed early on a new safety system, which actually only existed on paper. Partial known and unknown hazards were related to this development, contractually distributed across government and market parties. It is considered a token of courage to innovate in a period in which government retreats expecting market parties to take over the initiative to innovate. Based on recent experiences the pendulum seems to swing back with respect to market forces. With respect to the development of railway technology, in particular with major projects, a lasting role for government is desirable. Such a role comprises a role for an architect as well as a systems integrator. The relation between government and market parties can be formalised by a substantive assessment on performance and quality. So far, this assessment has focused on the nature of safety issues which reveal themselves as critical in the perception of the public and political decision making. During the design and construct of the High Speed Line railway, several of such safety critical events have occurred unexpectedly, such as the fires in the Channel Tunnel and Alp region, the derailment of a high speed train in Eschede in Germany and terrorist attacks on the metro systems in London and Madrid. These events have initially triggered several design modifications with sometimes major consequences for the rescue and fire fighting functionality and the availability of emergency resources for the operational phase of the High Speed Line project [1]. Such safety critical events eventually may trigger change at an institutional level. Due to the frequency and severity of the events, the European Commission issued a Directive on Tunnel Safety, in order to mitigate the consequences of these critical events.

¹ j.a.a.m.stoop@tudelf.nl; stoop@kindunos.nl

However, such critical events are not restricted to physical occurrences such as tunnel fire disasters, but also cover critical procedural and decision making events, causing loss of public faith in political, policy making and project management decision making issues. Delays in deployment of the ERTMS train signalling systems in the HSL railway project have caused such a critical procedural decision making event, due to which questions were raised in the Dutch parliament, without the occurrence of a previous disaster in practice.

A specialized team of independent experts from Delft University of Technology was composed in order to investigate the sequence of events and decision making processes which have lead to this safety critical procedural flaw in the development and implementation of the ERTMS signalling system.

1.1. Technology in development

In general, developing a major project such as the HSL with a high technology impact must be developed in phases. This comprises development, elaboration and implementation of new technical systems and applications. Due to the high degree of uncertainty in the beginning of a major project and the gradual accumulation of expertise and experience, intermediate adaptations and improvements are inevitable. Such a development is a continuous balancing of sense and utility for adaptation against expected delay and additional costs. This is not only a financial and planning issue.

The eventual goal of ERTMS is to guarantee safety at high speeds and to provide an undisturbed course of operational processes at the tracks themselves, transfers to other parts of the European High Speed network, the interconnections of the High Speed network and the mutual use of the regular infrastructure together with other rolling stock. High demands are put on availability, reliability and safety during a continued upgrading which will occur in the course of the life cycle.

Consequently, the questions raised do not only cover a unique issue during the development and implementation but may probably manifest themselves during future life cycles of the High Speed Line. In view of a life-cycle and availability approach, these issues raise deeper questions about the occasional or structural nature of present ERTMS issues.

Two major new railway projects were initiated in the past decade in The Netherlands, the Betuweroute dedicated freight railway between Rotterdam seaport and the Dutch-German border and the high-speed railway between Amsterdam Airport Schiphol and the Dutch-Belgian border to Antwerp (Belgium). Both projects were severely delayed. The Betuweroute railway was opened in the summer of 2007. Since then, only a very limited number of trains have used this railway. The high-speed railway to Antwerp is still not operational at all and it is not yet known when opening of the railway is due. Serious problems with respect to the installation of the European Rail Traffic Management System (ERTMS) are responsible for this situation.

This paper concentrates on the question whether the technical, institutional and organisational setting of the project was to a certain, maybe even considerable, extent responsible for this situation. It is mainly based on a study by a specialized team of Delft University of Technology for Dutch Parliament [2]. Parliament had the impression that the Ministry of Transport, Water Management and Public Works in the Netherlands, responsible for the management of the project in the Netherlands did not do its work well enough. It ordered an independent study dealing in particular with the following questions:

- How did the delays occur?
- Could these delays have been prevented and if so, how?
- What lessons can be learned from this project for new, large-scale infrastructure projects in the future?

1.2. European standardisation of railway signalling

European countries are working on harmonisation and standardisation of their national railway networks. This is a critical precondition for efficient cross-border (high-speed) railway traffic. Railway signalling is not standardised in Europe. More than twenty different signalling and speed control systems exist in Europe [3].

As a consequence, a train has to be equipped with all the systems used on the tracks in the countries it passes.

For instance, a Thalys trainset has seven different signalling systems on board: TVM (France), TBL (Belgium), LZB (Germany), ATB (The Netherlands), Crocodile/Krokodil (Belgium), KVB (France) and PZB/Indusi (Germany) [4]. TVM, TBL and LZB have been developed for use on high-speed railways and the other four systems are for use on conventional railways.

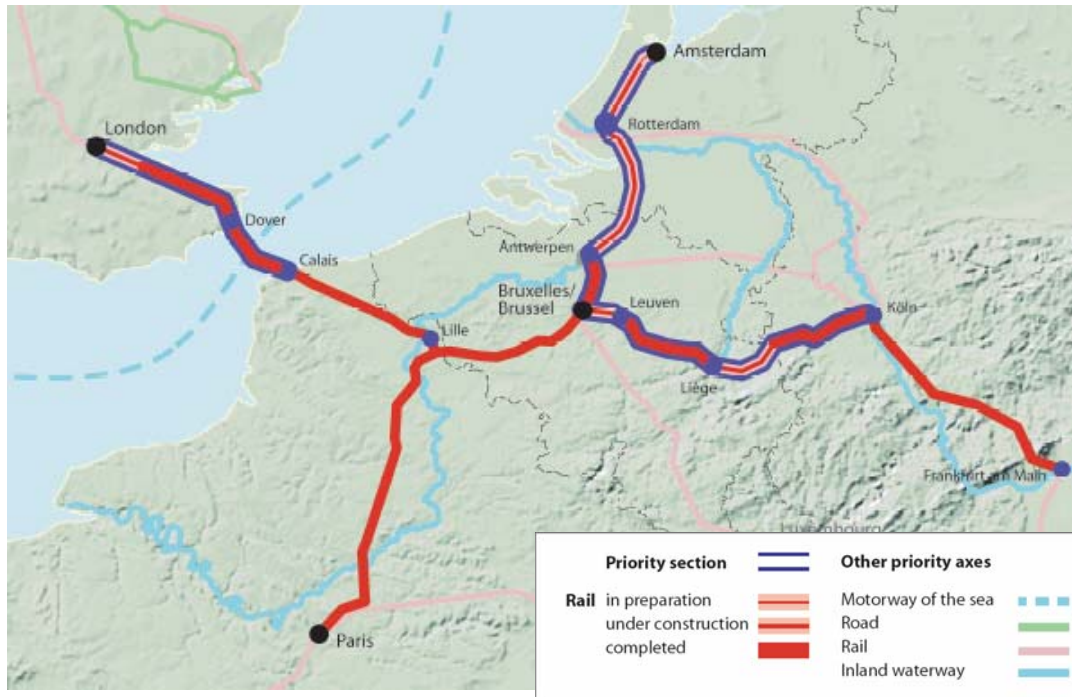


Figure 2: The high-speed railway Paris-Brussels-Cologne-Amsterdam-London
Source: EU, 2005

This large number of sometimes very different signalling systems unnecessarily complicates train protection (with a potentially negative impact on safety) and it strongly increases the purchase and maintenance costs of rolling stock and infrastructure [4].

1.3. Interoperability and the European Rail Traffic Management System (ERTMS)

European Rail Traffic Management System (ERTMS) is a system that consists of train control and communication, known as ETCS (European Train Control System), a dedicated mobile phone network for railways, known as GSM-R and the legal framework and operational procedures governing this system. ERTMS was proposed to become a European standard for railway signalling. In many countries in Europe and also in other parts of the world ERTMS projects have been started. Such projects will change the signalling system on one or more lines in a network. These ERTMS equipped lines can serve both national or international rail traffic.

Each country may have different motives to introduce ERTMS. SBB [5] mentions: development of a high-speed railway network (Spain, Italy, The Netherlands), interoperability (Belgium, Luxembourg), renewal (Austria, Hungary, Romania, Bulgaria) and development of a corridor (Germany, France). Various factors determine if and how ERTMS will be implemented: technical state of the art; traffic intensity and better use of capacity; quality of the network; the share of cross-border traffic and the financial situation in a particular country. The introduction of ERTMS is financially supported by the European Union.

Interoperability is a key issue for the Netherlands and Belgium. Interoperability is defined by Profillidis [6] as ‘the ability of a rail system to allow the safe and continuous operation of trains, under

achievement of specific performances'. In this case interoperability means that technical obstacles for cross-border rail traffic should disappear within a few decades.

The existing railway signalling system in The Netherlands was developed in the 1950s and installed throughout the network until the 1980s. It allows trains to operate with speeds up to 140 km/h. Operation of high-speed services demands the installation of dedicated high-speed equipment in both infrastructure and in rolling stock (e.g. cabin signalling instead of traditional track side signals).

ETCS consists of layers with different technical requirements and applications (Levels 1-3). A higher level involves less track side equipment, but more on-board equipment. This change also implies that the costs of the signalling system will migrate from the infrastructure providers to the train operators. Table 1 gives an overview of the three main levels and their function in ERTMS.

Table 1: ETCS Levels and their function

	Signalling	Train Detection
Level 1	infrastructure	infrastructure
Level 2	train	infrastructure
Level 3	train	train

Source: Wikipedia, 2007b

1.4. ERTMS and industry policy

In Europe the railway industry has some (regional) economic importance. Suppliers in Europe sell their technologies worldwide. The industry is dominated by a number of conglomerates. Technical standardisation demands co-operation between competitors. ERTMS is therefore a product of negotiations between experts in industry and regulation bodies in government. It is certainly not a product off the shelf to be used immediately, but much more a work in progress [7]. Step by step standards are being developed, which are subsequently translated into products for customers. Just like any other product there is a development trajectory, which takes a given period of time. Attempts to speed up technological development may cause negative consequences like higher costs or lower quality, which may later require re-engineering.

For the present signalling system Dutch railway infrastructure provider Prorail relies on (German) Siemens products. Siemens is also main supplier of the ICE-trains, which operate cross border services between The Netherlands and Germany. ICE-trains mainly use the German high-speed signalling system *Linienzugbeeinflussung* (LZB). This system is not compatible with the signalling system used by the high-speed trains connecting The Netherlands and France via Belgium. In these Thalys trains, among other systems, the French SNCF-owned *Transmission Voie-Machine* (TVM) system is used. LZB has a completely different safety philosophy (remote monitoring and management with the option of driverless trains) than used in France (with more autonomy for the train driver). In this perspective, the development of ERTMS could be regarded as a (political) compromise. To migrate to Level 1, Germany does not need to change much, while France tends to use two on-board high speed safety systems: the dual standard ('bi-standard') TVM430 and ERTMS Level 2. In order to migrate to Level 2, Germany and The Netherlands face a discontinuation with the past, while this is less the case in France and Belgium.

2. PARTIES INVOLVED AND THEIR RELATIONSHIP

In The Netherlands it was decided to develop the HSL-Zuid project in a public private partnership (PPP). This decision created a quite complex contract structure. The project was organised into three infrastructure projects and one transport project [8].

The Belgian HSL 4 project has a totally different main structure. Here traditional agreements were used instead of the Dutch project-based contracts

The Dutch choice for a PPP has met criticism. The Belgian choice for traditional agreements was based on decades of experience. Belgium has only recently started using PPP on a larger scale. More

in general in The Netherlands politics considered PPP as a goal as such [9] and not as a means to reach other goals.

The complex contractual situation in The Netherlands is one of the explanations for the technical differences between the Dutch and Belgian implementations of ERTMS. The functional specification left some freedom for interpretation. This in turn had disastrous consequences: the two implementations made by Alcatel (for the Dutch part of the railway) and Alstom (for the Belgian part of the railway) turned out to be incompatible.

To solve this serious problem, a 'dedicated' solution has been defined. It consists of a dedicated version of ERTMS (referred to as 'Version 2.3.0 Corridor', that replaces an earlier version) and a link between the two systems of different suppliers by a so-called gateway. This gateway is a system, that arranges the communication between the two ERTMS implementations and their Radio Block Centres on either side of the Dutch-Belgian border [10]. The gateway on HSL-Zuid/HSL 4 has yet to be debugged.

2.1. Choice of the system border

A second reason - next to the choice for PPP – why this international HSL-Zuid/HSL 4 project has been divided into two parts, was the choice for the national border as project demarcation instead of the system border. The latter is a point where the high-speed tracks connect with the existing tracks of the conventional railway system. If the system border would have been chosen instead, it would have been much easier to connect the signalling systems. This is the case, since it is no longer a problem connecting ERTMS on a high-speed section with a signalling system on a conventional line.

In every technological project at least implicitly the question arises whether to use existing technology or to develop new technology. Then the question arises which technical solution is most promising given the project aims and the demands from its environment.

The Netherlands used to have one single railway signalling system for decades. It is called *Automatische Treinbeïnvloeding* or ATB and it operates appropriately within the speed bracket of 40-140 km/h. Apart from a few minor changes, ATB is still available everywhere on the conventional rail network in The Netherlands, thus leaving the country unprepared for operating trains with high speed. In Belgium, however, the situation was quite different. The country was prepared for high speed operations, because it not only built the Belgian part of the high speed railway Brussels-Paris for speeds up to 300 km/h, but it also increased maximum speed of national intercity trains towards 200 km/h. Belgium invested in new technology, by developing a high-speed signalling system called *Transmission Balise-Locomotive / Transmissie Baken-Locomotief* (TBL) (which is functionally comparable with TVM) and it renewed most of its rolling stock. As a conclusion, this can be seen as a process of incremental system change, in which compatibility is well being taken care of.

The process of constructing the HSL-Zuid in the Netherlands may be considered as rather revolutionary, not only because of the need to close the technological gap with Belgium, but also because of its experimental institutional setting. PPP was not compulsory because of the demands of the project, but it was motivated by the political move towards liberalisation.

In The Netherlands ERTMS has been chosen at a moment in time when only a functional specification of ERTMS existed. ERTMS was not in operation anywhere in the world. The choice as such could be defended from the perspective of European standardisation, but from a business perspective it has been a high-risk (financial) choice. On other (international) high-speed railways the choice was made to install a proven signalling system. TVM, for instance, has been installed on Paris-Brussels and more recently on the Channel Tunnel Rail Link to London and on the French part of the POS-corridor (on the latter: dual standard TVM430 and ERTMS Level 2).

2.2. Fall-back options

Since ERTMS was not a mature product, the discussion about the necessity and benefits of fall-back options continued. From 2003 these discussions took place with the future operator HSA/NS. The minister of Transport, Water Management and Public Works rejected this idea by referring to the additionally by Siemens installed ERTMS Level 1 as fall-back option and because it did not seem

likely in November 2005 to install and certify one of three fall-back options as considered by HSL-Zuid and ProRail (TBL2, ATB-NG and ERTMS Level 1 Overlay) before the initially proposed opening date of April 1, 2007 [11].

3. CONSEQUENCES OF ERTMS

The conclusion may be that a choice for the French dual standard approach, using TVM430, would have been interesting, because this would have allowed high-speed trains to operate from Amsterdam to Brussels, Paris and beyond, as far as the Mediterranean and also from Amsterdam to London (via Lille). It would also have made it unnecessary to upgrade the existing Thalys trains. At a later moment, a (mature) ERTMS Level 2 could have been added. Instead of the now installed ERTMS Level 1 as a fall-back option on HSL-Zuid/HSL 4 (which still introduces a second signalling system next to ERTMS Level 2), TVM as a fall-back option next to ERTMS Level 2 would have been a good alternative, because, unlike ERTMS 1, TVM allows to operate trains with speeds up to 300 km/h, instead of 160 km/h as is the case now. Systems like ERTMS Level 1 are beacon based. Since present Dutch railway regulation requires continuous train detection, this demands an increase of the number of beacons in order to run at 300 km/h, at least in The Netherlands. TVM, however, does not show this problem, because it uses electrical track circuits and therefore offers continuous train detection.

3.1. Joint development of HSL-Zuid/HSL 4 instead of development as two projects

One of the options in this case would have been a joint development by The Netherlands and Belgium of the HSL-Zuid/HSL 4 project, instead of the present situation in which both countries developed their parts of the railway as separate projects. A joint tender could have reduced the costs because of economies of scale.

An good example is the joint Austrian-Italian project for the Brenner Base Tunnel (BBT), a 55 km long railway tunnel beneath the Brenner Pass, for which a so-called European Economic Interest Group was established [12].

3.2. The choice of a proven signalling system: e.g. TVM430 instead of ERTMS

Next to this comes the Dutch orientation on German railway (signalling) technology, while Belgium is traditionally oriented on French technology. Because HSL-Zuid/HSL 4 connects with France and the Thalys trains are also of French origin, it would have made sense to choose for the French TVM system. This would have been at least a sensible medium term solution. As soon as ERTMS would have become fully available, it could have replaced TVM as primary signalling system. What happened instead is that the risk of product development became concentrated in the HSL-Zuid/HSL 4 project.

3.3. The choice of traditional contracts instead of PPP

The institutional setting of this project in The Netherlands was completely different than the institutional setting in Belgium. The separation between the infrastructure and the transport contracts as has been chosen in The Netherlands did not really make sense, because it became much more difficult to implement a reliable signalling system. By putting the project mainly in the hands of private partners, The Netherlands have created an unnecessary contractual complexity, which in turn made co-operation with Belgium much more difficult. One of the results of this situation is that there are now two different interpretations of ERTMS (Alcatel and Alstom). Both interpretations will now be connected in a rather synthetic way by the so-called gateway.

3.4. The choice of system boundaries instead national boundaries as project boundary

The choice of the national boundary as system boundary is one of the main reasons why the whole project has been delayed for several years. If the project would have been developed as one international cross-border project, most, if not all technical problems could have been prevented. The

Netherlands could have made arrangements for planning the HSL-Zuid/HSL 4 as one project in the treaty with Belgium since The Netherlands paid a substantial part of the HSL 4.

4. DECISION MAKING ASSESSMENT

4.1. Decisions in retrospect

In retrospect, a number of options and their consequences for the decision making could have been addressed more prominently:

- a straight forward choice for a new signalling safety technology which was not yet operational at that time, while qualified systems were readily available on the market. This implies a choice for continuing the ERTMS development, in contrast with existing systems such as TVM 430.
- a choice for innovation instead of an incremental development; the development of signalling safety systems for high-speed lines has been much more an incremental process in Belgium. Belgium demonstrates an evolutionary development in TBL2, while the Netherlands makes a systems leap from the traditional ATB towards ERTMS
- the choice between coupling the Dutch system and the Belgium system at the country border or at a technically more simple point, i.e. the closest coupling point with the conventional network, such as North of Antwerp. This choice could have been settled in the Treaty between the Netherlands and Belgium, because the Netherlands has paid a substantial part of the Belgian HSL 4
- a contractual based deployment of ERTMS version 2.2.2 while 2.3.0 would become the new standard
- acknowledging the necessity for systems integration during the delivery of the integral system in practice.

4.2. Decisions in prospect

During the investigation, a number of knowledge deficiencies are noticed which have not been addressed sufficiently:

- structuring contracts with private partners to such an extend that the risks and costs are allocated to those parties which are most equipped with respect to the nature and content of the consequences. Contracts in which a technological development plays an important role, should be equipped with an adequate substantive check
- the migration and deployment of ERTMS towards increasingly higher levels (from ERTMS level 1 towards level 2 and from ERTMS level 2 towards level 3) shows that the costs and risks of railway signaling safety shifts from the infra provider towards railway operators. The reasons for this shift remains unclear and is even less clear whether this is a necessary development or not
- the process of software development will not stop with the delivery of the HSL track. An analogy with aviation clarifies the necessity of a frequent upgrade, whereas it remains unclear how this upgrade will be settled during regular operations beyond the level of a procedural approach.

Answering the questions of Parliament in terms of reasonability and fairness of the selected developments implies an as good as substantiated snapshot, in which uncertainties in decision making and technological development should be compensated by a flexible form of cooperation.

5. CONCLUSIONS

During this investigation, the focus has been on learning, providing wisdom by hindsight. Based on the insights by hindsight, recommendations are to be made which may stimulate the future success of major projects. Allocating blame has been irrelevant in this investigation.

The main conclusions of this investigation into the upgrade of ERTMS software are:

- The institutional environment has complicated the development and implementation of the project. The divisions that have been introduced, have created a necessity of a complex interface management
- The two main lines in contracting out the project have only indicated the necessity to create oversight by the end of the project. This division has not led a role for an architect or systems integrator, responsible for the integral coherence during implementation of the overall system
- The technological development of ERTMS is underestimated. There has been a tension between incremental progress on one hand and implementation in an existing railway network on the other hand with the ambitions on innovative ERTMS and public-private partnership.
- Safety critical issues of a non-physical nature may emerge during the design and construct phase, leading to recommendations for improvements during operational control and changes in the project management before disaster occurs.

References

- [1] Stoop, J.A. (2003). Critical size events: a new tool for crisis management resource allocation?. *Safety Science* 41 (2003) 465-480.
- [2] Stoop, J.A., Baggen, J.H., Vleugel, J.M., Kroes, J.L. de, and Vrancken, J.L.M. (2007). *HSL-beveiligingssysteem ERTMS. Een onafhankelijk onderzoek naar nut en noodzaak van de aanpassing van het HSL-beveiligingssysteem ERTMS*. Research project commissioned by the Onderzoeks- en Verificatiebureau van de Tweede Kamer der Staten-Generaal, The Hague.
- [3] EU (2005), *Trans-European Transport Network, TEN-T priority axes and projects 2005*, DG TREN, Brussels.
- [4] Viaene, D. (2005). *De seininrichting bij de NMBS*, NMBS, Brussels.
- [5] SBB (2007). *ETCS in Europe*, http://mct.sbb.ch/mct/infrastruktur/infrastruktur_innovationen/projekte-etc/etcs-europa.htm.
- [6] Profillidis, V.A. (2006). *Railway management and engineering*. 3rd edition, Ashgate, Aldershot, England.
- [7] Tweede Kamer (2005). *Nederlands deel van een hogesnelheidsspoorverbinding Amsterdam-Brussel-Parijs en Utrecht-Arnhem-Duitse grens*, vergaderjaar 2005-2006, 22026, nr. 239, SDU, The Hague.
- [8] HSL-Zuid (2007b). *High-speed alliance*, http://www.hslzuid.nl/hsl/organisatie/High_Speed_Alliance/index.jsp.
- [9] Tweede Kamer (2007b). *Risicobeheersing HSL-Zuid, Rapport van de Algemene Rekenkamer*, Tweede Kamer, vergaderjaar 2006-2007, 31072, nrs.1-2.
- [10] Tijdelijke Commissie voor de Infrastructuur (TCI). *Onderzoek naar infrastructuurprojecten (2004). Reconstructie HSL-Zuid: de besluitvorming uitvergroot*, Tweede Kamer, vergaderjaar 2004-2005, 29283, nr. 8, SDU, The Hague.
- [11] Vleugel, J., 2006, *Natural cross-border barriers to the development of Trans-European Transport Networks*. Report for EU Committee of the Regions in cooperation with Trip, J.-J. and Stead, D., Delft.
- [12] LREHC Infraproject Services (2005). *Definitieve rapportage second opinion beveiligingssysteem in HSL-Zuid infrastructuur*. Appendix of Tweede Kamer, 2005.