Securing safety

Resilience time as a hidden critical factor

Beukenkamp, Wim

DOI
10.4233/uuid:3dec02ac-c659-4741-980f-85619f2c4da6

Publication date
2016

Document Version
Final published version

Citation (APA)
Beukenkamp, W. (2016). *Securing safety: Resilience time as a hidden critical factor*. [Dissertation (TU Delft), Delft University of Technology]. TRAIL Research School. https://doi.org/10.4233/uuid:3dec02ac-c659-4741-980f-85619f2c4da6

SECURING SAFETY

Resilience time as a hidden critical factor

Willem R. Beukenkamp

Cover illustration by W.R. Beukenkamp
September 24, 2009 two freight trains and a passenger train collided at Barendrecht, south of Rotterdam. Time was an important safety critical factor in this fatal accident. Note that the loco 6514 was named ‘Wim’, same as the author of this thesis.

SECURING SAFETY

Resilience time as a hidden critical factor

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof.ir. K.C.A.M. Luyben;
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op
maandag 3 oktober 2016 om 10:00 uur

door

Willem R. BEUKENKAMP,
Technisch-bestuurskundig ingenieur
geboren te Rotterdam, Nederland

Dit proefschrift is goedgekeurd door de promotoren:
Prof. dr. ir. J. A. Stoop
Prof. dr. ir. S.P. Hoogendoorn

Samenstelling promotiecommissie:

Rector magnificus	Voorzitter
Prof. dr.ir. J.A. Stoop	Lund University, promotor
Prof.d r.ir. S.P. Hoogendoorn	Technische Universiteit Delft, promotor

Onafhankelijke leden:

Prof. dr. ir. R. Benedictus	Technische Universiteit Delft
Prof. dr. ir. R.P.B.J. Dollevoet	Technische Universiteit Delft
Prof. dr. ir. M.J.C.M. Hertogh	Technische Universiteit Delft
Prof. dr. C. Johnson	University of Glasgow
Dr. P.C.J. Neuteboom	Inspectie Leefomgeving en Transport

TRAIL Thesis Series no. T2016/18, the Netherlands Research School TRAIL

TRAIL
P.O. Box 5017
2600 GA Delft
The Netherlands
E-mail: info@rsTRAIL.nl

ISBN: 978-90-5584-210-0

Printed in the Netherlands

Preface

As always when you start a PhD study you have no idea what it is going to be and what will result from it. What is clear is what caught your attention, what it is that you want to research in detail. It requires tenacity to continue the research and bring it to a successful ending. There are inevitable moments that you are seriously questioning yourself if it is worthwhile to continue. Those are the moments that the support of others is very important.
It is almost cynical when doing research about how to deal with calamities and catastrophes that a year ago I myself was confronted with a life threatening physical problem. I experienced some of the aspects as written down in this thesis, not as an onlooker but as a core actor, a casualty. I observed the actions of professionals when the specialists in my local hospital were working out what was wrong with me and could not find the cause of my physical problems until it was almost too late.
I nearly lost my life because of a diagnostic process that got derailed through communication problems between expert professionals. I thank my life to the knowledge and skills of the emergency surgical team at the Amsterdam Medical Centre where I arrived late in the evening just in time. Having survived that critical situation I became more than ever motivated to complete this research and publish the results as shown in this thesis.
I would like to express my gratitude to my wife Josina van der Horst for supporting me during this long research. The successful ending of it could not have been possible without the guidance of prof. dr. ir. John Stoop of Delft University of Technology, my scientific mentor for many years now. We had many discussions usually starting with both of us having a certain view and disagreeing on each other's opinion, ending up agreeing on a third view, having discovered new insights.
Also I would like to thank prof. dr. ir. Serge Hoogendoorn of Delft University of Technology who guided me through the final stages of this research, prof. dr. ir. Rinze Benedictus, prof. dr. ir. Rolf Dollevoet, prof. dr.ir. Marcel Hertogh, prof. dr. Chris Johnson and dr. Peter Neuteboom for examining this thesis and making valuable recommendations to further improve it.
Furthermore I would like to thank the Dutch Environment and Transport Inspectorate (ILT) and ir. Marnix van der Heijde, manager of the rail enforcement section in particular. He recognised the importance of this study for the work of the inspectorate and allocated sufficient resources for me to finish it.
My final acknowledgement is to the thousands of victims of transport and other accidents Worldwide over the years. Although each fatal accident is one too many, often their lives were not lost in vain. We have learned from fatal accidents and we are still learning from them, although unfortunately in some cases over time lessons are lost or worse: ignored.

Haarlem, September 2016.

Content

1. Security and safety, what fails?

1.1 Introduction

This chapter introduces the problems when dealing with matters of safety, security and risks. The Netherlands is quite advanced in is having risk related policies which are laid down in several acts. Nevertheless the policies aimed at containing risks are not always clear. Their chief focus is on safety, the unintentional risks. Security, intentional risks, are relative new, although our society is learning fast from terrorist events at home and abroad.
Sometimes the risk mitigating policies are dominated by inevitable policy-decision making dilemmas where the costs of safety and security have to be balanced against other priorities. These dilemmas create uncertainty resulting in instability of the system. The challenge is to develop an approach which is at systems level both efficient and effective in dealing with large effects of low probability risks relating to transport systems. There is a continuous tension between theory, practice and engineering. This might require a focal expansion from an explanatory approach to addressing change itself.

1.2 Safety, security and risks

Our society is increasingly becoming more complex and thereby more vulnerable without most people being aware of this. At the same time safety standards in our society are such that the life expectancy of an average inhabitant is longer than ever before. People tend to die from wealth-induced diseases such as heart diseases instead of major accidents. The overall image is that of a low risk society, where safety is no longer a matter of serious discussion at strategic level, that is until a serious problem arises[1].
The present standard of living is the result of over 200 years of (technological) innovation. This innovation drive has made us aware that risks exist and if not controlled, sometimes culminate in horrific accidents, such as the 1953 Flood disaster ('Watersnoodramp[2]') in the Netherlands, or more recently hurricane Katrina in New Orleans, 2005. Not only nature has taken its toll, technological development has claimed many victims as well. Many countries have a history of serious railway accidents, most of which have contributed to the present day railways being one of the safest transportation systems[3] that we have. Still, these modern sophisticated railways are not free from accidents, even major ones happening occasionally[4]. It is through investigating these accidents that we have learned (and continue to learn) how to reduce risks to acceptable levels by either preventing accidents or mitigating the effects.

Another lesson learned is that risks can be reduced but never eliminated. A characteristic of some major disasters is, that they occurred as a result of one or more very unlikely scenarios, i.e. the low probability large effect scenarios. The classic one is the Titanic disaster, but there are many more where history shows that given time and a large amount of occurrences, sooner or later the disaster jackpot will pay[5].
We have also learned that inherent but as yet unknown properties of materials and structures only show themselves after thorough research and extensive testing. Classic cases like the Tay Bridge disaster[6] and the Comet jet plane[7] crashes have been costly; yet they have given us valuable insight into until then unknown engineering design phenomena (flutter, fatigue). All these developments can be classified under the term 'safety', meaning the safeguarding against unintentional failure of structures and systems[8].
Recent events such as the 9-11 attacks in the USA (2001), the Madrid (March 2004) and London (July 2005) public transport bombings have shown that security[19] is increasingly becoming a national issue in many countries. Standard risk management methodologies based on probabilistic risk models fail when dealing with security issues. There are several reasons for this problem, the most important being that security problems are not statistically independent. Indeed, at the uppermost rung of the security ladder, terrorism looks for weak spots in the targeted system. It is as if a fire is deliberately creeping towards the most explosive part. Furthermore, security related problems have a very low frequency, making any model based on statistics inherently unreliable. These issues when related to safety critical systems such as transportation systems, require another risk management methodology then commonly used for safety related problems.
At present there is an inherent discrepancy between risk management at object level and at systems level as Stoop has shown[10]. Safety is more often than not dealt with at object level. At systems level, safety and security are seldom-dominant issues until much later in the process, when the design of new infrastructures is hampered by safety and security related problems[11]. This apparent vulnerability of risk management at strategic and tactical level indicates a necessity for a different approach. This necessity is supported by the way terrorism operates nowadays. Events like 9-11, Madrid and London show that international terrorism has started to operate at systems level as well. Although Stoop gives some answers to repair this discrepancy, his model like other similar models is still somewhat static. The notion of time dynamics as a key factor in determining the properties of risk sensitive systems is not fully explained by these models.
This thesis will show that a scenario-based risk analysis in combination with process management is capable of determining a more robust, effective and efficient safety and security policy when dealing with risk management of safety critical systems at systems level. Furthermore, this thesis will indicate that when dealing with low frequency-large effect risk related problems (such as terrorism), a shift from damage control (reactive risk management) to controlled damage (pro-active risk management) could result in better protection with less effort. This requires a redesign of scenario-analysis as a strategic and tactical management tool to control apparent system uncertainties. This way of thinking culminates in the so-called Citadel Principle[12], concentrating limited resources where it really matters and accepting a certain level of damage anywhere else. Furthermore the notion of resilience time is introduced as a function of system criticality.

1.3 Risk policies in the Netherlands

Risk related policies in the Netherlands have developed through a series of stages. The most important aspect is the development of societal risk related policies. The first recorded major accident in the Netherlands as a result from the use of hazardous materials was the Delft gunpowder store explosion (1654). A similar explosion in Leiden (1807) resulted in a decree by King Louis Napoleon, putting limitations to the operation of establishments dealing with hazardous materials such as explosives. In 1814 this imperial decree was converted into a Royal Ordinance, aimed at preventing danger, nuisance and damage to third parties.
In 1875, this Royal Ordinance was converted into a new act: the Factory Act (Fabriekswet). In 1896, the so-called Nuisance Act (Hinderwet) was introduced, setting specific rules and requirements for establishments and industries, which could cause a nuisance to the environment. The Nuisance Act was one of the first true environment acts in the Netherlands and lasted for a long time. In 1963 this act was supplemented by a specific act aimed at limiting the risks of hazardous materials (Wet gevaarlijke stoffen).
A fundamental change in policy came in 1989, when the Dutch government[13] published a policy memorandum 'Omgaan met risico's' (Premises for risk management). Based on individual and societal risk, several risk domains were identified including standards for acceptable levels of risk. This memorandum introduced the principle of risk calculation based on statistical parameters, paving the way for probabilistic based designs, which are still standard in the Netherlands and have been extended to the transportation of hazardous materials as well[14].
The memorandum was the first to distinguish between individual risk and group risk (societal risk). Since then it is the latter that has played a major part in risk control policies in the Netherlands. Special tools were developed to calculate the risk of various activities. The risk models were based on publications of the national committee for de prevention of disasters ('Commissie Preventie Rampen' CPR). These publications, usually known by their colour (such as 'Purple Book', 'Yellow Book' et cetera) not only described failure scenarios of almost every conceivable industrial equipment, but also its probability, the effect range and the likelihood of casualties (probit function[15]).
Infrastructures showed a similar development. Over many centuries the Netherlands has been struggling to defend itself against water and to reclaim land from the sea. The basic approach was a reactive, deterministic one: when dikes failed, they were enlarged, until they failed again, after which the same process repeated itself. Occasional flooding was more or less seen as inevitable. The first change came with the 1916 flooding around the then Zuiderzee[16], when massive parts of the country including the area north of Amsterdam, were flooded. This catastrophe resulted in de Zuiderzeewerken to prevent a repetition of such disasters.
The approach was still deterministic, but this time some form of risk analysis was done, when studies were carried out towards the various possibilities to diminish this specific risk and the impact these solutions would have on the economy and the environment in the affected areas. Transforming the Zuiderzee into the IJsselmeer implied changing a saline ecosystem into a fresh water system. Traditional coastal fishing would disappear as a trade as it did (and was later succeeded by another type of fishing).
The earlier mentioned 'Watersnoodramp' of 1953 in the South West of the Netherlands resulted in a national act to improve the coastal defences ('Delta Wet'). This act introduced a probabilistic element into national law, by determining the acceptable level of flood risk for various part of the Netherlands. The basis for this was a cost-benefit analysis, based on economic values including the value of (statistical) life.

The outcome was a probabilistic parameter, known as 'Delta Height' (Deltahoogte), being the required height of coastal defences, such as dunes and dikes, in relation to an expected storm surge with probability of occurrence every X years, X being the local parameter, e.g. once every 10,000 years for the west of the Netherlands (the economical centre), once every 4,000 years for Zeeland and so on. In 2005, the Delta Act was incorporated into a new act on water defences (Wet op de waterkeringen), which took river defences into its scope as well. This was a direct result of the 1993 and 1995 river floods, which required massive evacuations[17].
The probabilistic design school became gradually accepted in the Netherlands, culminating in the Maeslant storm surge barrier. The design of this barrier (the largest movable barrier in the world) was a probabilistic one, where the outcome of sensitivity analyses was set to match the required failure rate, being better than once every 1000 times. One of the design specifications was the total elimination of the human operator on grounds of unpredictability and therefore unreliability. Very soon after it was commissioned this barrier proved not to be as reliable as predicted and designed. This case will be dealt with in more detail in this thesis. The outcome of the Maeslant Barrier case was a return to more defensive design principles, including bringing back the human operator into the system.
However, in general, the national political attitude towards risk management was still a probabilistic one. This was not difficult to defend for risks with a known history and thereby statistical reliability, such as emanating from chemical industries. Applying it to transport safety proved to become more disputable. The so-called 'COEV' studies[18] showed that at best, crucial railway stations were going to remain external safety bottlenecks, not only now but in future as well. In 2005, the Ministry of Transport & Water management published the policy document on mobility (Nota Mobiliteit). This policy document still accepted probabilistic parameters such as Individual Risk and Societal Risk, but introduced a new approach as well[19], based on scenarios and contingency planning, amongst others stipulating the importance of the ability of self-rescue for the people affected.
All this was fine when dealing with risks resulting from true accidents. However, since the beginning of the 1980's the Dutch have played an increasing international military (peace keeping) role, resulting in operations in Lebanon, Sinai, Cambodia, the Balkans, Eritrea, Iraq and Afghanistan. This enhanced the risk of terrorist actions against the Netherlands. A national security evaluation of vital infrastructures took place as a result from the 9-11 attacks. This process was speeded up after the attacks in Madrid (2004) and London (2005), when it became clear that Europe was increasingly being targeted by international terrorism. The Dutch department of transport, public works and water management (Rijkswaterstaat) was very quick to react, using guidelines set by Beukenkamp et al as a standard policy[20]. These guidelines abandoned the idea of a probabilistic approach, stipulating a contingency and functionalistic policy instead.
The national evaluation by the Ministry of the Interior[21] at the time followed a similar approach, stipulating that from a probabilistic point of view in the Netherlands there is hardly any case to answer for regarding terrorism. The protection of vital infrastructures should be put in a wider context than resulting from the threat of terrorism alone according to this study. At the same time the threat is such (certainly after Madrid, 2004 and London, 2005) that doing nothing would have been unacceptable to the public in general and parliament in particular[22].
A simple incident regarding a brick thrown from an overpass, killing a motorist near The Hague in January 2005, illustrates this shift in attitude all too clearly[23]. Indeed, this case (as in some other cases) showed that one of the management problems regarding safety and security issues is the value of statistical life[24] (VSL). This problem will be addressed in this thesis.

Furthermore, the 2005 study addressed the problem that dominates security issues in general, i.e. risks which are difficult to calculate, compared to risks emanating from technical or organisational failures[25].

1.4 Lessons learned and challenges for the future

1.4.1 Control variables

History shows a couple of important lessons to be learned. Safety and security are often not very high on the political agenda, until something serious happens. The problem is that the costs of safety and security are usually clearly visible, yet at the same time it is very difficult to show the benefits of such a policy. What is needed is a clear insight at systems level into the criteria needed to prioritise between the various policy options.
Looking at the past, control variables can be identified which could play an important role in these decision-making processes. What are these control variables? They are not found in the communication to outside stakeholders like the public using the media, because this will result in perception management without tackling the real problems of the system.
They are neither found in the probability of an attack, because a probabilistic approach means that the risk of a terrorist attack is ignored given its very low occurrence. The real control variables can be found in the properties of the system itself, because controlling vulnerabilities results in a crisis tolerant strategy. This thesis will show these variables and why they are essential in controlling the safety in decision-making processes regarding infrastructures.

1.4.2 First lesson: the George dilemma

The **first lesson** is that societies only tend to learn by means of shocks[26]. Because criminality is not visible and the resulting damage is spread out over a large part of industry and society, the effect on society as a whole is underestimated both by the politicians and by the population. As long as there is no publicity around it, it is taken as part of every day's life by those not directly involved.
In contrast a major accident or act of terrorism has a shock effect, which stirs up things tremendously, even though it's real impact is many times smaller than the impact of other problems such as casualties resulting from traffic accidents[27]. There is at any time tension between safety and security responsibilities on the one hand and the economic possibilities on the other, like the choice between ad hoc (political) reaction and long term, but more cost effective measures. George described this tension in his exchange dilemma for the policy decision-making process of US presidents[28], see §2.3 and §3.5.3.

1.4.3 Second lesson: media and design and control of systems

The **second lesson** to be learned is that it is necessary to incorporate the media in the design and control of emergency sensitive systems. The media can play a positive role before a crisis occurs, because they can bring problems to the political arena, thereby contributing to making public systems such as major infrastructures more stable and safe.
During and after a crisis however, the media can play a far less positive role by increasing the pressure on government and forcing it to take immediate action to satisfy the public opinion. The involvement of the media at this stage might in fact decrease stability. The outcome can be an escalation of the problem instead of de-escalation. If the media are seen as partners in a difficult process, every day's practice indicates they will play their role as best as they can, given their public/economical responsibilities. Recent developments around Al-Qaida propaganda are a good indication of this. Perhaps this does not apply to all media, but certainly to the quality media amongst them[29].

1.4.4 Third lesson: methodical approach

The **third lesson** to be learned is, that methodical research is needed to assist in policy making when dealing with safety and security matters. Too often security and safety is seen as something to be solved by experts at object level and therefore not being a prime responsibility of the management at systems level. Too often experts appear late in the decision making process, when important decisions with safety and security implications have already been made and are difficult to reverse.
A more methodical approach to safety and security related matters could prevent extreme reactions as mentioned earlier, thereby saving money, men and means. These savings can be used to further improve safety and security where it really matters, thus creating a positive feedback. A pure technical engineering approach appears to be insufficient though.
If the organisation of the system immediately after an incident turns into chaos, every precaution is bound to fail. Therefore three pillars are needed to safeguard security of (transport) systems:

1. Organisation
2. Information
3. Technical measures

This approach is known as the 'The Hague Method'. It is generally used in the Netherlands when dealing with security matters like criminality, vandalism et cetera.

1.4.5 Symptom management

In addition to the above-mentioned pillars, four fundamental questions regarding the design of the system should be asked to ascertain its vital components:

1. Why is this (part of the) system vital?
2. What can be done to protect the system, or to diminish its vital position?
3. How can the system be protected or made less vital?
4. With what can the system be protected or made less vital?

Too often, attacking the items 2, 3 and 4 (preferably in reversed order) solves problems or so it seems, leading to symptom management (short term decision-making). This policy is more or less dictated by the George dilemma as described in §2.3. But if there is no reasonable answer to question 1, the outcome runs every risk of being sub optimal if not utter nonsense, certainly in the longer term. Science and research can do much to counter this problem and make sure that the fundamental questions at systems level are asked and answered first, before solutions are agreed upon[30].

1.5 Need for a different approach

The earlier mentioned problems and historical lessons clearly indicate a need for a different approach. Instead of the classic object oriented engineering approach, an approach at systems level is required. Not so much the way systems and their components are constructed matters, but the way they function and influence other systems or are influenced by them is crucial. A view at systems level brings forward a need to define the boundaries of each system. Otherwise, the view will be cluttered by undefined boundaries, resulting in lack of clarity when decisions are to be made.
Future holds many uncertainties, but one thing is certain: technical evolution will continue, making society as a whole increasingly complex[31]. This puts an increasing strain on safeguarding safety and security related activities such as transportation systems. Furthermore, environmental issues such as global warming are increasingly dominating the political agenda, competing heavily with safety and security for scarce resources.

In the Netherlands, this dilemma is known as the SEE-framework (VEM-raamwerk), whereby safety, environment and economy have to compete against each other in policy decision-making processes, see §4.3.4. One of the dominant parameters in the approach to safety at policy level are the costs and benefits of safety offset against other costs and benefits such as environment or company profit.

1.6 Scope, research questions and approaches

The Dutch society and the Ministry of Infrastructure, Transport and the Environment (IenM) in particular are increasingly confronted with the risks resulting from transportation systems. Both the land use around infrastructures as well as the transport shows a continuous growth. Present risk management policies show increasing signs of inadequacies when dealing with these risks. There is a threat that if not changed, these policies could result in unnecessary limitations on transport on the one hand, or costly and possibly less effective measures on the other.

Serious transport incidents and accidents are scarce, specifically when we look at large-scale incidents such as railway accidents, terrorism and transportation of hazardous goods. On the one and this results in an increasing unreliability of probabilistic based risk management tools. On the other, it creates an atmosphere where safety and security are no longer dominating issues in the decision-making processes regarding major infrastructural projects such as the new High Speed Railway (HSL-South) and the new freight railway to Germany (Betuweroute)[32].

Indeed, it appears as if as if safety is something[33] to be solved by engineers in the design, construction and maintenance phases of a project or system. In part this is caused by the high engineering standards as they prevail in the Netherlands and elsewhere. Dutch engineers for example have been capable of finding answers for most if not all the problems they encountered regarding infrastructures such as coastal defences, building tunnels through soft soil et cetera. They have learned from disasters in the past. The Dutch coastal defences are world famous and serve as examples for other parts of the world, New Orleans after the 2005 Katrina disaster being a marked example.

Cases such as the discussion around the installation of sprinkler systems in the tunnels of the Betuweroute freight railway barely two years before it is going to open, show that process management is not adequate in dealing with crucial matters, such as safety. In this case, incorporating a number of additional tunnels in the planned route has circumvented environmental problems. Only at a later stage (when the operational licenses were needed) was it realised that these tunnels required additional safety measures, for which neither provision was made, nor was a matching budget available. Indeed, in many ways this case showed a repetition of the safety process around the HSL-South tunnel under the Green Heart of the Netherlands[34]. The outcome was that this issue delayed the formal operational status of the railway by more than a year.

A similar situation arose in the HSL-South project, because of problems with the ERTMS signalling system. The latter resulted in a formal investigation by TU-Delft[35] at the request of the Lower House of the Dutch parliament. Again, crucial safety issues were either ignored or underestimated when decisions regarding this project were made at strategic and tactical level[36].

There are more indications that at tactical and strategic level the safety and security issues are not properly safeguarded. This can be deducted from (amongst others):

- Report Commissie Sorgdrager 'De prijs van mobiliteit'; 2005
- Report TCI; Tweede Kamer, 2005
- Evaluation of the 'Nota Risiconormering Vervoer Gevaarlijke Stoffen'; AVV, 2004
- Report 'Veiligheid tram en wegkruisingen'; AVV, 2004
- Report 'Veiligheid Spoedwetprojecten'; AVV, 2003
- Report 'Veiligheid, een zorg van bestuurders'; Raad voor Verkeer en Waterstaat, 2000
- Grote projecten: besluitvorming en management; de Bruin et al, 1996

Problem statement:
It appears that present risk management policies fail to safeguard the role of safety and security at strategic and tactical level when dealing with major infrastructures and therefore might result in an increased risk level without policy decision makers and managers being aware of this.
Based upon this problem statement, the following research aim is defined:

Research aim:
To develop an approach, which is at systems level both efficient and effective when dealing with large effect low probability risks relating to transport systems.

To achieve this aim, this research focuses on the following research questions:

Research question 1:
What are accepted risk management techniques related to infrastructures?

Approach: A literature research will be conducted to reveal the present situation regarding the risk management approaches (chapter 2).

Research question 2:
What role do safety and security issues play in the decision-making processes regarding large-scale infrastructural projects?

Approach: Based upon current Dutch policy instruments regarding risk management of major infrastructures, hidden dangers in these policies are shown (chapter 3 and 4).

Research question 3:
If this role is insufficient, what are the causes of this?

Approach: Existing methodologies as used in the Netherlands related to road safety, external safety and social safety and their outcome are studied and analysed (chapter 4).

Research question 4:
What methodologies exist, which can be used to improve this situation?

Approach: Existing policy tools regarding risk management are examined in more detail using five case studies. Based upon these studies which span the field of major infrastructures, the concepts, methods and techniques of risk management are examined (chapter 5).

Research question 5:
If existing methodologies are not adequate in dealing with these issues, which improvements are possible?

Approach: Using knowledge gained from analyzing literature regarding risk management of infrastructures, studying and analyzing some typical cases, the application of risk management techniques in retrospect, a new approach with regard to risk management of safety critical systems is proposed. This approach is specified in more detail in terms of concepts, methods and techniques for risk management and policy decision-making (chapter 6).

To ascertain the practical value of the new methodology as proposed in this study, the sixth research question must be addressed:

Research question 6:
To what extend does the theoretically developed methodology provide answers to questions of managers in infrastructure projects in practice?

Approach: The practical value and relevance of the proposed new methodology is examined by applying it first in retrospect to an existing situation and then in a new situation. The perception thus gained is evaluated, based upon opinions of experts who have shown interest in working with this methodology.

1.7 Scientific contributions of this research

The most important scientific contribution of this research is that it shows how to translate operational and organisational problems to design and engineering principles. In other words: how to move from factor and event to vector and system requirements. It also shows how resilience engineering can be used in practice as an engineering (design) tool, where at present resilience engineering appears to be focussed on organisations. This results in a better physical and organisational design, capable of withstanding unexpected, uncalculated and unpredicted operational conditions.
Many present risk analysing tools appear to lack the capability of dealing with the chaos and unpredictability that surrounds accident events. They offer good answers when dealing with the known knowns or the known unknowns. They struggle however with a situation of unknown unknowns. The outcome whatever it may be tends to be presented as a calculated risk that sometimes happens to turn out badly and yet has to be accepted.
This research will show that perhaps the accident itself may be inevitable, but the outcome of the event is not lost on forehand. It is sometimes possible to escape from the chaos that surrounds an accident with minimal or no lasting damage. It is possible to survive that chaos if such a condition has been thought of during the design stage. The Citadel principle is such a tool that can be of help here.
The examples used in this study are mostly taken from Dutch practice. However, they are not uniquely confined to the Netherlands, they could just as well have happened elsewhere. The methods as proposed in this thesis to deal with unpredictable situations can be applied all over the world to every type of transportation.

1.8 Outline of this thesis

In chapter 2, the risk management literature regarding infrastructures (including transportation systems) is studied. Existing methods and techniques are investigated to determine their possible usage to analyse safety and security aspects of transportation systems.

Chapter 3 takes a look at the real world: empirical lessons from practice. Five characteristic cases are analysed, illustrating the problems regarding the role of safety in decision-making processes. The dilemmas facing the positioning of safety and security in infrastructural processes and the conflicts arising from them are shown.
§3.2 has been published earlier as part of the proceedings of the 30th ESReDA seminar, 2006. Though two authors are mentioned in this paper, with the exception of paragraph 3.2.8 the paper was entirely written by the author. It has been partly rewritten by the author and updated for this thesis.

Chapter 4 offers a third perspective: large projects with much emphasis on safety ex ante, protocols and procedures. Current policy instruments are analysed, which should (in theory) safeguard safety and security issues. The reasons for their shortcomings are shown.
§4.4 was originally written jointly by Beukenkamp and Stoop under the title 'Monitoring safety in design and construct; the HSL-South case study'. It was published as a paper for the ITA World Tunneling Congress, Amsterdam, 2002. It has been adapted by the author and updated for this thesis.

Chapter 5 investigates what might be missing at present: risk management models are somewhat static, ignoring time as a missing dimension. Furthermore it analyses hidden dangers in policies, such as entrapment, groupthink, George dilemmas and the struggle to achieve safety and security at reasonable cost (SEE-framework). Together chapters 1, 2, 3, 4 and 5 represent a detailed survey of the research problem. The research is based on the analysis of actual cases relating to transport accidents.
§5.2.2 has been published earlier as part of the proceedings of the PSAM-8 seminar, New Orleans, 2006. Four authors are mentioned in this paper: Sandra IJsselstein, John Stoop, Maria Kuiken and Wim Beukenkamp. The part represented in this thesis was entirely written by the author, who came up with the idea of accelerations and decelerations in decision-making processes.
§5.2.3 has been published earlier as part of the proceedings of the 36st ESReDA seminar, 2009[37]. It was entirely written by the author.

Chapter 6 not only looks at the way risk sensitive systems are used but also the states and transitions of these systems. It shows another important decision making dilemma, the Collingridge dilemma and its implications for the safety of a risk-sensitive system. Furthermore this chapter takes another look at resilience and resilience engineering.

Chapter 7 shows why resilience and the citadel approach are capable of explaining and enhancing the behaviour of complex dynamic systems both in design and practice. It is possible to avoid surprises such as the George dilemmas and the unknown unknowns.

Notes

[1] Ref. Stoop, 1999: 'Niet anders dan door schokken' (Only by means of shocks). The Enschede fireworks disaster (2000) in the Netherlands exemplifies this postulation, because it resulted in a parliamentary investigation and a much tighter safety policy at government level since then.
[2] During the night of January 31 to February 1, 1953, the west of the Netherlands was hit by a series of storm surges, resulting in massive flooding, costing the lives of 1836 people and creating enormous

economic damage. As a result, the post-war reconstruction process was severely hampered, because scarce resources had to be reallocated to rebuilding and improving coastal defences (Delta-plan).

[3] In 1962 the Harmelen (near Utrecht) train crash in the Netherlands claimed 93 casualties, resulted in the compulsory introduction of Automatic Train Control (ATB) on the entire network. This introduction took nearly half a century and will be described in more detail in this thesis.

[4] An example is the Eschede railway disaster in Germany in 1998, when a high speed train derailed because of tyre failure, claiming the lives of 101 people; furthermore 88 were wounded

[5] Two accidents occurred near Amsterdam Airport Schiphol, first in September 1992 when a El Al Boeing 747 crashed on a housing estate in Amsterdam and more recently in February 2009, when a Turkish Airlines Boeing 737 crashed in a farmland west of Amsterdam. They show that such accidents on or near major airports are inevitable, given time and traffic intensity.

[6] This railway bridge, designed by Sir Thomas Bouch, collapsed as a result from inadequate knowledge of material properties and poor craftsmanship on December 28, 1879, only one month after it was opened. In 1888 it was replaced by a fully redesigned new bridge, which still stands. In 1940, the collapse of the Tacoma Narrows Bridge had a similar effect on suspension bridge design. The Tacoma Narrows Bridge was a mile-long (1600 meter) suspension bridge with a main span of 2800 feet (850 m) (the third-largest in the world when it was first built) that carries Washington State Route 16 across the Tacoma Narrows of Puget Sound from Tacoma to Gig Harbor, Washington, USA. The first version of the bridge, nicknamed 'Galloping Gertie', was designed by Clark Eldridge and altered by Leon Moisseiff. In 1940, it became famous for a dramatic wind-induced structural collapse, an event that was caught on motion picture film. The replacement bridge opened in 1950. More recently Rotterdam (Erasmus Bridge, 1996) and London (Millennium Bridge, 2000) struggled with new unstable bridge designs, both of which required substantial alterations to make them stable.

[7] A structural flaw in design of the De Havilland Comet mark 1 passenger jet plane caused at least two fatal accidents, both in 1954. The first came just after the New Year, on January 10. BOAC Comet G-ALYP left Ciampino airport in Rome on its way to London. The Comet had crashed into the Mediterranean Sea about 16 miles from the island of Elba. Just three months later, another Comet crashed, this time it was South African Airways G-ALYY, which was also flying out of Ciampino and crashed near the Etna, killing all 21 people on board. It was only after a complete fuselage was tested under real time flight cycle conditions, that the apparent design flaws resulting in fatigue failure of the pressure cabin, showed itself. The wreckage that was retrieved from the two crash sites vindicated the outcome of this research.

[8] There are many definitions of safety, which have more or less the same meaning: safety is the condition of being protected against failure, damage, error, accidents, or harm. Protection involves here both causes and exposure (effects) (en.wikipedia.org/wiki/Safety).

[9] Security (en.wikipedia.org/wiki/Security) is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security. The word 'security' in general usage is synonymous with 'safety,' but as a technical term 'security' means that something not only *is secure* but that it *has been secured*. In telecommunications, the term security has the following meanings: A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (Sources: from Federal Standard 1037C and adapted from the Department of Defence Dictionary of Military and Associated Terms). Security has to be compared with and contrasted with other related concepts: safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of active malicious agents attempting to cause destruction. In other words: the key factor in security is dealing with *intentional* harm.

[10] Ref. Stoop, 1990

[11] The ERTMS problem of the Dutch High Speed railway between Amsterdam and Antwerp (HSL-Zuid) is an example of this. A study by Stoop et al at the behest of the Dutch Lower House of Representatives (2007) showed that the safety implications and management aspects of the ERTMS system were underestimated when this system was chosen as the new signalling system for the HSL-Zuid.
[12] Beukenkamp first suggested the Citadel Principle in a study for the Dutch Ministry of Transport in 2001. Since then, it has become the general policy of this Ministry when dealing with security related matters. This principle has been further researched and is one of the subjects of this thesis.
[13] Ref. Tweede Kamer, 1989
[14] Ref. Tweede Kamer, 1989
[15] The idea of probit was published in 1934 by Chester Ittner Bliss (1899-1979) in an article in Science on how to treat data such as the percentage of a pest killed by a pesticide. Bliss proposed transforming the percentage killed into a 'probability unit' (or 'probit') which was linearly related to the modern definition (he defined it arbitrarily as equal to 0 for 0.0001 and 1 for 0.9999). He included a table to aid other researchers to convert their kill percentages to his probit, which they could then plot against the logarithm of the dose and thereby, it was hoped, obtain a more or less straight line. Such a so-called probit model is still important in toxicology, as well as other fields. The approach is justified in particular if response variation can be rationalized as a lognormal distribution of tolerances among subjects on test, where the tolerance of a particular subject is the dose just sufficient for the response of interest. (en.wikipedia.org)
[16] Since 1932, this inland sea has been cut-off from the North Sea by a massive 32 km long barrier, the Afsluitdijk. From then on, the former inland sea became a large fresh water lake, known as the IJsselmeer. Four large polders have been reclaimed in this area, the last one being Zuidelijk Flevoland, 1968.
[17] From January 30, 1995 till February 3, 1995 nearly 250.000 people were evacuated from the central part of the Netherlands between the main Rhine and Meuse rivers. This was necessitated because of extreme water levels in these rivers in combination with river defences (levees), which were long overdue for improvement. This near catastrophe resulted in a special act (Deltawet Rivierengebied), giving the national and local governments special powers to speed up processes for the reconstruction of these river defences and bypass some public consultation procedures.
[18] Ref. AVV, 2004
[19] Ministry of Transport & Water Management, 2005, p. 108: 'To make it possible to transport hazardous substances over the long-term a new pro-active approach is needed. The central government must no longer focus on resolving local bottlenecks (note: such as resulting from societal risk), but must study the entire chain of hazardous substances, from production to usage, together with local government, infrastructure managers and business and industry. Based on this approach, as well as on transport and spatial planning developments, the state wants to define a national basic network for the transportation of hazardous substances. The state will stipulate conditions for the transportation on and spatial planning around this network, so that the transport over the network is as safe as possible'.
[20] Ref. Beukenkamp, 2001
[21] Ref. MinBZK, 2005
[22] Ibidem, p. 7
[23] On Sunday, January 9, 2005 a perpetrator dropped a paving stone from an overpass over the A4 motorway in Rijswijk near The Hague. The stone went through the windscreen of a car travelling on the motorway, killing the driver. The incident made headline news in the Netherlands, becoming known as 'Stoeptegel incident'. Resulting from this incident, a national risk analysis was ordered by the Dutch minister of transport. This risk analysis showed that in probabilistic terms, the risk was such that in most cases only basic actions were justified. Nevertheless under pressure from Parliament the minister of transport ordered a € 30 mln retrofit program to protect overpasses with safety fences.
[24] Also known as the quality-adjusted life year (QALY). This is a measure of disease burden, including both the quality and the quantity of life lived. It is used in assessing the value for money of a

medical intervention. The QALY model requires utility independent, risk neutral, and constant proportional trade-off behaviour.
The QALY is based on the number of years of life that would be added by the intervention. Each year in perfect health is assigned the value of 1.0 down to a value of 0.0 for death. If the extra years would not be lived in full health, for example if the patient would lose a limb, or be blind or be confined to a wheelchair, then the extra life-years are given a value between 0 and 1 to account for this.
[25] MinBZK, 2005 p. 60
[26] Stoop, 1990; Toft et al, 1994
[27] On September 11, 2001, 2752 people were killed. This compares with 40.000 people killed in traffic in the USA in the same year.
[28] George, 1980
[29] Developments in and around the BBC in the Iraq case underline this. In 2004 the BBC was accused of sloppy journalism in its investigation concerning the role of the British government leading to the second Gulf War. This was not accepted from a quality broadcasting station like the BBC.
[30] Ref. Committee for Countering Terrorism, 2003 and Heyman, 2001
[31] Ref. Perrow, 1999
[32] Ref. Stoop et al, 2007
[33] Ref. Veiligheidsbalans 2008, IVW
[34] Ref. Beukenkamp et al, 2002
[35] Ibidem
[36] Ibidem, p.95
[37] Beukenkamp et al, 2006

2. Risk management of transportation systems

2.1 Introduction

Although risk management is relative new as a scientific subject, in itself it is already quite old as will be shown in this chapter. Furthermore risk management is dealing with dilemmas. One of the dominating dilemmas is the George dilemma as explained here. Is the George dilemma a trap from which no escape is possible? This thesis will show in chapter 6 that an escape from such a dilemma is possible.
This chapter aims to answer research question 1: *What are at present accepted risk management techniques related to infrastructures?*
A number of determining publications and the way they handle risk management of complex systems are researched regarding this subject, chiefly those published by Slovic, Stirling, Perrow and Petroski. Furthermore three Dutch theses by Stoop, van Poortvliet and Rosmuller have been studied in detail, because they discuss some fundamental problems when dealing with the subject of risk management of transportation systems in the Netherlands.

2.2 Risk management in a historical perspective

Risk management is a relative new aspect of scientific research regarding risks in relation to transportation systems. Managing transport systems and infrastructures implies management of risk. Risk management, as an explicit management task however is a post-1960s phenomenon, stemming from the insurance industry.
Risk management in the earlier days included insurance buying. Risks that could not be controlled by internal activities or risks stemming from uncertainties in the business and organisation were transferred to external parties and translated into financial liabilities. These insurance brokers calculated the risk by using statistical data and depended the premiums based on these risk calculations. In this form risk management is old.
At first loss of seagoing vessels was deemed inevitable. For example the Dutch East India Company (VOC) in the 1600's and 1700's owned many ships that sailed between Holland (Amsterdam) and the Dutch East Indies, present Indonesia. On average, these ships could manage 3 – 4 return journeys before they were lost at sea, wrecked or otherwise deemed unfit for further service. The profit on these voyages was such that one voyage was enough to recoup the investment on the ship.

Some of them, including the famous Batavia (wrecked of the coast of Western Australia in 1628) and the Amsterdam (wrecked on the beach of Hastings, UK in 1749) never made it at all because they were lost on their maiden voyage. As a result of the high risks involved, these ships were built relatively cheap, with a short lifespan in mind. Human life didn't count at all: the crew only got their wages after they returned safely in their Dutch port of origin. This was a well-established practice, not only in the Netherlands but in most other European countries as well[1].

The next step came with the construction of railways. Again in the beginning safety was primarily a shareholder issue, where the value of safety measures was weighed against the potential loss of profits to the companies, in modern terms: shareholder value. This utter neglect of attention by management of transport systems to the value of human life resulted in the first political interventions in modern transport. Britain led the way with two Acts of Parliament in 1840 and 1842, empowering the Board of Trade to appoint railway-inspecting officers. Their job was to make sure that public safety became a management problem, requiring some form of risk management aimed at reducing the risk to human life.

Technical innovations (air travel, computers), scaling up of the use of infrastructures (roads, air travel) and at the same time a reduction of public acceptance of incidents and accidents have all combined to create the modern subject of risk management, i.e. thinking about risks and their acceptance and weighing of risks against each other. At the same time, the value of human life came into the picture of risk management. The Warsaw convention (1955)[2] in the airline industry was one of the pioneering treaties where internationally the liability of the operator against the loss of human life was formalised, next to the loss or damage of properties. At present, the value of human life is still first and foremost a financial liability (usually transferred to insurance companies), i.e. an economical problem[3].

The Dutch Deltawet (Delta Act) of 1958 legally introduced a probabilistic approach into risk regulation. This was followed in the Netherlands in 1989 by a national policy document called 'Omgaan met risico's' (Coping with risks)[4]. This governmental document put down values for acceptable statistical risks and differentiated between individual risks and societal (group) risks. Since then Dutch society as a whole is characterised as a society where risks are part of every day's life, governed by probabilistic limits of acceptance.

The economical centre of the country in the west has a much lower level of acceptable risk resulting from flooding (once every 10,000 years) than the rural areas in the east (once every 2.500 years in some cases). According to Beck[5] the present society is typified by the term 'risk society', meaning that risk today has a different significance for everyday life from that applying in previous historical eras. Human activity and technology in 'advanced modernity' he claims, produces as a side-effect risks that need specialized expertise to assess and recognize, are collective, global, and irreversible in their impact, and thus potentially catastrophic on a scale never seen before. According to some a collective risk mania exists[6].

As well as a 'risk society' we are also living in a regulatory state[7]. The idea of such a state is the emergence of a new policy style, in which government's role as a regulator advances, while its role as a direct operator declines through privatization and bureaucratic downsizing. Examples of regulatory growth are the development of EU regulations on these matters or the new Dutch railway act (Spoorwegwet 2005) on a national scale.

2.3 Conflict in decision making: the George dilemma

Decision making in transport policies is all about choosing between contradicting options. George has investigated one of the dominating policy decision-making dilemmas at top political level. The lessons learned from his investigation can be applied to transport policies as well, as will be shown in this thesis.

There is at any time tension between safety and security responsibilities on the one hand and the economic possibilities on the other, like the choice between ad hoc (political) reaction and long term, but more cost effective mitigating measures. George[8] (1980) described this tension in his exchange dilemma for the policy decision-making process of US presidents (figure 1):

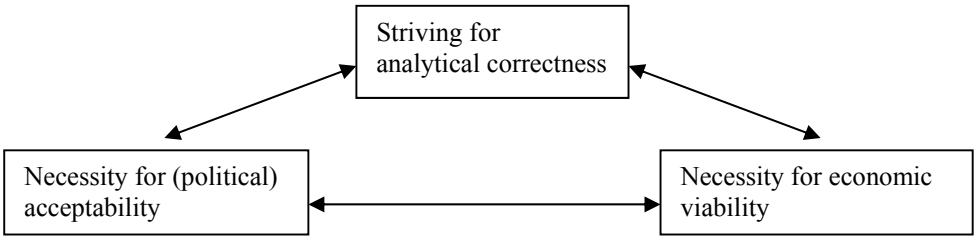

Figure 1. Decision-making dilemmas according to George

This model postulates that in practice the risk of analytical inaccurate decision making (positive failure) is weight against the danger of not getting the necessary political support (need for acceptance) or that the financial/economic consequences do not justify the action. George[9] states 'The important point is that only in the most trivial decisions can policymakers maximize quality and acceptance, while minimizing the expenditure of time and resources.' However, a security problem is not a trivial matter. Therefore there is a need to strive for analytical correctness in these cases.
Sometimes more damage is caused by the government's response in the aftermath of an attack, than by the initial terrorist act itself (the positive feedback mentioned above). The events in the USA following September 11 (the shutting down of the entire civilian airline system in the whole of the USA, causing severe economic damage to the entire industry worldwide) are a clear example of this. Such an apparent overreaction can be traced back to the psychological shock of the act itself plus the experienced political obligation to 'do something about it', to appear decisive.
Only three weeks later, two hoax bomb threats against strategic Dutch motorway tunnels resulted in the largest transport disruption in the history of the Netherlands after the Second World War. It took more than six hours to clear the resulting traffic jams, which spanned every motorway, main and secondary road in the west of our country, the economic heart of the Netherlands. Planes could not depart from Amsterdam Airport Schiphol, because neither passengers nor crews could reach the airport.
Two phone calls, each costing only a few cents, caused economic damage to a total of more than € 30 million. With hindsight, though understandable given the situation prevailing at that time, this is another example of overreaction at systems level. This overreaction resulted from a lack of knowledge into the inherent properties and vulnerabilities of the transport system at that level.

2.4 Theory of risk management: Slovic, Stirling and others

Risk management of transport systems is old, yet as an explicit subject of scientific research it is relatively new. In this thesis a couple of studies have been identified as having specific relevance on the present subject. First and foremost are the publications by Slovic[10] and Stirling[11], because they identified the four schools of risk management and their interactions, implicitly identifying four schools of thought.

'Normal accidents' by Perrow[12] is a scientific classic on this subject, where he shows that accidents are normal in high-risk systems, in the sense that in these tight coupled complex systems unexpected interactions can happen and are not easy to prevent. 'To engineer is human' by Petroski[13] is another important publication.
Petroski shows how important it is that failures sometimes occur. It is only through failures that we can learn about the true properties of systems and its operational boundaries (the operating envelop). Petroski pleas for fail safe designs and safe life criterions. Indeed, Petroski puts the fundamental question on the table of how much safety at what cost?
On a national scale, Stoop[14] looked at risk management of transportation systems from a systems approach. He identifies dynamic interactions between various elements and combines this in a new conceptual model, the DCP diagram (see 2.4.5). Rosmuller[15] studied risk analysis of transport corridors, where risk interactions occur between various individual systems. He focused on the two dominating approaches in risk management: the probabilistic approach and the deterministic approach and applies this to transport corridors. Van Poortvliet[16] researched the question of how high-risk issues are managed within the transport sector and what the relationship is between the structural characteristics of risk management and the occurrence or non-occurrence of disasters.

2.4.1 Slovic

Paul Slovic published several papers on the subject of risk and risk analysis. His earliest paper, titled 'Perception of risk'[17], was fundamental in linking a technological/mathematical approach of risk with a social approach. Since then many authors have been building on his papers. Slovic aims[18] 'to aid risk analysis by providing a basis for understanding and anticipating public responses to hazards and improving communication of risk information among lay-people, technical experts, and decision makers.'
His work[19] 'assumes that those who promote and regulate health and safety need to understand how people think about and respond to risk. Without such understanding, well-intended policies may be ineffective.' Slovic came up with his since then famous classification of risks in four quadrants along two axes: a horizontal axis representing the dreaded risk (effect), and a vertical axis representing the observable risk (probability).
Slovic identifies both quantitative and qualitative risk characteristics. According to Slovic, risk perception is very much dependent on the perceived level of risk. 'Most important is the horizontal factor 'dread risk.' The higher a hazard's score on this factor (the further to the right it appears in the space), the higher its perceived risk, the more people want to see its current risks reduced, and the more they want to see strict regulation employed to achieve the desired reduction in risk.
In contrast, experts' perceptions of risk are not closely related to any of the various risk characteristics or factors derived from these characteristics. Instead, as noted earlier, experts appear to see riskiness as synonymous with expected annual mortality. As a result, conflicts over risk may result from experts and lay people having different definitions of the concept[20].'

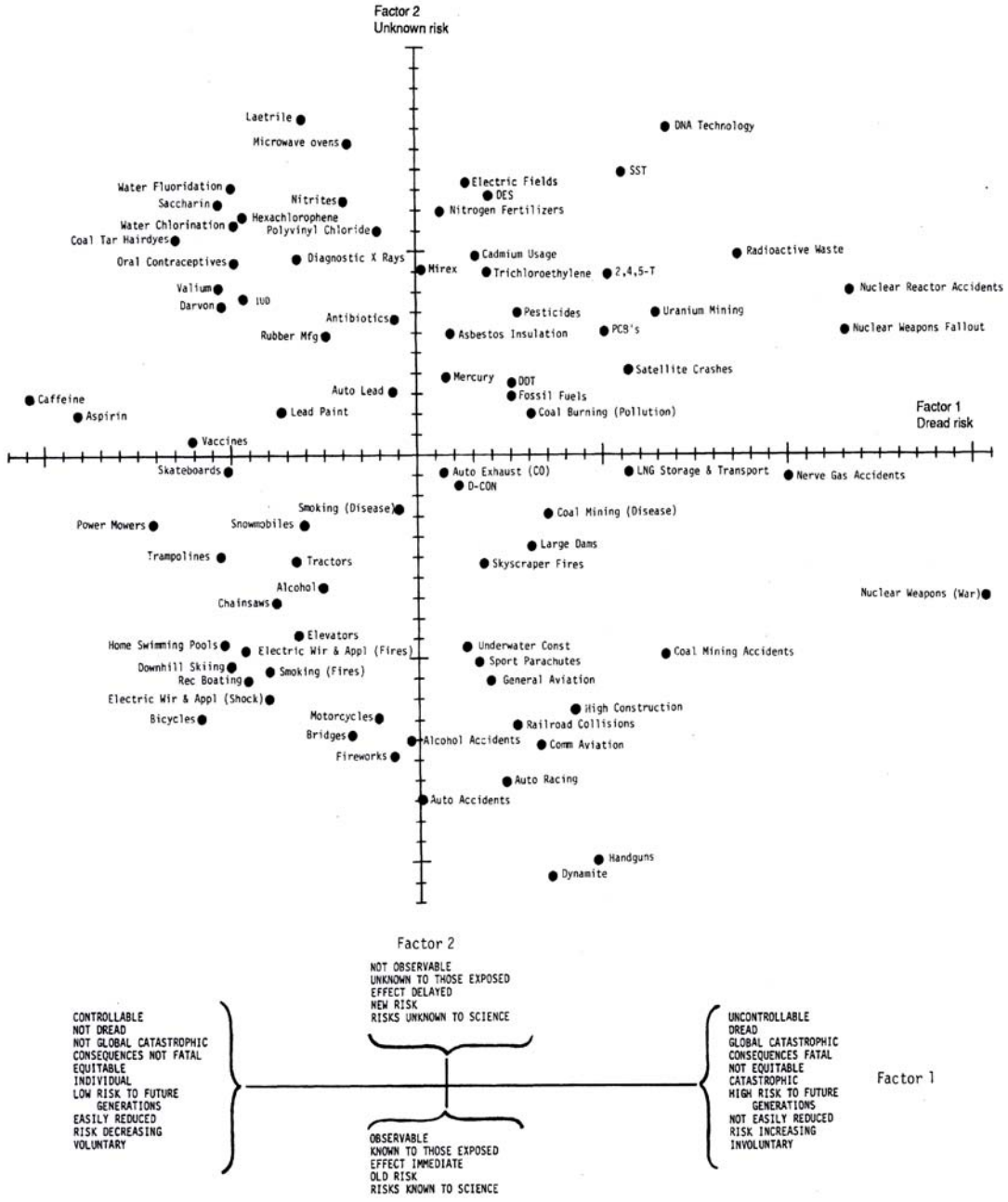

Figure 2 Classification of risks according to Slovic[21]

2.4.2 Stirling

As stated before Stirling took on Slovic' proposals and elaborated on them. In his paper 'Precautionary Approaches to the Appraisal of Risk' (2000) Stirling states[22] 'Within the bounds defined by the domain of plural social discourse, no one set of values or framings can definitely be ruled more rational or well informed than can any other. Even were there to be complete certainty in the quantification of all the various classes and dimensions of risk, it is entirely reasonable that fundamentally different conclusions over environmental risk might be drawn under different - but equally legitimate - perspectives.

It is a matter of the science of risk itself, then, that there can be no analytic fix for the scope, complexity, and intrinsic subjectivity of environmental and health risks. The notion that there can be a single unambiguous 'science based' prescription in the regulatory appraisal of risk is not only naïve and misleading; it is a fundamental contradiction in terms.'

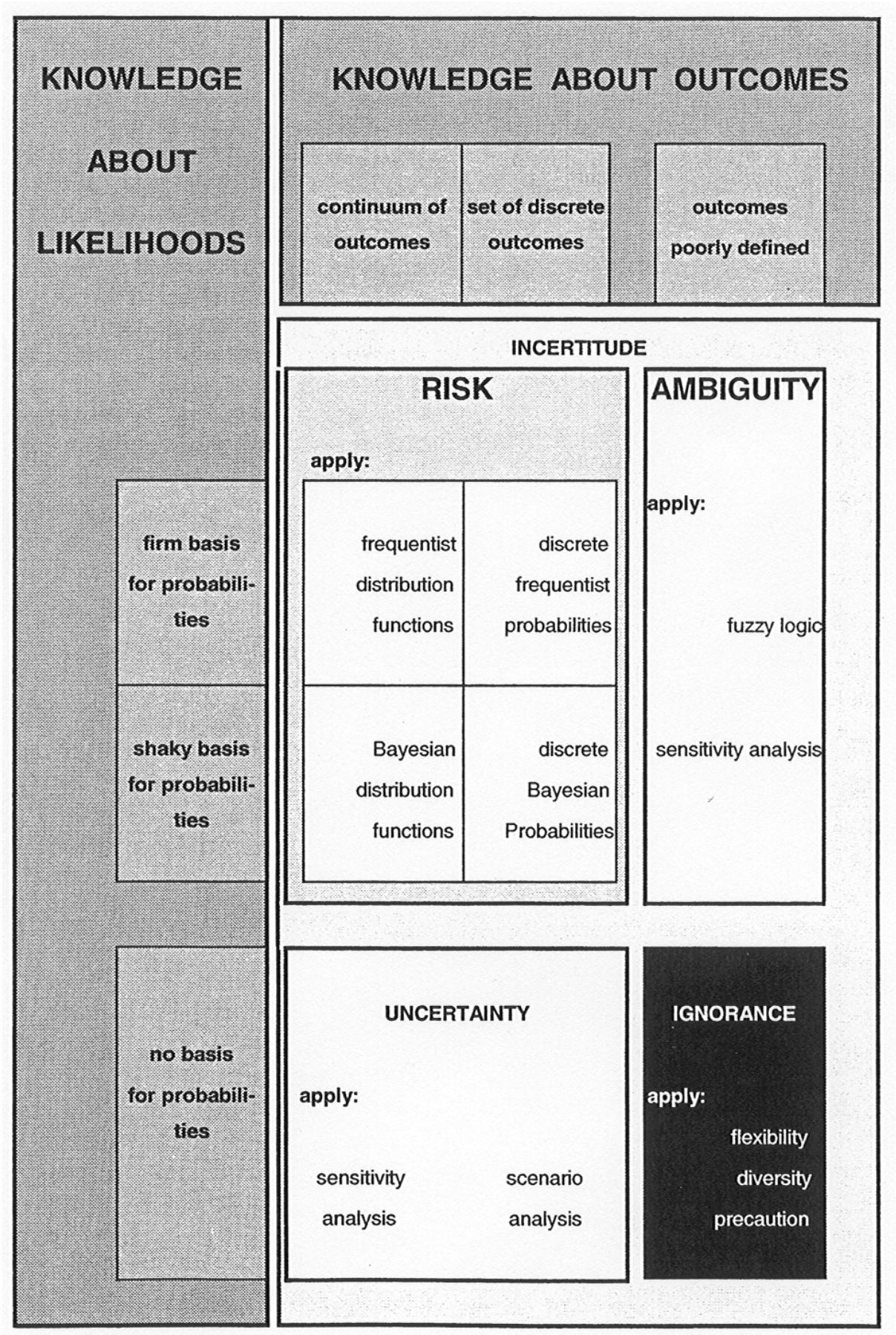

Figure 3. Approaches to the appraisal of risks by Sterling[23]

In the form as represented by Stirling in figure 3 the horizontal axis represents the effect of a hazard, what we do know about it. The vertical axis represents the likelihood of an accident to happen (what we should know about it). It is in this form that Slovic/Stirling is best known, as exemplified by the RIVM publication 'Coping rationally with risks[24]'.
In his paper, Stirling states[25]: 'The crucial point is that intractable uncertainties, ambiguities, and ignorance are routinely treated in the regulatory appraisal of technologies simply by using the probabilistic techniques of risk assessment. This treatment of uncertainty and ignorance as if they were mere risk effective amounts to what economist Hayek dubbed (in his Nobel acceptance speech) 'pretence at knowledge'.
Far from displaying a respect for science in regulatory appraisal, the effect of such scientific oversimplification is actually to ignore and undermine the scientific principles on which risk assessment itself purports to be based. Given the manifest inapplicability – in their own terms – of probabilistic techniques under uncertainty and ignorance, this is a serious and remarkable error. The self-contradictions in aspirations to a 'science-based' approach reliant solely on quantitative risk assessment (…) are thus further underscored and reinforced.' This thesis will show through de Maeslant Barrier case how right Stirling is when we are dealing with innovative complex systems.

2.4.3 Perrow

In 1984 Charles Perrow published his book 'Normal accidents'. In his introduction Perrow states[26]: 'As our technology expands (...) we create systems – organizations, and the organizations of organizations – that increase the risks for the operators, passengers, innocent bystanders and for future generations. (…) Most of these risky enterprises have catastrophic potential, the ability to cripple the lives of hundreds of people in one blow, or to shorten the lives of thousands or millions or more. Every year there are more such systems. That is the bad news. The good news is, that if we can understand the nature of risky enterprises better, we may be able to reduce or even remove these dangers. (…) There are many improvements we can make which are fairly obvious, such as better operator training, safer designs, more quality control, and more effective regulation.
Experts are working on these solutions in both government and industry. I am not too sanguine about these efforts, since risks seem to appear faster than the reduction of risks. (…) Rather I will dwell upon characteristics of high-risk technologies that suggest that no matter how effective conventional safety devices are, there is a form of accident that is inevitable. This is not good news for systems that have high catastrophic potential, such as nuclear power plants, nuclear weapons systems, and recombinant DNA production or even ships carrying highly toxic or explosive cargoes. It suggests for example that the probability of a nuclear plant meltdown with dispersion of radioactive materials to the atmosphere is not once in a million year but more like once in the next decade[27].
Most high-risk systems have some special characteristics, beyond their toxic or explosive or genetic dangers, that make accidents in them inevitable, even 'normal'. This has to do with the way failures can interact and the way the system is tied together. It is possible to analyse these special characteristics and in doing so gain much better understanding of why accidents occur in these systems, and why they always will. If we know that, then we are in a better position to argue that certain technologies should be abandoned, and others, which we cannot abandon because we built much of our society around them, should be modified[28]. Risk will never be eliminated from high-risk systems, and we will never eliminate more than a few at best. At the very least, however, we might stop blaming the wrong people and the wrong factors, and stop trying to fix the systems in ways that only make them riskier.'

Perrow introduces two notions, complexity and tight couplings, which he uses to explain this unexpected, yet 'normal' accidental behaviour. Regarding the latter notion he states: 'The system is suddenly more tightly coupled than we had realized. When we have interactive systems that are also tightly coupled, it is 'normal' for them to have this kind of an accidents, even though it is infrequent. It is not normal in the sense of being frequent or being expected-indeed, neither is true, which is why we were so baffled by what went wrong. It is normal in the sense that it is an inherent property of the system to occasionally experience this interaction'.
Perrow distinguishes between linear systems and complex systems.
According to Perrow, special segregation, dedicated connections, segregated subsystems, easy substitutions, few feedback loops, single purpose, segregated controls, direct information and extensive understanding characterize linear systems. In contrast complex systems are characterised by proximity, common-mode connections, interconnected subsystems, limited substitutions, feedback loops, multiple and interacting controls, indirect information and limited understanding. Tightly coupled systems have more time-dependent processes: they cannot wait or stand-by until attended to. The sequences in tightly coupled systems are more invariant. In tightly coupled systems the overall design of the processes allows only one way to reach the production goal. Tightly coupled systems have little slack[29].
According to Perrow rail systems are linear, tightly coupled systems. I can add that since then the dependency of rail systems on other infrastructures such as GSM-R[30] and in future GPRS[31], make it more and more complex, very tightly coupled systems. In fact through its characteristics rail is developing gradually towards a similar complexity as an airline system.
Even road systems, which are at present linear loose coupled, have a tendency to become more complex and tightly coupled. Many drivers use traffic aids such as auto navigation. They are lost if they fail, although there is nothing wrong with neither the car nor the road. Cars are already communicating with each other to keep a safe distance. Many governments have introduced systems of road pricing or will introduce them at some point in the not too distant future. These systems are at present land-based system with tollgates, but the alternative is a satellite based car born system.

2.4.4 Petroski

In 1984 Henry Petroski published: 'To engineer is human. The role of failure in successful design.' He states[32]: 'I believe that the concept of failure – mechanical and structural failure in the context of this discussion – is central to understanding engineering, for engineering design has as its first and foremost objective the obviation of failure. Thus the colossal disasters that do occur are ultimately failures of design, but the lessons learned from those disasters can do more to advance engineering knowledge than all the successful machines and structures in the world. Indeed, failures appear to be inevitable in the wake of prolonged success, which encourages lower margins of safety. Failures in turn lead to greater safety margins and, hence, new periods of success. To understand what engineering is and what engineers do is to understand how failures can happen and how they can contribute more than success to advance technology.'
Petroski states[33] that engineering success is foreseeing failure. 'No one wants to learn by mistakes, but we cannot learn enough from successes to go beyond the state of the art[34]. Contrary to their popular characterisation as intellectual conservatives, engineers are really among the avant-garde. They are constantly seeking to employ new concepts to reduce the weight and thus the cost of their structures, and they are contently striving to do more with less so the resulting structure represents an efficient us of materials.'

Petroski touches a very important point when he states: 'Thus designers often try to build into their structures what are known as alternate load paths to accommodate the rerouted traffic of stress and strain when any one load path becomes unavailable for whatever reason. When alternate load paths cannot take the extra traffic or do not exist, catastrophic failures can occur.' The problem is that these alternate load paths are extra in the construction and therefore cost money without enhancing the functionality of the system. Therefore increasingly they are designed out of structures and systems.
This is encouraged by the development of sophisticated design methods, such as based on finite element methods, which make it possible to study the behaviour of structures in minute detail and design every part as accurately to its **expected** loading as possible. Even failure of parts can be simulated. However, what sometimes gets overlooked is that the input of such design systems is still a set of scenarios, drawn up by the designer himself. In other words: garbage in, garbage out.
One of the earliest forms of risk management in engineering and design is the introduction of the safety factor in constructions. This is a term describing the load carrying capacity of a system beyond the expected or actual loads. Essentially the factor of safety is how much stronger the system must be designed than it usually needs to be for an intended load. Over time, when we learned more about behaviour of materials and developed better, more accurate design methodologies, the factor of safety declined.
What is ignored is that the safety factor created a margin, which could be used for future developments, without the necessity for expensive reengineering of structures or complete replacement. Many railway bridges of the 19thy century were built with a considerable margin of safety. In England, the Royal Commission, appointed to investigate the use of iron in railway bridges set the margin of safety at 6[35]. Over time this was a rather pessimistic value, yet it created an opportunity to introduce longer trains with higher axle loadings. Many of these bridges survived well into the 20th century and some of them are still in use today! In contrast, quite a few modern bridges have an unexpected short life span because they were designed more accurately, lean and mean.
Petroski advocates two important notions: fail safe and safe life[36]. With fail safe he means designs that should they fail, do it in such a way that safety is not compromised. Failure must be arrested and detected. According to Petroski, safe life is the criterion that allows for the inevitability of failure well beyond the service life of the structure.
Petroski puts the arrow in the bulls-eye by stating: 'No designer wants their structures to fail, and no structure is deliberately under designed when safety is an issue. Yet the designer, client, and user must inevitably confront the unpleasant questions of 'How much redundancy is enough?' and 'What cost is too great? ' (…) Ironically, structural failure and not success improves the safety of later generations of a design. It is difficult to say whether a century old bridge was overdesigned or how much lighter the frames of forty-year-old buses could have been.'
It is these fundamental questions that play a key role in risk management, without many being aware of this. Indeed, to my opinion, too often risk management is seen as a problem to be solved by the engineers and not a managerial problem. Yet, the engineer can only operate within boundaries set by management decisions. If for political reasons an infrastructure must be built in a tunnel, this is inevitably more risk sensitive than the same infrastructure being built on an embankment. In other words: the decision to go for a tunnel cannot be seen separately from the questions of safety management caused by that same tunnel.

This sounds so obvious, yet in reality it isn't. This is exactly what happened in the final stages of the construction of the Betuweroute freight railway from Rotterdam to Germany. For environmental reasons this route runs through a couple of tunnels. In the final stages of construction emerged the fundamental discussion of fitting these tunnels with sprinklers or not. The fire brigades insisted on these sprinklers, yet the ministry of transport considered them a waste of money compared to spending money on other risks.
Risk analysis showed that it was far more cost effective to invest the money in other measures, such as eliminating level crossings in the rest of the rail system than equipping these tunnels with sprinklers. Yet the local fire brigades won this safety battle, mainly because their supreme commanders, who were the lord majors of the towns next to the railway, supported them and refused to issue an operational license for the railway over their territory without these extra safety measures.

2.4.5 Stoop

Stoop[37] states that through history the role of safety and thereby risk management has changed from a 'posteriori application of good engineering practice in the reduction of damage and injuries to a priori scientific approach in the prevention of accidents.' Stoop proposes a linking between safety and the design process. Either explicitly or implicitly safety plays an important role in the decision making in the engineering design process by defining specific risk levels during Analysis, synthesis and evaluation.
According to Stoop, 'safety has always been an aspect in the design of artifacts. The need to implement safety as early as possible in the design process is frequently argued on the basis of cost and effectiveness' (and when looking at recent cases such as the HSL-Zuid and the Betuweroute railway just as easily ignored, resulting in increased costs and project delays further on in the engineering process). According to Stoop: 'to provide an answer to the question how and in what phase of the design active safety should be incorporated proves not to be so simple.'
Stoop states that there are two extremes possible in the approach to safety in the design process:

- A historically based engineering approach on an ad-hoc basis;
- A safety integrated design approach on a conceptual basis.

Stoop indicates that the historically bases engineering approach can be divided in three phases:

1. The material phase[38], which started in the middle of the 19th century where attention in relation to safety problems was concentrated on dust, noise, heat, fire, explosion, disasters and fatal accidents. Safety in the case of technically caused accidents focused on material properties, construction methods and static loads. Gradually an integral approach to health and safety issues emerged. Risk management evolved by learning from disasters, such as bridge failures, boiler explosions, train accidents or industrial catastrophes. Characteristic of this period was the focus on the technical component level and the reliance on gaining experience by a posteriori disaster case study.
2. The energy phase, which emerged at the beginning of the 20th century, where attention in safety engineering widened under influence of the new energy distribution networks (gas, electricity, steam, oil). Safety was primarily according to Stoop 'a matter of discussion between engineers of the Labour Inspectorate and leading industries[39].' The approach to safety was a deterministic one, monocausal and empirical according to Stoop. After WWII some concepts of epidemiology were applied. 'Accidents were defined as unexpected damage by an outburst of energy and were considered to be a special type of 'disease' in the man-agent-environment model. Attention emphasized the damage and injury mechanism, rather than the accident process'.

Preventive engineering strategies (i.e. risk management at engineering level) 'concentrated on the reduction of damage and injury by a number of simple strategies dealing with the elimination or isolation of the source of the hazard, personal protection for thee exposed persons or strategies to reduce damage and injuries. Only in the more complex industries and transport systems was accident prevention emphasized.'[40]

Safety analysis techniques emerged, based on a systems approach. The failure probability of components was subjected to calculation in the engineering of complex systems (e.g. the nuclear industry), which led to standards and certification procedures at the component level and to multiple safeguarding in systems design. Design concepts with respect to safety problems were developed such as safe-life and fail-safe principles[41, 42], crash worthiness and damage tolerance. Accidents according to Stoop 'were considered as essentially multicausal and described as a coincidence of probabilistic and deterministic factors.' The direct effect to risk management was the recognition of the human factor as a key interest (and at the end of the 20th century a growing tendency to eliminate the human factor from safety critical processes, sometimes with adverse effects as illustrated by the Maeslant Barrier Case as described in this thesis).

3. The information phase. The general introduction of the computer to control processes introduced the information phase starting at the beginning of the seventies of the last century. Interest in safety problems and thereby risk management has shifted from reliability of hardware to human behaviour and error and from the safety of machines to software reliability. Computers and cognition are the main topics in the new role of the human being in the man – machine interface according to Hale (1985). 'Great attention is paid to artificial intelligence, expert systems, rule based systems, decision aids, fuzzy functions and normative decisions. Experience is no longer gained from accidents and disasters, but also from near misses, incidents and deviations (Gregory, 1984).'

   It can be added that because of the calculating power of computers, a shift in designing systems and thereby risk management occurred from a deterministic design aimed at preventing specific risks to a probabilistic design, aimed at reducing risks and controlling them at an acceptable level. The Netherlands was on the forefront of this development with the introduction of its impressive coastal defences (Deltaplan) culminating in the earlier mentioned Maeslant Barrier, which is a pure probabilistic design. Human life seen as a subject of risk, with a price tag added. In other words, we started to calculate with lives! And sometimes, the value of life varied according to the economic importance of the area or the activities of the subjects involved (Deltawet / Wet op de waterkeringen). Fundamental was the general acceptance of risk in the Netherlands as part of every day's life, when the policy document 'Coping with risk' was published in 1989[43]. In other words: risk is not something to be eliminated (deterministic, ALARP[44]), but to be controlled at acceptable levels (probabilistic, ALARA[45]).

Stoop advocates a scientific design bases methodology, which deals with three items:

- The structure of the process
- Creativity
- Communication

Stoop identifies five different decision points where risk management is crucial:

1. Safety as a design aspect, using scenarios as an instrument for decision making. This requires a decision towards to operating envelope of the design required.
2. Choices related to the characteristics of the technology chosen. This decision deals with cost effectiveness and attainable levels of safety in later phases of the design process.
3. Level of conception. This decision deals with limitations and assumptions and therefore with risks inherent in risk modeling.
4. Choices related to the level of detailing. This decision deals with aspects of which hazards will be subject of intervention, what intervention strategies will be used (varying from hazard pattern elimination to damage reduction). The aspect of residual risk comes to light, being a function of all previous decisions concerning scenarios, hazards, hazard patterns et cetera.
5. Choices related to safety as an aspect of the evaluation of the design. This decision deals with residual risks, side effects and new risks emerging from the operational phase. It tries to foresee adaptation of the system during its life span including maintenance, upgrades and large-scale modifications.

Stoop identifies the cyclical nature of the management decision-making process. This is supported by the process management theories by amongst others De Bruin en Ten Heuvelhof [46]. According to Stoop 'the design process is repeated until a technical design solution is achieved which satisfies the needs. As it is not likely that all risks can be eliminated, a residual risk strategy must be formulated after completion of the technical design solution. Additional organizational and social measures must deal with the residual risks and side effects emerging from the culture and context in which the artifact is deployed.' [47]

In his thesis Stoop proposes the DCP-diagram as conceptual model to describe the way management of safety should be achieved in complex technical systems. This model will be described in §2.5.2.

2.4.6 Rosmuller

Rosmuller researched the safety aspects of transport corridors[48]. He developed an approach to improve the way safety is analyzed. Clustering of infrastructure is increasingly popular in the Netherlands. This country is very small (35.054 km^2 excluding water areas), yet it has 16.4 mln inhabitants (2007). As such it is one of the most densely populated countries in the world. Space is at a premium. Protecting the environment including the rural areas is also high on the political agenda. This resulted in an increasing policy towards combination of line infrastructures in transport corridors. Examples are the HSL-South high-speed railway from Amsterdam to Antwerp en the Betuweroute freight railway from Rotterdam to Germany.

Rosmuller identifies six traditional steps to distinguish the conduct of risk analysis:

1. hazard identification
2. scenario development
3. frequency analysis
4. consequence analysis
5. risk calculation
6. risk evaluation

According to Rosmuller 'despite the differences between a probabilistic and a deterministic approach of safety, they do not necessarily exclude each other for application. Moreover, both approaches should be employed complementarily. A deterministic approach is needed to develop scenarios for a potential hazardous system and subsequently a probabilistic approach to prioritize and suggest adjustment to the system under consideration. Next, a deterministic approach could yield additional scenarios for the redesigned system[49].

Rosmuller goes on by researching the general single dimensional approach towards risk analysis and safety assessment of transport corridors. Single dimensional in the sense of analyzing each infrastructure in its own right and supposing that the probability of accidents and failures is independent of what happens outside the infrastructure (i.e. no mutual interference and dependencies). More important: this excludes domino effects, where an accident on infrastructure A may influence normal operation on infrastructure B.
Also according to Rosmuller the synergetic effect is being ignored by this traditional approach. 'Because of the occurrence of two or more accidents at the same time, impacts of these accidents may increase the total impact in a way that the consequences are greater than the sum of the individual accident consequences.'
A good example of this latter problem is the power failure west of Amsterdam in 1983[50]. At some time in the morning the auxiliary (emergency) power supply of the major steelworks complex at IJmuiden (Hoogovens, now Tatasteel IJmuiden) was tested, which required energy distribution operation in manual mode. After the test the system was not switched back to automatic mode, as it should have been.
In the evening at the beginning of the peak period at the nearby Velsen electrical power plant an additional generating unit was brought online as was custom, which required some 150 kV switching of generating units. Due to mechanical problems in one of the switches this failed resulting in an unbalance between the phases of the local grid. This imbalance should have triggered the switch board at the steelworks to automatically cut off from the grid to prevent an overload of the local 150 kV node. This didn't happen because the energy surveillance system was still set to manual operation.
Due to an emergency elsewhere in the internal power supply of the steelworks, the operators in the energy control room of the steelworks failed to notice that the outside power supply was in trouble and that the supervising system in their switchboard was not responding. The result was that at some point the entire steelworks was being fed through the 150 kV switching station, i.e. the 150 kV was being switched under full industrial load. In the ensuing flash-over the switches in the 150 kV room vaporized in a massive electrical explosion.
The consequence of this accident was serious and wide-spread. The entire generating plant at Velsen with four electricity generating units was cut off from the national grid at a time of peak demand, after which the local section of the national grid became overloaded. The resulting domino effect was only stopped by cutting off the entire northwestern area around Amsterdam from the main grid, bringing trains to a halt, stopping communication (local telephone network), traffic, industry (the steelworks itself had to shut down completely), and homes (domestic supply). Two incidents which had nothing to do with each other and as a single accident should have resulted in minor damage, hardly noticeable outside the system. In practice they caused a major power failure in a large area of the Netherlands, resulting in millions of euro's damage.

2.4.7 Van Poortvliet

Van Poortvliet studied possible mechanisms for preventing disasters and for reacting adequately if major (unwanted/unexpected) events occur[51]. He analyzed three passenger transport systems and compared them to understand the way high-risk problems are dealt with, and the level of safety that results. These systems (ro/ro passenger shipping, rail transport and large civil aviation) provide insight and understanding of safety problems in general when dealing with complex systems such as transportation systems.

Van Poortvliet shows that in ro/ro passenger shipping 'most of the officials involved in risk management point to the stunning crew errors that caused the incidents, accidents and disasters. From the present analysis, however, it is clear that the concerns regarding direct costs deter from taking actions to keep up with technological developments, that regional safety issues are difficult to manage at an international forum, and that it is exactly the easy attribution of events to failures of individuals involved in operation that camouflages the essence of the problems. The Dutch rail sector shows almost the opposite. It reveals how a blend of conflict, rhetoric, procedural behaviour, analysis and technology meant that safety was warranted, but at high financial costs[52]. Risk management in aviation, (..) relies heavily upon the use of standards. The decision making in this sector is consequently technocratic, resulting in numerous technical issues being largely under control, but at the same time also resulting in social vulnerability'.
Van Poortvliet developed the hypotheses that relate the characteristics of risk management to safety performance. 'The existence of groups focusing solely on safety is found to make disasters less likely, and, if these events occurred, better able to prevent them in the future. Rivalry and ad hoc coalitions between such groups contributed to advocacy for safety, which is necessary to overcome the short-term interests when far-reaching choices have to be made. Guaranteeing quality by means of standards reduces the likelihood of accidents occurring, but makes the actors involved also less sensitive to uncovered issues. Unless great effort is made to keep standards up to date and other strategies are implemented, it will be difficult to prevent disasters from occurring. Programs for targeted, in-depth risk reduction are found to be effective for reducing major risks, however, in non-hierarchies with many players they are difficult to establish. It has also been observed that large programs distract attention from other risks; therefore, priority setting is only beneficial for safety if there are obvious largest risks apparent from comprehensive safety oversight. Learning (..) is only partly the result of intention. It may also result as a side effect of the use of strategies and emerge from non-planned, interactive processes[53]'.

2.5 Conceptual models

2.5.1 Behaviour of a risk sensitive system

Based on a model made by the Ministry of the Interior, Beukenkamp designed a graphic illustration of the behaviour of risk-sensitive systems in day-to-day operation. There are three clear boundaries. The first one is called the normal operational level. This is the level at which the operator chooses the system to function. This must be somewhat higher than the minimum acceptable level of operation, because there will always be fluctuations in the systems behaviour. On the other hand, an operator might choose to operate at a much higher level than required, because the improved quality of the system thus achieved can be an extra selling point, despite the higher operational costs.
The second one is set by the agreed minimum level of normal (service) operation, usually resulting from service level agreements. This level is therefore called the SLA-level. The second level is the minimum level at which a system can operate to fully support its intended functions.
The third level is the minimal acceptable operational level of the system. This level is the minimum level at which a system can operate to function at all, the minimum operational level. It is the level at which the system can function without shutting down are otherwise dying. Below this level the system can only be saved from collapse with outside help.

During normal operation disturbances of the regular situation can occur. Either these disturbances are planned (testing, maintenance, upgrades) or unexpected (failures, damage to live and properties). This can result in a situation where the operation of the system dives below the SLA-level. This is what we call an accident.
A resilient system is capable of a quick recovery, where the deterioration of the system is stopped quickly and recovery takes place almost moments after the initial failure. If the deterioration of the system continues unstopped, it might result in a situation where the existence of the entire system is in jeopardy. This is usually called a crisis or worse, a disaster. To recover from this condition, a backup is required, because the original system is too much damaged to recover on its own. If backups or fallback arrangements are not at hand or fail, the existence of the entire system is under threat. It might shut down completely or fail irreparably (such as a ship sinking or a plane crashing).
One of the most complicated systems of all, the human body, behaves in such a way. An example of a fallback arrangement in crisis is bystander Basic Life Support after a circulatory failure. Chest compressions and mouth-to-mouth resuscitation applied by bystanders help the body to recover from heart failure until the heart is capable of doing its job properly. Without this outside help, the casualty will die, because his brains won't survive the lack of oxygen for more than five minutes.

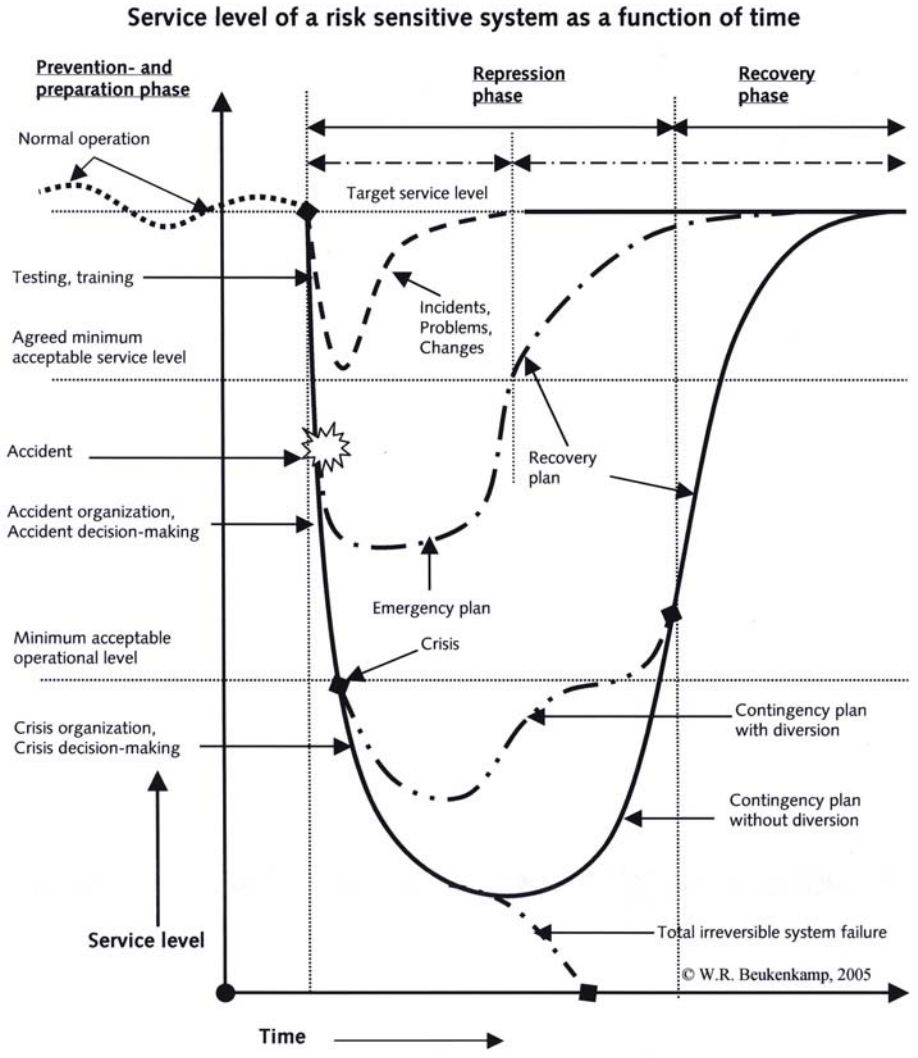

Figure 4. Behaviour of a risk sensitive system

2.5.2 DCP-diagram by Stoop

To bring rationality back into the design and control process of transport systems, Delft University (Stoop) developed the DCP-diagram. The idea behind the Delft methodology is that it combines the design process of systems like transport systems with a process model for policy making. It shows the consequences when strategic decisions do not include security and safety aspects, thereby causing them to be positioned both (too) late in the design process and (too) low in the management hierarchy.
In fact it shows that some level of overreaction by management or government is to be expected when a serious problem like a terrorist attack occurs, given the way systems are designed and operated and given the need for governments not to look indecisive. This notion consists of three principal elements, being Design, Control and Practice (DCP). They can be interrelated along three dimensions, being a systems approach, a life cycle approach and a design approach. Together they constitute an integrated safety and security prototype: the DCP diagram (figure 5).

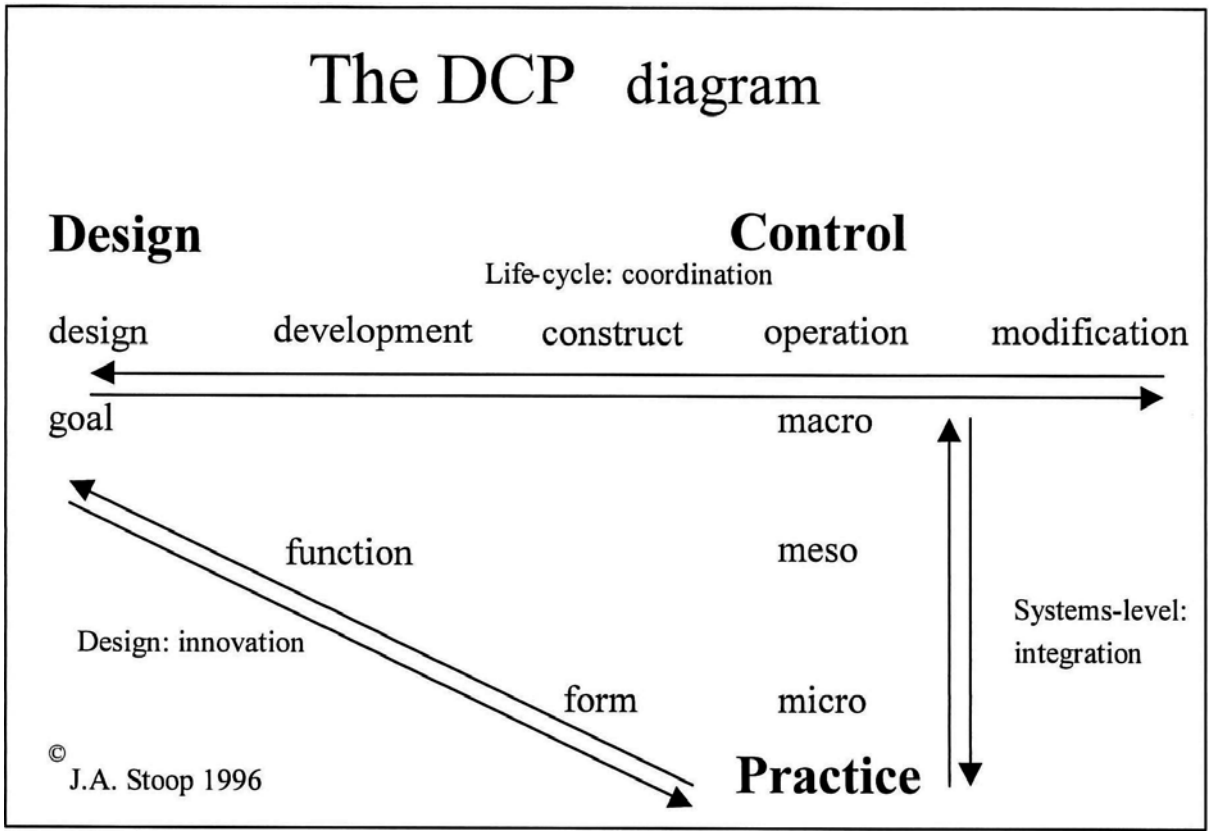

Figure 5. DCP-diagram (Stoop, 1990)

A **systems dimension** defines three levels:

1. The micro level of the user/operator;
2. The meso level of organization and operational control;
3. The macro level of institutional conditions.

In this dimension the issue of integration of administrative and emergency organization across the various levels is crucial.

The **life cycle dimension** defines a series of subsequent phases, being:

1. Design;
2. Development;
3. Construction;
4. Operation;
5. Modification or demolition

In this dimension the coordination of decision-making among actors across the phases is crucial.

The **design dimension** identifies three principal phases in design, being:

1. Goal -expressed by a program of requirements, concepts and principles;
2. Function -expressed by design alternatives;
3. Form -expressed by detailed design complying with standards and norms.

In this dimension the potential of technological innovation for new safety solutions is crucial.

Eventually only in practice is safety visible and actual consequences of accidents or terrorist attacks occur. At each of the other levels and phases however, separated in time or space, safety critical decisions have been made by different actors. The diagram demonstrates who, how, at which moment can contribute to safety, security and risk assessment.
A transport system designed this way can be made resilient towards threats like terrorism for the following reasons:

- At the top (political) level decisions are made what the government, representing society, is prepared to accept as damage and what it does not want to accept, i.e. the prize it is willing to pay. Also the necessary organisation to deal with such extreme situations is established.
- The consequences of these decisions are translated into systems requirements, such as performance requirements like maximum allowed downtime or scenarios that should never ever happen, never mind the costs.
- These requirements translate themselves both into design parameters before the system is build (organisation, information and technology), and control procedures when the system is operational to prevent its use outside the design envelope, due to midlife updates or modifications of systems with a long life span.
- Problems in control of the system or during its construction loop back to the (management) level where the requirements originally came from or the original decisions were made and must be re-evaluated there (and not at a lower level as often happens).

2.5.3 Rounds model by De Bruin, Ten Heuvelhof and In ‘t Veld

In 1998 De Bruin et al published a book, titled ‘Proces Management’. They described a new approach to the design process, which to their opinion was not a linear process, as many would like us to believe, but a far more dynamic series of phases, whereby each phase represents a round. De Bruin et al come up with several notions to describe this, being the decision making in networks, individual versus collective rationality, process design, science and decision making and quality of the decision making process.
In systems components play an important role, whereas in networks actors are important. The rounds model couples structures to processes. Decision-making processes usually take place in networks. This implies that multiple actors are involved with different and sometimes conflicting interests and mutual interdependencies.

Dependencies imply that actors are not capable of solving a problem themselves. They must cooperate to realize their own goals. There many differences between actors (pluralism), which make it very difficult to cooperate into a decision-making based on mutual consensus. An extra complication is that during the process, actors appear and disappear. Because of this, the decision-making process in networks works out in a whimsical way.
If during the course of the process an actor notices that his interests are being harmed by the emerging solution, he might be tempted to block further decision-making. This is a form of strategic behaviour stimulated because in networks usually there is no apparent hierarchy. Because of this the decision making process in a network shows more signs of a process that is characterized by rounds, like a sports game (a boxing match according to de Bruin et al). However, in a boxing match, according to De Bruin et al, the number of rounds is fixed, unless the match is ended by a knockout.
In decision-making processes new rounds can be added by actors if they feel a need for it. Such an additional round can be judged necessary by an actor, if there are new developments; the looser can see opportunities in such a situation to make good his initial loss and try to revoke the original decision. On the other hand, new actors can enter the arena. It is also possible that some actors reappraise their original position and to try to backtrack on their original decision.
Another problem is that new external information becomes available, that warrants a reappraisal of the original problem and/or solution.
Finally some actors only become active at the end of the process, when the solutions become mere visible and more touchable. It is only then that they realize the (possible negative) consequences of this for their own position. They might be tempted to block further decision-making or try to redirect the process[54]. Another problem is that new issues can be coupled to existing ones, despite the fact that at first sight, there is no direct connection between them. This could be the result of a desire by an actor to be compensated for earlier losses. And last but not least actors can behave in a strategic way. They might show a low profile and take some losses earlier in the process, to hit back later on, because these losses might give them a stronger position in a later phase of the process.

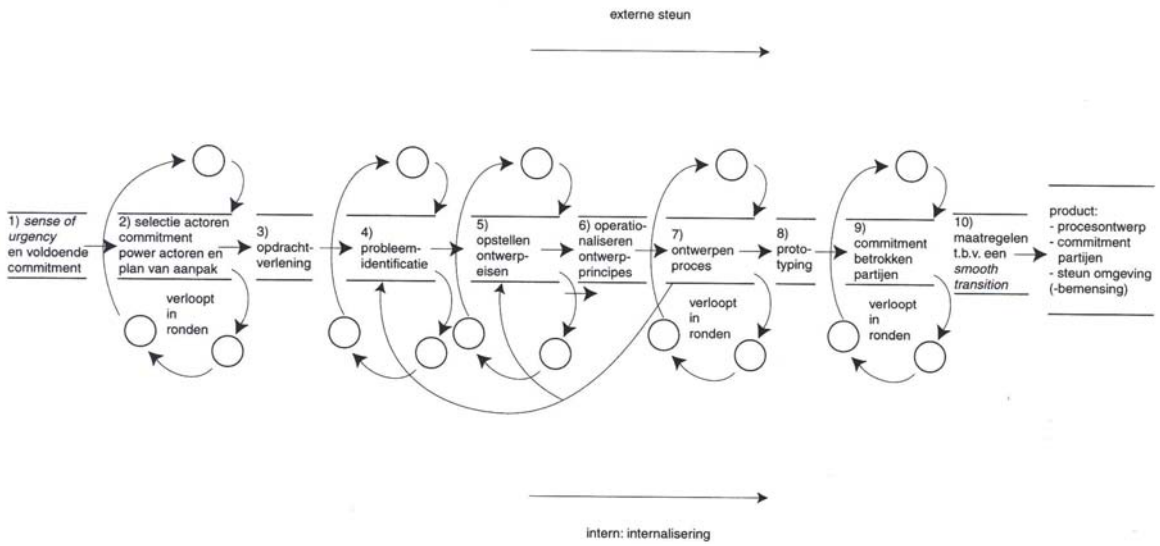

Figure 6. Rounds model by de Bruin & Ten Heuvelhof

2.5.4 AVV WAI model

Based on the DCP diagram of Stoop as previously shown and the theories of De Bruin et al, AVV/Transport Research Centre developed a more dynamic model of the decision making process in complex systems, called the WAI model. This model introduced levels of communicative interactions with various actors interacting and sometimes interfering with the development of a system.

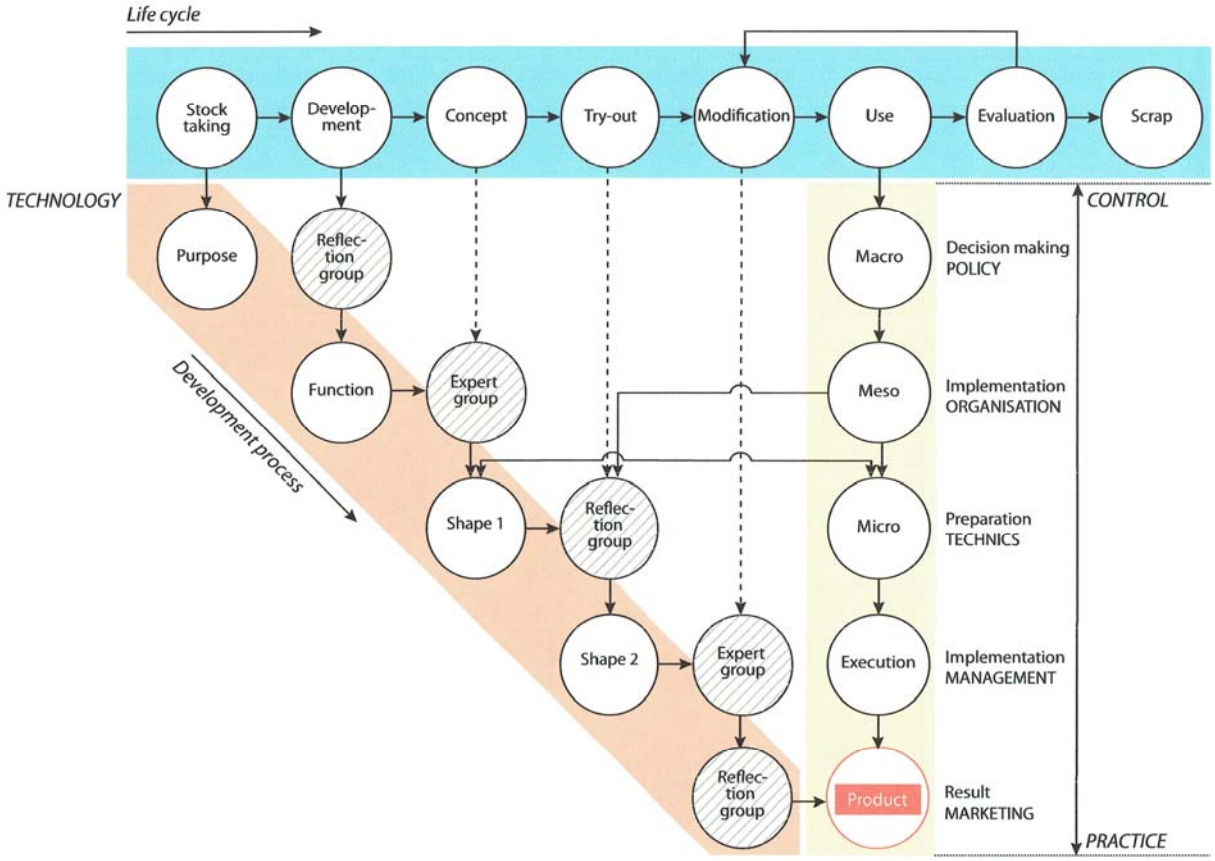

Figure 7. AVV WAI diagram

2.5.5 AVV Pizza model[55]

Traffic is a typical phenomenon of the transport system. People and goods travel from A to B. If they do not do this on foot they will use a vehicle for this movement. On foot or by vehicle they travel on roads. Those roads in turn are part of the spatial environment. The road network and the immediate environment are usually referred to with the concept of infrastructure. Traditionally the transport system is seen as a system in which the elements 'road user', 'road' and 'vehicle' interact with each other. From road safety analysis it appeared that it would be more appropriate not to speak of 'road' but of the 'physical environment', since the surroundings of the road are a factor in road user behaviour as well.
Methorst[56] argues that from the pedestrians' perspective, not only movement but also sojourn in public space should be regarded and that from a pedestrians' perspective the system is made up of four groups of element: pedestrian, the social environment (other humans in the environment), the transportation system (a variety of vehicles) and the physical environment. This can be pictured in a model, see figure 8, that helps detecting fundamental relationships.

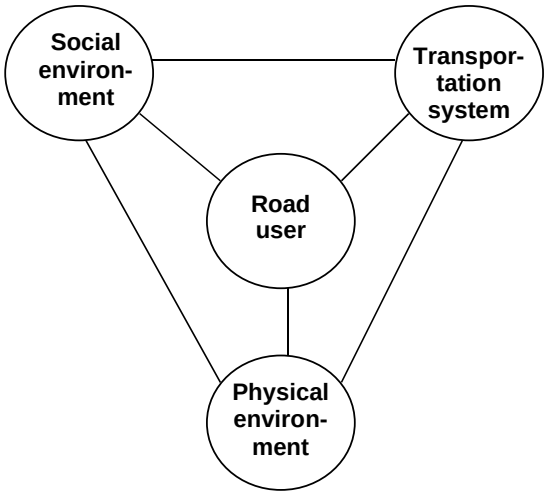

Figure 8. Representation of a road transport system

With regard to interventions there are a number of relevant levels of interaction: a micro level relating to (short term) operational behaviour of road users, a meso level relating to medium term tactical decisions that stakeholders make and a macro level that relates to long term stakeholders' strategic decision.
As a means for policy development the Pizza model[57] was developed. Its aim was to form a source of inspiration for devising comprehensive transport and road safety interventions. Basically it is a picture-checklist. It aims at helping the policymaker to check whether all options are included in the desired comprehensive approach.
At a general level the Pizza model (figure 9) shows that interventions can be directed at the various components: interventions can be directed at the mobile part of the transport system (**internal**) and the stationary (**external**) part. Another perspective is that interventions can be directed to **human** factors or to 'things' **(technology**).
More target oriented, interventions can be directed on a number of levels:

- **Micro level**: the quality of the interaction on the operational level depends on the characteristics of individual road users (pedestrians and others), individual vehicles and the immediate surroundings (place).
- **Meso level**: provides conditions and organisational context for the interaction of the individual elements
- **Macro level**: provides the structural preconditions for the interaction on the strategic level

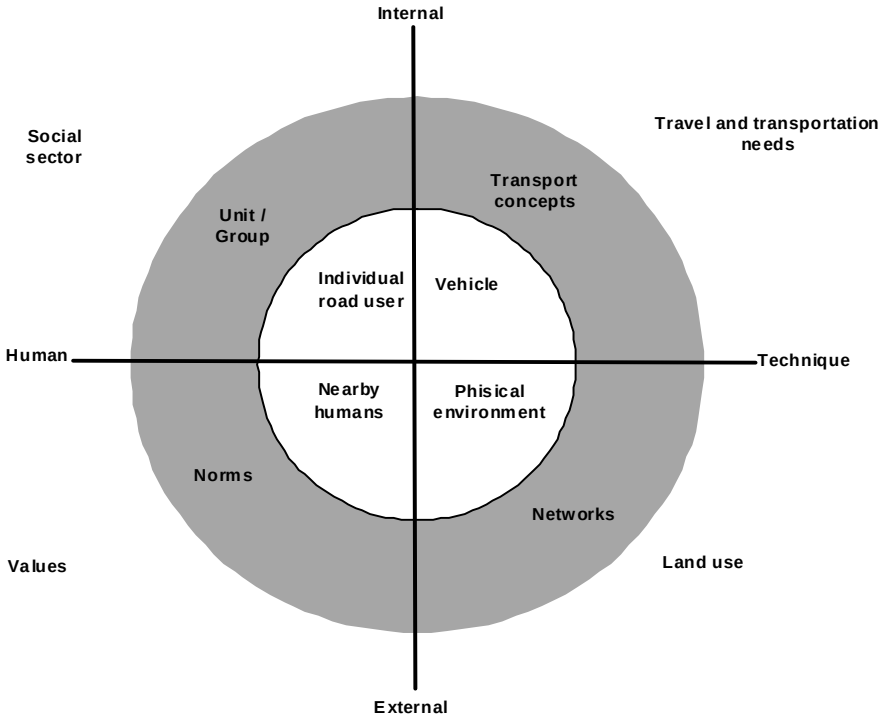

Figure 9. Pizza model; checklist for interventions

Traditionally transport and road safety policy was mainly aimed at the core of the pizza, or the concrete measures that can be realised on the relatively short term and that produce relatively fast results. The middle level concerns mainly measures that are more far-reaching, take substantially more preparation, in the order of magnitude of 3 to 5 years, and usually do not result in demonstrable effects in the short term. In the outermost layer processes take place gradually but very slowly. It can sometimes take thirty years for a change to have noticeable effects.
Evidently the Pizza-model can also be used as a starting point for making forecasts. Since preconditions change slowly and gradually, relatively reliable volume effects can be deduced from them. Meso level items can help to indicate quality effects, but core level behavioural items do not have great potential for forecasting, since these are not very constant.

2.6 Conclusion

Whatever risk management technique you use, sooner or later you will encounter decision making dilemmas such as described by George. Research question 1: *What are accepted risk management techniques related to infrastructures?* can be answered as follows. Generally accepted risk management techniques related to infrastructures follow the lines as generally set out by Slovic and Sterling. Slovic ranks risks according to the factual knowledge about them (the unknown factor) versus the perceived risk, the dreaded risk.
Sterling showed that you could identify risk and their most effective approaches by ranking them more or less similar to Slovic according to the effects of a certain hazard versus likelihood of the accident actually to happen. Perrow introduced the notions of complexity and tight coupling thus explaining sometimes unpredictable behaviour of systems.

Petroski showed that given enough statistical data in general the probability of a specific hazard can be quantified. However, in many cases the failure itself remains unpredictable in time and mode. One thing is certain: sooner or later the system will fail in a way that was never foreseen, yet it was inevitable given the complexity of some systems.
All these analysis are quite static in their approach. Time is not a dominant factor, although it is not difficult to show that the behaviour of a risk-sensitive system changes constantly over time. Stoop looked at the life cycle of a system, thus introducing some kind of dynamic behaviour. Like De Bruin and Ten Heuvelhof he supports the cyclical nature of management decision-making processes. His model was improved by AVV/Transport Research Centre into the WAI model which paid attention to dynamic interactions between the various levels of design and operation. Rosmuller and van Poortvliet show that present risk management strategies tend to be static, to emphasise on prevention. Learning from disasters in a dynamic way is difficult at present.
All these approaches and conceptual models are still based on precaution and prevention. They do not address the complexity of the accident itself, the chaos, the dilemmas that face the decision makers when dealing with the unknown unknowns. Nor do they fully address the behaviour of the system itself during use (although Stoop goes a long way), ignoring deviations from a once stable predictable state that can result in drifting into failure.
Important is the transition from system to network and from component to actor. The importance of this will be shown in the next chapter, dealing with conflicts in risk management. Finally the question can be asked what has resulted from the discussion concerning developing all kinds of models? Perhaps it is time to look again at cases from practice and their relation with the design process.

Notes

[1] In Britain under common law, any chattel which brought about the death of a man was *Deo Dandum* (to be given to God) and so liable to be forfeited to the Crown for pious uses. The value of the deodand was to be decided by the jury involved. This was usually a total sum, not necessarily resulting from a calculation of the cost of the individual victims. This sum was not awarded to the victim or his family, but to the magistrates of the location of the accident. In other words: it was a fine. As an example, in the railway accident of December 24, 1841 at Sonning cutting near Bristol, the jury laid a deodand of £ 1.000 on the engine 'Hecla' and her train, payable by Crown Grant to the Lord of the Manor of Sonning. This was subsequently challenged by the Board of Trade and reduced to a nominal sum.
[2] Art. 17: The carrier is liable for damage sustained in the vent of death or wounding of a passenger or any other bodily injury suffered by a passenger, if the accident, which caused the damage so sustained, took place on board the aircraft or in the course of any of the operations of embarking or disembarking.
[3] This was clearly illustrated by the political discussions in Britain in the aftermath of the Southall (September 19, 1997) and Ladbroke Grove (October 5, 1999) railway disasters near London. In both cases, automatic train protection (ATP) could have prevented these accidents and thereby could have saved many lives. However, given the value of statistical life (VOSL) as used in the UK (valued at the time at a level of approximately £ 2 mln) and the likelihood of these accidents, it was analytically not justifiable to introduce ATP on a large scale in the UK, because ATP would cost up to £ 14 million for each additional life saved (Murray, 2002 p. 64). This is a classic example of the George dilemma.
[4] Ref. Tweede Kamer, 1989
[5] Ref. Beck, 1992
[6] Ref. Sapolsky 1990: 83
[7] Ref. Majone 1994

[8] Ref. George, 1980
[9] Ibidem
[10] Ref. Slovic, 1987 – 1999 – 2004
[11] Ref. Stirling et al, 2000
[12] Ref. Perrow,1984
[13] Ref. Petroski, 1992
[14] Ref. Stoop, 1990
[15] Ref. Rosmuller, 2001
[16] Ref. Van Poortvliet, 1999
[17] Ref. Slovic, 1987, p. 280-285
[18] Ibidem, p. 280
[19] Ibidem, p. 280
[20] This is clearly illustrated by the problem of the transportation by rail of chlorine in the Netherlands. In 2002, after a lot of social and political pressure, the ministers of the environment and economic affairs in the Netherlands agreed to pay € 65 mln to the chemical industry (AKZO) to relocate the chlorine production plants closer to the end users. Experts considered this to be a waste of money, because from an analytical point of view, the risk related to the movement of chlorine by rail was negligible, being less than 10^{-9}/year. In fact other transports such as ammonia scored much higher on the risk lists, yet they were not the subject of such fierce debate.
[21] Ibidem, p. 282
[22] Stirling, 2000 p. 297
[23] Stirling, 2000 p. 298
[24] RIVM, 2003 p. 23
[25] Stirling, 2000 p. 299
[26] Perrow, 1984, p. 3-4
[27] Remember that this was written two years before Chernobyl. The Maeslant Barrier case (see §3.2) is a further example of how true this statement is. Again an estimated (designed) probability of failure of once every 1000 times in practice turned out to be more like once every ten years before remedial action was taken.
[28] The future of the ERTMS/ETCS train signalling and control system is typical for such a problem. Researchers from Delft University (Stoop et al, 2007) investigated this in relation to the problems that have occurred in the commissioning of the HSL-Zuid high-speed railway from Amsterdam to Antwerp. They warned, given the complexity of the system and the expected increase of complexity in future upgrades, to be very careful to move ERTMS/ETCS to higher levels. '*It is desirably to carry out a safety effect report for ERTMS software and system development. This applies in particular for the development and possible introduction of ERTMS level 3. This assessment should have the effect that in practice no hidden deficiencies and unforeseen consequences occur due to implicit design decisions.'*
[29] An example of such a development is the removal of a great many points (switches) in railway systems, because they are seldom used, cost much to maintain and create additional derailment risks. However, at the same time, these secondary (often little used) switches created a form of flanking protection, whereby a train running through signals at danger could be diverted away from a conflicting train movement (resilience of the system). Accidents such as the one ad Ladbroke Grove, 1999, could have been prevented if such a flanking protection had existed. Now, there was only one path left for the rogue train, a path to disaster. By removing the secondary switches, the already tight-coupled system became even more tight-coupled.
[30] GSM-R, Global System for Mobile Communications - Railway or GSM-Railway is an international wireless communications standard for railway communication and applications. A sub-system of European Rail Traffic Management System (ERTMS), it is used for communication between train and railway regulation control centres.

[31] General packet radio service (GPRS) is a packet oriented mobile data service available to users of the 2G cellular communication systems global system for mobile communications (GSM), as well as in the 3G systems.
[32] Ref. Petroski, 1984, p. viii
[33] Ref. Petroski, 1984, p.62
[34] Again, the ERTMS/ETCS case is an example of the importance of this notion. It was only through testing that the fundamental problem of incompatibility between two systems designed and built under common specifications emerged. Despite this, the pressure was very strong to cut short the testing phase. Indeed, the Stoop report (Stoop et al, 2007) urged the Dutch ministry of transport to execute a full testing on this system and not pinpoint itself on commissioning schedules.
[35] Ref. Petroski, 1984, p. 101
[36] Ref. Petroski, 1984, p. 114
[37] Ref. Stoop, 1990
[38] As this thesis indicates, the material phase is preceded by a financial phase, where only financial risk of cargo and ship counted and human interests such as labour safety were being ignored.
[39] On the factory floor perhaps this is true, but in many countries safety legislation appeared already in the midst of the 19th century, e.g. for railways and the storage of dangerous goods, indicating that at quite an early stage in modern technological history safety became a national political issue as well.
[40] This is very well illustrated by the fact that in most Western European countries after WWII some form of automatic train protection was introduced to protect against collisions between trains. However, a similar development took place by the end of the 19th century, when automatic continuous train brakes were introduced (air and vacuum). This tends to indicate a different safety cycle: introduction – accidents – growth – disasters – risk awareness – risk reduction (preventive measures/legislation) – accidents – innovation.
[41] See Petroski
[42] One of the first examples of a fail-safe design is the automatic train brake as invented by Westinghouse around 1860. If the train parted or the air pump would fail, the brakes of the carriages automatically would come into action and the train would be stopped. The vacuum brake as used in some countries worked on the same principle, but used vacuum to keep the brakes of instead of compressed air. This vacuum was created by the use of a steam ejector or other means of vacuum exhauster.
[43] Ref. Tweede Kamer, 1989
[44] As low as reasonably possible (sometimes also jokingly expressed as ‘As low as reachable politically’)
[45] As low as reasonably achievable
[46] De Bruin et al, 1998
[47] The Dutch Ministry of Transport and Water Management (MinV&W) supported this latter view, when it formulated its new policy towards safety and risks ‘Verder met veiligheid’ (On with safety) (MinV&W, 2002). This policy document formulated four ambitions for a common view on safety:

1. Permanent improvement
2. Explicit and transparent consideration towards mitigating measures
3. Preparation towards the management of inevitable (residual) risks
4. Implementation of safety management and a safety culture within the ministry

[48] Ref. Rosmuller, 2001
[49] Indeed I can add that although Rosmuller identifies two approaches (a deterministic and a probabilistic one) he mentions in fact two more, which are being used in these processes as well, i.e. the scenario analysis and the sensitivity analysis. In fact Rosmuller implicitly identifies the context as described by Slovic and Stirling as determining factors in a dynamic process of developing complex systems with continuous interactions between all four approaches.
[50] The author was actively involved in this accident through his work for the engineering department of the steelworks.
[51] Ref. Van Poortvliet, 1999

[52] See the case about automatic train control, further on in this thesis
[53] Notice that Van Poortvliet wrote this shortly before the Enschede fireworks disaster (May 13, 2000) and the Volendam pub fire (December 31, 2000), both of which resulted in national inquiries.
[54] An example is the problem of fire safety in the tunnels of the Betuweroute freight railway. Only in the final phase of the building process emerged the problem that the fire brigades were not happy with the way fire-safety was dealt with by the project management.
[55] The Pizza-model was introduced in 2000 in the road safety section of the Dutch handbook on transport and traffic sciences (Methorst, 2000). The model was published in English in the Vulnerable Road Users report (Methorst, 2003)
[56] Ref. Methorst, 2003
[57] Ref. Methorst, 2000

3. Empirical lessons from practice: hidden dangers

3.1 Introduction

The previous chapter has shown that it is important to look at the transition from system to network and from component to actor. This chapter will show this in more detail by looking at conflicts in risk management and how they are dealt with. Also this chapter take will another look at cases from practice and their relation with the design process.

Complex safety-critical systems are at the core of modern society. They dominate everything from transport to digital banking systems. Usually they perform quite well. Problems arise when they break down. Sometimes expensive defensive systems are designed and build to counteract such a failure. They themselves are also safety-critical and susceptible to unexpected failure.

This chapter aims to answer research question 2: *What role do safety and security issues play in the decision-making processes regarding large scale infrastructures in the Netherlands*?

The previous chapter showed the importance of looking at the behaviour of systems over time. Where once they were very reliable and predictable, after many years of use their reliability and predictability can diminish. Risk management techniques should address that inevitable property of such systems.

Sometimes they fail to do that, either because their design approach was static or the boundaries of the initial design envelope were not safeguarded (drifting into failure). This chapter will show important empirical lessons from practice. Although they may appear to be anecdotic it will be shown that they are exemplary of every day's practice regarding safety critical systems, by exposing some of their hidden dangers and conflicts in risk management.

3.2 Unravelling criticality: the Maeslant Barrier

Figure 10. Headline in AD national newspaper: 'many errors in Maeslant barrier'; an example of framing and scoping by the press

3.2.1 System citicality: three dimensions

Safety-critical systems have become a general part of every day's life. With increasing reliability of technology, serious failures have become less common than a couple of decades ago. Yet catastrophic failures still occur in safety-critical systems.
The increasing reliability of the hardware is sometimes overshadowed by seemingly increasing unreliability of control parts (software and firmware). The resulting unpredictable behaviour of dynamic complex systems becomes the focus of many discussions as recent events have shown (automotive industry among others): failures of luxury motorcars due to software problems in the control units (Mercedes, BMW and most others).
Questions should be asked not only how systems have become critical, but also why they are critical. What does criticality means? Three dimensions can be identified:

- Structural systems integrity;
- Response time envelope;
- Knowledge deficiencies.

These dimensions play a major part in explaining the behaviour of safety-critical systems as developed by the Delft University of Technology in cooperation with its research partners AVV/Transport Research Centre[1] and DHV. This paper deals with the latter aspect of knowledge deficiencies. The other mentioned aspects will be subject of future studies.

3.2.2 Multi-actor decision-making processes

In multi-actor decision-making processes a definition of criticality becomes actor-, aspect- and context-dependent, adding new dimensions to Charles Perrow's systems dimensions of complexity and coupling[2]. Criticality becomes a multi-dimensional notion, where uncertainty in such decision-making processes hampers a concise identification of systems criticalities and their consequent mitigation.
In order to identify and analyse criticalities, analyses should cover all relevant factors, actors, aspects and decision-making options in order to achieve societal support for and cost-effectiveness of responding to critical events as George described in his model of dilemma's facing policy decision-making[3].

Retrospective accident analysis in high-tech systems such as aviation and the railway industry enabled the identification of essential physical design principles, like fail-safe/safe-life, crashworthiness and damage tolerance, graceful degradation, mode- and situation-awareness, as Beukenkamp has shown following Petroski[4]. Timely adaptation and modification of critical systems should prevent recurrence of similar events in the future.
At a systems level, analysis of systems characteristics and deficiencies is required in order to prevent the next critical event by analysing accidents and catastrophic failures beyond the level of systems technology. In the earliest stages of the design process, criticalities should be identified and eliminated or mitigated by detailed systems analysis along lines of decomposition of architecture, time line and causal sequence dependencies and knowledge uncertainties in order to identify system deficiencies of a technical, organizational and institutional nature.

3.2.3 Problems with the Maeslant Barrier

In 1997 Queen Beatrix of the Netherlands formally commissioned the Maeslant Barrier. This Barrier is the final part of the massive Delta-project, started in 1953 after the disastrous floods in that year. Design of the Barrier started around 1986 as part of a competition. Six designs were evaluated of which the Maeslant Barrier was the winning one (see figure 11).

Figure 11. Maeslant Barrier in normal position (left) and closed position (right). Its design was dictated by the need to comply with a preset risk estimation.

In 2002 first signs indicated that the Maeslant Barrier turned out to be potentially far less reliable than originally calculated. The problem became more serious when the knowledge about this resulted in articles in national newspapers[5],[6] at the beginning of 2006, forcing the deputy-minister of Transport, Public Works and Water Management to explain these problems in Parliament.
According to an article in the national press[7], the problem was that ‘Because of hitches in the Maeslant Barrier near Rotterdam, the coastal defences behind it might have to be reinforced. Then deputy-minister of Transport, Public Works and Water Management Mrs. Schultz van Haegen reported this with some reservations in a letter to the Dutch Lower House of Representatives. Sometime later it became apparent that the Barrier near Hook of Holland safeguarding the entrance to the Port of Rotterdam and a major urbanized area to the north of it, was less safe than anticipated. The fully automated closure of the two doors were expected to fail once every nine times, whereas the accepted (and originally designed) failure rate is only once every thousand times.

Minister Schultz van Haegen wanted the Barrier, entitled by her as the 'front door', to function properly. She ordered research into the likelihood of the failure rate being permanently more than once every 1000 times and the effects this has on the present probability of a major flood in the areas protected by the Barrier. She would not exclude that research could show that additional measures in these areas would be necessary, if no other options were left.
Some actors urged the Ministry to order the dykes to be raised after all. Others claimed that this was utter nonsense because the prohibiting costs of raising the dykes were the original justification to building this massive Barrier.
Professor de Ridder of Delft University of Technology, actively involved in the design and construction of the Barrier, stated publicly: '*If you use your common sense you don't raise the dykes because a computer program doesn't function properly. I wouldn't know how high the dykes should be build*' .
Conclusion: uncertainty at the level of data on surge frequency and consequences has to be combined with uncertainty on technological reliability of operating the Barrier and the structural integrity plus knowledge deficiencies.

3.2.4 Dynamic complex system

The Maeslant Barrier shows every characteristic of a dynamic complex system. The system is dynamic because of:

- Interactions with the surrounding areas;
- Predictability of functioning becomes only predictable during operation.

The system is complex because of:

- Interactions with the transport system of the Port of Rotterdam;
- Continuous upgrades of the command and control systems (software), creating life-cycle instabilities.

The Maeslant Barrier is without doubt a vital system, according to the definition of vital as used by the Ministry of Transport, Public Works and Water Management. Failure of the Barrier could inflict more than 1,000 lethal casualties and/or more than € 5,000 mln damage. Does this vitality make it a safety-critical system? A valid question because not every vital system is critical, since criticality implies that failure of the system results in imminent danger, progressive collapse and irreversible loss of functionality of the system under protection.
Given the original alternatives including raising the dykes behind the present Barrier, it must be concluded that the Barrier is indeed critical. Failure of the Barrier gives not enough response time for alternative actions. In fact as IJsselstijn et al have shown[8] that failure under such conditions implicates possible negative response time, i.e. the required response time is less than the available time.

3.2.5 Probabilistic design

The functioning of the Maeslant Barrier depends on three elements:

- The decision support system BOS, which indicates when there is a possible storm tide situation that could justify closure of the Barrier. BOS communicates with the Dutch national high tide warning system HMS.
- The control system BES, which controls the processes during closure and opening of the barrier.
- The hardware of the barrier itself.

The design of the system is a pure probabilistic one, based on proven reliability. One of the consequences of this presumption was that the Barrier was designed and built as a fully automated system since the human interface was regarded as being too unreliable.
The other reason for opting for a 100% computer controlled system was that dynamic instabilities during the final phases of closure make it very difficult for a human operator to control this part of the closure process by feedback control at the actual systems state. It requires a lot of training, which in practice is difficult to achieve since the Barrier only closes once a year for testing and once every five to seven years in anger. More frequent closures are unacceptable for the operation of the port of Rotterdam, one of the largest ports in the world. Feedback learning potential from operational experiences is limited by necessity.
This fundamental design required very sophisticated command and control models, using some form of artificial intelligence. Proving the reliability of the hardware was not an easy job, but overshadowed by proving the reliability of the two software systems. However, given the state of the art (around 1995), software architecture was not complex enough to make it impossible to prove its reliability. Therefore, the design was accepted and delivered.
Unforeseen during design and construction was the speed at which software developed. Frequent new releases were (and still are) common, making it difficult for the operators and even more for the technical system managers to keep pace with their knowledge of these systems.
In fact, during time, the whole Barrier became more and more dependent on outside (expert) knowledge. The other question of 'proving the proof' after each update became more urgent, as the internal reports have shown. As one of the system managers stated during an internal security review: '*I feel like a tourist on my own system*[9]*'*. Such a visitor's role perception raises questions about identification and management of critical strategic control capabilities and information supply.

3.2.6 We don't know what we don't know[10]

As the Dutch National Institute for Public Health and the Environment has shown[11], the Stirling model[12] can be modified into the following scheme classifying risk along two axes:

Knowledge about likelihood	Knowledge about effects: High	Knowledge about effects: Low
High	Conventional design: Quantitative Risk Analyses (QRA) Data uncertainty	Technological design: Simulation / Modelling Method uncertainty
Low	Multi-actor decision-making: Fuzzy Logic / What-If analysis Decision-making uncertainty	Precaution: Citadel approach / Scenario analysis Scenario uncertainty

Figure 12. Positioning of various risk analysis methodologies (Beukenkamp)

During the design phase of the Maeslant Barrier it was assumed that most if not all the key aspects of the design where either known or predictable, justifying a design based on the QRA approach. Since then, the actual behaviour of the system moved away from the left upper quadrant, at first towards the left lower quadrant, later on moving further to the right.
At present, a situation has arisen where it can be stated that we don't know exactly what the uncertainties and hidden problems are regarding the command and control of the Barrier system. In other words: we don't know what we don't know[13]. This justifies a more defensive, precautionary approach as Beukenkamp et al[14] have indicated. The reaction of the deputy-minister of Transport, Public Works and Water Management underlines this analysis.
The whole problem with the Barrier can be summed up as follows: the decision support system BOS is not the boss anymore and the control system BES is not always in control while BOS and BES are sometimes out of tune. The 'unreliable' human being is brought back in the operation to guard the guardians (i.e. to improve reliability!). In this case, the crucial factor regarding criticality is focused around knowledge and presumptions in the controllability of the actual modus operandi. Knowledge of the way the various systems functions, knowledge of known and unknown deficiencies, knowledge of the proven reliability and so on. What can be done in future to prevent such a situation to reoccur? This will be explained in the next paragraph of this paper.

3.2.7 Unravelling criticality

Like mentioned before the design of the Maeslant Barrier is purely based on the QRA approach. This means that all the information required for proving its reliability was either presumed or known. However, the presumptions introduced data uncertainty in proving the reliability of the system. For example the speed at which software has developed was unforeseen at the time of design and construction of the Maeslant Barrier. Because of the frequent new software releases the operating envelope of the system changed which affected its reliability.
The current problems with the Maeslant Barrier show that it is important to identify uncertainties. Because of the data uncertainty the probabilistic approach should be complemented with techniques such as a deterministic scenario analysis (figure 12). With this analysis, the nature of uncertainty moves from data uncertainty to scenario uncertainty.
Since the beginning of this century the relevance of a deterministic scenario analysis as an additional decision-making support tool towards QRA is more and more being recognized:

- In 2003, the National Institute for Public Health and the Environment developed a risk policy-making strategy Coping rationally with risks[15]' that focuses on the layered structure in decision-making and the position of different types of risk analyses, including a deterministic scenario analysis, in decision-making.
- Simultaneously, the Ministry of Transport, Public Works and Water Management, the Ministry of the Interior and Kingdom Relation, and the Ministry of Housing, Spatial Planning and the Environment developed a policy document concerning tunnel safety[16]. This policy document focuses on a methodology containing probabilistic risk analyses as well as a deterministic scenario analysis to gain insight into the safety performance of a tunnel.
- In 2004, the Parliamentary Inquiry Committee Duivesteijn[17] identified several phases of policy decision-making processes with deficiencies in risk assessment procedures. New policy-making support procedures and notions for multi-level decision-making are needed, because of the multi-actor context.
- Finally, a scenario analysis is essentially a multi-actor decision support tool combining frequentist information with scenario information providing a quantitative and narrative picture of the sequence of events[18].

3.2.8 Scenario analysis

In contrast with a probabilistic approach, a deterministic scenario analysis is not aimed at calculating the risk (reliability) to establish if a system meets the safety performance level. A deterministic scenario analysis is focused at the evaluation of system safety. In a deterministic scenario analysis, accident scenarios are designed to identify crucial factors and possible safety bottlenecks in a system. The accident scenarios describe accident processes of potential or actual sequences of events in time, in a specific context and operating environment.
A deterministic scenario analysis can be applied at three different moments of the design and construction process[19]:

- In the conceptual design phase, in which design alternatives are based on a Program of Requirements, shared by all actors and encompassing all relevant design aspects.
- In the functional design phase, in which a limited set of most preferable alternatives is selected for further elaboration and detailing.
- In the detailing phase, in which the construction details and safety measures of the final alternative are elaborated into a construction-planning phase.

However, a deterministic scenario analysis is most valuable in an iterative process of adjustment and improvement through the three phases of the design and construction process.
These accident scenarios can be designed in two different ways:

- Top down (a prospective way of designing scenarios), which means that the scenarios are derived from a decomposition of the system. Already at the time of design, engineers have insight into the structure and the content of the system and can define intended and foreseen complexity, interactions and interfaces. At that time the accident scenarios can be used as a conceptual design tool to remove hidden deficiencies before they lead to accidents. These scenarios can be characterised as a 'technical construct'.
- Bottom up (a retrospective way of designing scenarios), which means that the scenarios are derived from accident analyses of existing analogous systems. During these analyses, learning from proven deficiencies in order to prevent their recurrence becomes possible. These scenarios can be characterised as a 'technical reconstruct'.

In case of the Maeslant Barrier, a deterministic scenario analysis could have identified knowledge as a crucial factor, as was indicated by the internal investigation into the operational problems of this Barrier, later appearing in the newspapers[20]. In this case, possibilities to prevent knowledge from becoming a safety bottleneck could and should have been researched.

3.2.9 Conclusion

It is of utmost importance that safety-critical systems show predictable and controllable behaviour in particular when they are complex, dynamic, technologically sophisticated and unique/innovative. Failure of this notion can create conditions for which these systems have been designed to prevent. The case of the Maeslant Barrier shows that an in itself innovative design can be hampered by life-cycle instabilities. Especially when a design is a pure probabilistic one, it is crucial to keep on ascertaining during its life span whether the system still answers to the original specifications of reliability, in other words: proving the proof.
If it is clear that the conditions no longer satisfy a QRA approach, a more precautionary one is justified. Scenario analysis can be an important tool to determine where the hidden problems of a system are located. In the case of the Maeslant Barrier using scenarios could have identified knowledge deficiencies as a crucial factor.

3.2.10 Epilogue

This article could give the impression that the design of the Maeslant Barrier was a major failure and a waste of money. The actual course of identifying and analyzing deficiencies in the Barrier's design demonstrates a discrepancy between factual technical diagnosis of the design and public perception of a potential catastrophic failure. This discrepancy resulted in the necessity to perform a complete systems test in practice at least once a year.
Without these problems, economical pressure from the Port of Rotterdam could have prevented such tests to be carried out. Each time the Barrier was tested it worked. The only times it had to close in anger it did its job very well. And last but not least special software has become available to test the reliability of the command and control software, thus reducing the uncertainty about its performance and reliability.
The Maeslant Barrier is still an engineering masterpiece without equal anywhere in the world, consisting of two horizontally moving Eiffel towers (but four times more heavy). On the other hand, the scale of operation makes it also a laboratory for extreme engineering, which we can use to learn. That is exactly what Petroski[21] meant when he wrote his book 'To engineer is human: the role of failure in successful design'.
The design of the Maeslant Barrier is still successful and serves as an example to the rest of the world despite its failures, simply because in practice it is doing the job as it was designed for. After all, each investigated failure was an opportunity to further improve this and similar systems.

3.3 Ageing in transport systems as a hidden danger

3.3.1 Ageing: natural process with hidden dangers

Ageing starts when a system is handed over to its users. This natural process creates hidden dangers, which are usually not very high on the political agenda. The main reason is that ageing problems only start to show in the long term, after ten years or more, whereas most political views are usually far shorter than this. These threats are nevertheless very real as Methorst has shown[22]. Ageing of people imposes different operating requirements and quality demands on transport systems. Ignoring this aspect creates a possible threat to society, e.g. counter effecting the present improvements in road-safety.
The ageing problem is not limited to human beings. Beukenkamp[23] has shown that technical systems suffer from ageing problems as well. The lifespan of systems is improving continuously, but this does not apply to all its parts. Therefore deviations from the original design start to occur very soon after its first implementation. These deviations are the result of difficulties in maintenance and uncertainties about the true nature of the behaviour of these systems. Using the Pizza-model as developed by AVV-Transport research Centre[24] the long term threat of ageing regarding transport systems can be shown.

3.3.2 Context of rational policy process

A rational policy approach starts with the identification of a problem that needs to be tackled: an unacceptable number of accidents, a negative trend, rising societal costs. The first thing that needs to be done after that diagnose is to identify causal factors, like ageing of the population, growth of traffic and goods transport, expiration of the design envelope, faulty management.
Based on that assessment policy decisions regarding objectives have to be made and solutions for dealing with the identified causal factors and a policy program must be developed. The Pizza model can help checking whether all angles and reasonable options were included.

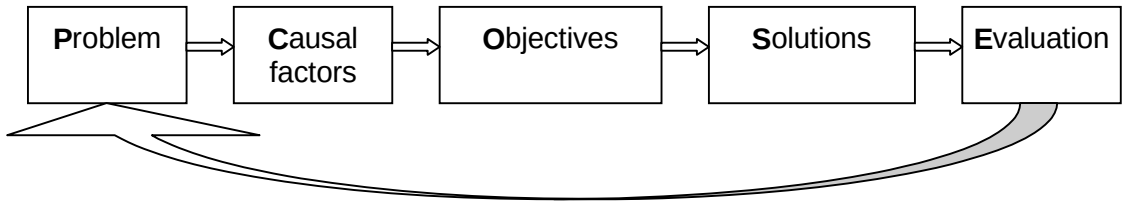

Figure 13: rational policy process

3.3.3 Ageing of transportation systems

Ageing regarding transport systems is a widespread and at the same time underestimated problem as the next paragraphs show. The examples given are typical for the range of technical problems that ageing causes in transport systems and the effect it has on the people involved, operators, their management and the users (public at large). In this paragraph several cases will be used to show how the problem of ageing of transportation systems should be addressed already in the first phases of the design and decision-making regarding these systems.

3.3.4 Geriatrics

For a long time ageing was not a clear problem in transport systems. Either it was not too difficult to detect the effects of ageing and repair them (like cracks in frames of 50 year old locomotives or bridge structures) or they didn't occur because the economical lifespan was far less than the technical lifespan, the vehicles being scrapped before they became unsafe. Nevertheless, the problem was there, waiting to strike.

The airline industry became aware of this when in April 1988 a Boeing 737-200 of Aloha Airlines with many flight cycles suffered a partial in-flight failure of the main fuselage (figure 14). The following investigation revealed simultaneous presence of small cracks at multiple rivet locations of a disbanded lap-joint, known as widespread fatigue damage (WFD). This incident raised serious concerns about the structural integrity of 'geriatrics', aircraft with a high number of flight cycles (in contrast to aircraft with many flying hours).

Figure 14: Aloha Airlines Boeing 737-200 after fatigue failure of the main fuselage, 1988

Why did it take till 1988 before this problem became acute? The main reason was that until that time aircraft were economically outdated well before they were technically life expired. Most of the modern prop liners of the 50's were scrapped only ten years later. However, in the 60's designs were introduced which were lasting, such as the Boeing and Douglas jetliners, the Fokkers and the Airbus family.
Many aircraft were sold on to smaller carriers after they were taken off the main routes. Some of them were given other duties, such as cargo planes. At present there are hundreds of civil airliners flying around which are more than 30 years old, not only in third world countries, but in some western countries as well. The fleet of former Eastern Bloc cargo planes is notorious for its poor condition, yet this is no exception and not limited to second and third world countries as the Aloha incident showes[25].

3.3.5 Ageing of knowledge

For a long time mechanical and civil engineers had limited possibilities for strength and stress calculations. Therefore they needed large safety margins to cope with these uncertainties. E.g. in the Netherlands the initial safety margin for reinforced concrete constructions was 1.7 after 28 days, resulting in a factor 2 or more after 20 years due to the continuous crystallization process in the concrete matrix.
The introduction of advanced computer analysis software such as based on finite element design methods in combination with powerful microprocessors, made it possible to increase the accuracy of designs to such an extent, that safety margins could be reduced considerably, sometimes to 1.2 or even 1.1. The economic gain resulting from this is immense.
It creates a danger as well. These modern design techniques require comprehensive insight in determining scenarios, such as expected loadings and loading conditions. However, a lot of the outside world is still not fully understood. Fortunately, with hindsight, in many cases it can be stated that the engineers were too pessimistic.
For example the Haringvliet Barrier south of Rotterdam was designed to withstand a wave front 200 m wide, whereas in reality the width of these waves never exceeds 80 m. Unfortunately there are also cases where the real world conditions are underestimated, creating hidden dangers when this outdated knowledge keeps on being used without verification.
The Estonia disaster in the Baltic[26] in 1994 (figure 15) is an example of an accident resulting from hidden ageing of design knowledge. The ship was originally designed for operation in the Baltic, but as it turned out after the tragic accident, the official design loads for operation in that area were not in accordance with the true loads that could occur. There had been other ships that suffered from partial failure of bow doors, designed according to the same design loads. Each time a bow door failure occurred it was attributed to poor craftsmanship of the shipyards that had built and repaired the ships. As a consequence each time the shipyard in question kept its problems to itself.
It was not until after the disaster that it turned out that the design specifications were outdated because of lack of knowledge of wave behaviour[27]. The knowledge of the behaviour of the real system had aged, with neither the design and maintenance engineers nor the management of the company, the crew of the stricken ship or the inspectors being aware of this.

Figure 15: Upturned Estonia, 1994.

3.3.6 Ageing of experience

There is another problem relating to the previous mentioned development of modern design methods as well. Sometimes older designs are more robust than present designs, because they are over engineered. In modern designs there is an increasing tendency to eliminate secondary carriageways, making them more susceptible to sudden and progressive collapse. Lessons from the past are more and more forgotten[28] (ageing of experience).

A good example can be found in the design of modern railway coaches. Their design loads have not changed much since WWII. What has changed is their failure characteristic. A traditional coach was a body shell placed on a solid under frame. When loaded to their extremes such as resulting from serious collisions, the frame takes the brunt and buckles, usually a couple of meters from the end, leaving the centre part intact.

Modern coaches are for part self-carrying constructions, whereby the body shell plays an integral part in the strength and stiffness of the carriage. Recent railway accidents in the UK[29], Germany[30] and the Netherlands[31] (figure 16) show a dangerous tendency of coach failure, whereby the entire passenger compartment fails, because the end balconies are no longer capable of absorbing the energy of the collision and function as a crumple zone. This is all the more remarkable where in the automotive industry the opposite development took place, whereby cage constructions were introduced to protect the passengers in case of serious collisions.

This design attitude can only be explained by the fact that unlike the automotive and airline industries the railway industry does not test their products under extreme conditions (test to failure, life cycle tests, collision tests et cetera). Sometimes (though fortunately very infrequently) the proof of the pudding comes only in the eating after 20 years or more, when a real time test takes place, this time with real casualties instead of dummies.

Figure 16: Low speed collision (<40 km/h) with serious consequences, because the coach broke its back; Amsterdam CS, 2004

3.3.7 Ageing of the design envelope

Additionally history of technical systems shows that in many cases the use of a system develops during its lifespan. What happens is that the operating envelope of the system starts to fill the design envelope and at some point in its history exceeds it. That's the moment a system becomes inherently instable and thereby dangerous, usually without the operators being aware of this situation, let alone the passengers or users.

The Y2K problem brought this to a highlight. Many computer systems designed in the seventies and eighties were still running by the end of the century. When originally designed, nobody had expected these systems to live so long. Therefore no provision was made for a date after the last second of the 20th century. In other words: their design envelope finished at the end of the 20th century. And now these systems were expected to continue to operate well beyond that date.

Because of all the upgrades during their lifespan it took an immense amount of work to relearn the true characteristics of each of these systems, in order to establish the best way of dealing with this problem. Such a process is known as reverse engineering: redrawing the designs according to how it was actually build, sometimes decades ago. Other systems were so complex that there was no other option left than wait and see and hoping for the best. It resulted in a worldwide scare, followed by crash actions to counter the possible effects, which in cost terms far outstretched recent damage by terrorism[32].

3.3.8 Ageing of tight coupled complex systems

Ageing is also proving to be an upcoming operational and maintenance problem in ICT command and control systems. The lifespan of ICT system generations is sometimes very short, usually only a couple of years. That means that during its entire lifespan a technical platform encounters many updates and at least two or three upgrades of its control systems. All these updates and upgrades introduce additional functionalities, some known and others hidden. They make the system more complex and, without being realised by the operator, quite often more tightly coupled according to Perrow[33].

At the same time management processes are not adapted to these changes. Maintenance is in many cases still being done the way it was done ten years before. Improvements in reliability are used to cut on maintenance costs. Comprehensive testing of parts and systems is increasingly being skipped, because of economic pressure and overconfidence in the reliability of new technology, or because it is not possible anymore to do such a comprehensive test within a reasonable time span of a couple of days. Indeed it is accepted practice that modern software contains hundreds of errors, some of them fatal, which only show during long term testing if at all. The service packs of Windows are examples of the continuous repairs necessary to improve the reliability of these systems but certainly not exceptional ones.

At the same time as the systems become more complex and dependent on computer technology, the operator or user becomes older. He/she is having difficulties keeping pace with all the frequent changes. User manuals are outdated within months. Computers reducing the role of the operator to overseer, do more and more primary control. Is the operator/overseer really in overall control or in reality reduced to a butler status?

As pointed out in chapter 3.2 a case like the Maeslant Barrier shows the latter to be true, when the main supervisor of the Barrier stated that he felt like a tourist on his own object. His knowledge of the system had aged considerably. At the same time there was an increase in complexity of the command and control systems. The outcome was that after ten years in service the reliability of the entire system had been reduced to an alarming level, without the operators being aware of this.

Significant was that the best way to increase its reliability was to bring the human operator back into the primary processes of the system, thereby going against one of the original design fundamentals, eliminating the human operator on grounds of lack of reliability.

3.3.9 Ageing of fleets

Another ageing problem is the paradox that more reliability could lead to less safety! The automotive industry suffers from this phenomenon. What happens is that in the old days the technical lifespan of motorcars was reasonably short. When it was necessary to introduce new safety measures such as seat belts, after ten years most of the fleet was equipped with such a device, because most if not all of the non-fitted cars had been scrapped.

Nowadays, cars are much more lasting. In the Netherlands at present 53% of passenger cars is older than 6 years, 2.4% (1 in 40) dating from before 1995[34]. The average age of passenger cars has increased from 7.2 years in 2000 to 11 years in 2012[35]. The consequence of this is that it takes much longer to introduce widespread safety devices such as second generation airbags, automatic braking systems and so on. Though the technical development of safety devices is sometimes very rapid, market response is increasingly slower because of ageing of the fleet in general.

From the user point of view this development is worrying. Often young drivers buy older cars. Their inexperience and behaviour makes them more susceptible to accidents[36]. And now because they drive older cars they are no longer sufficiently protected by modern safety devices. This is an example where as a result of ageing reliability contravened safety.

3.3.10 Ageing of rules and regulations

A final example of ageing having a negative effect on the functioning of transport systems is the matter of rules and regulations. It takes many years, sometimes 5 or more, before laws and bylaws are implemented regarding the safeguarding of transport systems and the like. In many cases present rules and regulations are geriatric, such as railway acts which sometimes date from the steam age[37].

Care must be taken though when new rules and regulations are proposed to formulate them in such a way that they do not stifle new developments, aimed at further improvement. On the other hand in some cases rapid (technical) developments can be noticed, which could have adverse effects on safety[38]. It is therefore a given fact that rules and regulations are always at least one step behind the actual state of the transport world. Sometimes rules and regulations are already obsolete by the time they are introduced. This puts a heavy burden on the ethics of designers such as engineers, because these rules and regulations do not give 100% protection to the future users of their new designs.

3.4 Finding solutions using the Pizza-model

To show how the Pizza model works solving problems like arising from ageing of part of its complexity, the example is used of the coach behaviour during the train crash at Amsterdam Central[39]. The problem originates from the inner circle in the right upper quadrant (the transportation quadrant), as could be concluded from the official reports[40]. Does this suggest that the solution can and must be found there as well?

The traditional way of thinking would be to look at the design of the coach itself and adjust the design parameters if necessary. Not only does this limit the perspective of the problem to one quadrant, it goes further by reducing the possibilities for a solution to one shell within that quadrant. In fact, quite often forensic investigation looks primarily for the explaining variables, ignoring the importance of the steering variables. In many cases the adage of ‘pilot error’ or ‘driver error’ is much too short-sighted to really explain what caused to accident and better: how to prevent it effectively and efficiently[41].

Using the Pizza-model a different perspective comes forward. First of all the influence of the spatial quadrant is taken into account. Amsterdam is a very compact major conurbation with large passenger traffic flows. Because of congestion on the roads the railways play a very substantial part in commuter traffic, which is equal to the use of cars (35%). Most of this rail commuter traffic converges on Amsterdam Central Station, because that is also the main hub for the local tram and metro network. As a result Amsterdam Central has to cope with a massive traffic flow in short time, separating various trains only by minutes. This creates a narrow window of safety when looking at the time scale. A minimal delay of one train creates havoc in the automatic system of track allocation, as was determined to be one of the underlying causes of this accident[42].

The second problem that played a major part in this case is the partial failure of the automatic train protection system ATB. For various design reasons ATB does not intervene when a signal is passed at danger at low speeds (<40 km/h), a known problem since it was developed in the last century but at the time accepted on grounds of envisaged limited risk and high costs to fix this hiatus.

Therefore ATB could not prevent the rogue train in question from going through a signal at danger (Signal Passed At Danger = SPAD). This defect of ATB was an underlying factor in several other recent low speed collisions as well[43]. Eventually ATB was improved to close the 40 km/h gap, resulting in ATB-Vv (Vv meaning ‘Verbeterde versie’ or improved version). This became operational from 2008 on, although it is still not fully implemented (2016).

A third problem arose from the physical environment. Many years before this accident during the modernization of the signalling at Amsterdam Central, signal 278 was positioned in such a way that its visibility was poor. During the years through training most of the drivers became aware of this problem (design error) and learned to deal with it. In fact the recognition of the danger as such aged, because it was well known and in practice didn't cause any serious problem like a great number of SPADS[44]. It wasn't until a new recently trained driver (who was not yet told of this hidden danger) entered the scene, that the hidden danger became a real one[45].

This clearly shows where the most obvious solutions to the problem of weaknesses in the design of railway coaches lies. Railway coaches are not designed to sufficiently withstand crashes with other trains, for the simple reason that the general policy is that railway crashes are unacceptable and therefore should not happen. This implies that the signaling system should be properly designed, the railway staff must be well trained and that safety systems such as automatic train protection should do their job properly as a second line of defence. But each and all of them fail from time to time. The last line of defence in these cases could very well be the strength of the coach body.

The other weakness is the separation in time of conflicting train movements. The track allocation should be such that the automatic allocation system takes into account the fact that trains can be delayed. A rule existed already that at busy junctions conflicting train paths should be separated by at least 5 minutes. This rule was not implemented in the automated track allocation system of Amsterdam Central, one of the busiest hubs in the Netherlands.

Nevertheless accidents in situations like Amsterdam Central can always happen, even if the signaling system is designed as it should and works properly. Material defects such as axle fracture or rail fracture can never be excluded, although thorough inspection programs could minimize these risks as well[46]. In congested areas such as Amsterdam the effect could be that as train derails and comes into the path of an oncoming train, the latter is already to close by to stop in time. A (semi-)frontal collision is inevitable under these conditions (right lower quadrant of the Pizza-model). Therefore again the strength of the coach is the last line of defence.

It can be justified that to absorb the crash-energy, not only could part of the body shell crumple, it should crumple as long as the main body (the central passenger compartment) remains intact. This is all right for coaches that have small end balconies, not designed for standing passengers but only for getting in and out of the train, such as to be found on long distance stock. Modern commuter stock however has either large end balconies[47], designed as a standing space for commuter traffic or balconies not separated from the main passenger compartment[48], making the passengers extra vulnerable (right upper quadrant of the Pizza-model: vehicle and concepts) because the whole coach is one large open space.

Perhaps the answer lies in different load specifications for coaches with and without a crumple zone, instead of the present uniform design requirements (left lower quadrant of the Pizza model: norms in relation with both right-hand quadrants, to protect the traveler in the left upper quadrant and give him/her a safe feeling). The interregional double deck train of the VIRM type, introduced by Dutch railways (NSR) from 1994 on, is a good example of a crash worthy design, as shown in the following picture of the front section of a VIRM multiple unit, which hit a fully loaded lorry at a speed of 130 km/h near Wijhe in 2005[49]. None on board the train were killed or seriously injured.

Figure 17: Collision between a Dutch Railways VIRM type electric multiple unit and a 40 ton loaded lorry, November 3, 2005. Although the damage to the train was severe, its resilient design prevented fatalities in the train.

3.5 Precaution: buying time with the Citadel approach

The terrorist attacks shortly before and during 9/11 made it clear that a different thinking was required when dealing with unpredictable risks. In 2002 when working at AVV/Transport Research Centre the author first developed what later became known as the Citadel Approach. At the time it was simply impossible protecting every vital object in the Netherlands without bringing the economy to a standstill. Later on this same approach was used when dealing with other accidents with difficult to predict consequences.

3.5.1 Trouble in transport

On July 15, 2003 a lorry collided with a viaduct pillar on one of our most busy motorways near the town of Eindhoven at a major junction. The accident itself was not unusual except that the trailer was carrying 18 tons of liquefied Isobutylene gas. In the immediate aftermath of this crash, the truck went on fire with a possibility of a hot BLEVE[50]. The damage would have been enormous, potentially as catastrophic as the Enschedé fireworks disaster of May 2000. The accident resulted in a major disruption of an important part of the national motorway system (figure 18), the A2 corridor. Also, nearby offices had to be evacuated, increasing the societal disruption.

Figure 18. Burning Isobutylene gas tanker near Eindhoven, July 2003. Photo: Telegraaf Newspaper

Each day thousands of tons of LPG (liquefied petroleum gas) are being carried over the Dutch motorway system. Yet nothing serious has gone wrong since it was first introduced as motor fuel some 40 years ago. Anybody can imagine what a terrorist can do with 40 tons of LPG. At present, none of these road shipments are under special surveillance. They operate under a hazardous goods licence, but they do not require police escort, previous announcements and so on.
Another complication is the need to increase multiple use of land-space, including building over motorways. The Netherlands is a very densely populated country where space is at a premium. Recent developments indicate a growing tendency to build over infrastructures, in particular in and around the major conurbations. This would bring additional potential victims within reach of terrorists using the transport systems. The situation in Amsterdam (figure 19) shows this all too clearly.

Figure 19. Multiple use of land space in relation to transportation of hazardous materials

These examples show the Dutch infrastructure to be a tight-coupled complex system in accordance with Perrow[51]. In the aftermath of 9-11 AVV/Transport Research Centre published a quick scan regarding the vulnerability to terrorism of the Dutch transport Infrastructure[52]. The methodology used in this quick-scan was to focus on those parts of the transport system where a progressive collapse on a national scale could occur.

This strategy coupled vulnerabilities to inherent properties of the system itself and dependencies on other systems. In this way, the methodology used was a further development of earlier research[53].
The basic idea was that in security matters risk as a probabilistic function couldn't be calculated. Only the terrorist himself or herself knows for certain where and when an attack is going to take place. A transformation can be made whereby the objective notion of risk is replaced by the subjective notion of threat, see §3.5.2. The threat is dependent on the objectives of terrorists on the one side (is the Netherlands attracting attention of terrorists?) and vulnerabilities of possible targets on the other:

- Where can maximum damage and/or casualties be inflicted?
- How predictable is this effect?
- Is containment and quick recovery possible?
- Does it develop over a short or longer time span?
- If the system collapses, is this a controlled or controllable collapse or not?

Since an inherent property of a catastrophe is that the accompanying scenarios are highly unlikely, resulting in society not being prepared for it, research should be done into exactly these scenarios, the Titanic scenarios.

3.5.2 From risk to threat

The classic approach to safety and security is the standard formula:

$$R_{Sc} = \sum P_{Sc,\,i} \times E_{Sc,i} \quad [1]$$

R_{Sc} is the calculated risk given a scenario, P_{Sc} the probability of an event given that scenario and E_{Sc} the effect of it. The problem is that the formula [1] is incomprehensible for non-experts, like ordinary citizens and politicians. For example under Dutch law coastal defences must be able to withstand a storm surge that can occur once every 10,000 years. But what does this mean? The layman will translate this into 'over 10,000 years'. Yet there is a probability perhaps remote and looking negligible that disaster can strike tomorrow. And what is the actual range of once per 10,000 years? Is it really somewhere between once per 9,900 years and once per 10,100 years, or is it given the inevitable uncertainties more likely to be in the range of once per 5,000 years and once per 15,000 years? It gets even worse when dealing with terrorism, because the probability of an attack is unknown to all except the terrorists themselves.
Adapting the original formula can make a translation to something more comprehensible to uninitiated. If 'probability of a scenario' is replaced by 'threat due to a scenario', the risk formula becomes:

$$R_{Sc} = \sum T_{Sc,i} \times E_{cm,Sc,i} \quad [2]$$

Risk given a scenario (R_{Sc}) is the experienced threat of such a scenario (T_{Sc}) times the credible maximum effect ($E_{cm,Sc}$) of it. This formula [2] is capable of explaining the attitude of society and its population towards various risks, but also the way of thinking of terrorists and other criminals. As such it is a worst-case analysis for rare events which lack sufficient casuistic evidence. This requires a different approach from frequent events.
What is needed is a more objective approach to risks that are at present dictated by subjective perceptions. In other words: in the George dilemma policymaking should move as much as possible towards analytical correctness. Instead what we can observe is that during a crisis perception of the problems gets separated from system characteristics, thereby moving the George dilemma away from this analytical correctness.

One warning must be given. When dealing with the 'low probability, large effect risk' in the opinion of the public (usually lay people) experts tend to underestimate these risks. The nuclear industry is a classic example of this. On the other hand: experts are sometimes accusing the public of overestimating such risks. Public actions against rail transport of Chlorine in the Netherlands are an example of this. Be careful though when overestimating the knowledge of experts and at the same time underestimating the knowledge of lay people. Not the probability of an occurrence but the characteristics of the system should be central in these discussions.

3.5.3 The George dilemma

As mentioned in §2.3 in 1980 George[54] studied the decision-making processes of US-presidents in foreign policies. He noticed a dilemma that occurred repeatedly and has since been known as the George dilemma (see figure 20). This dilemma occurs in situations of decision making when there is a time constraint. One way or another the person or persons involved in (policy) decision making experience a sense of urgency.
There is an internal or external pressure on them to do something, yet the problem is what to do? There is no time for analytical correctness (knowledge based) although the problem is far from clear. There is no time to implement a strategy that avoids unnecessary damage. In fact collateral damage is seen as inevitable (political acceptability).

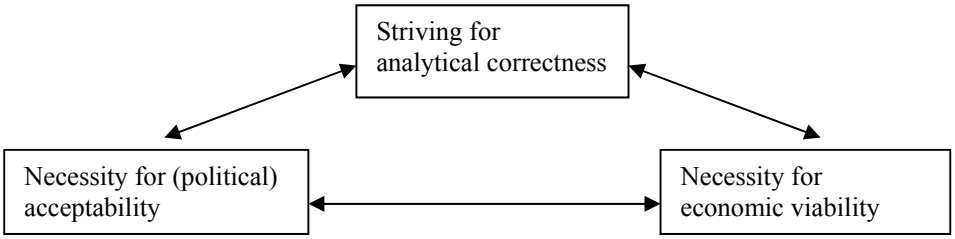

Figure 20. Decision-making dilemmas according to George

Applying the George dilemma[55] it is not too difficult to understand why it is almost impossible for a country like the Netherlands to protect its entire infrastructure (belt defence). It would either lead to a police state, where fundamental constitutional rights such as the freedom of opinion, religion and political parties are no longer valid, yet it would still be vulnerable to security threats like terrorism. Or such a policy would outstretch police and defence budgets, thereby crippling the Dutch economy. It would also be detrimental to our economy in another way, because it would hamper the free flow of traffic to and from our trading partners. Added to this a belt defence still requires a second line of defence to stop inevitable leaks, further increasing the costs of such a system.
In the George dilemma this would implicate a policy that is moving towards political acceptability (satisfying the electorate) for the short term, ignoring longer-term consequences (analytical correctness and/or economic viability). The Citadel principle helps the policymakers to study the system as a whole above the level of individual components, thereby showing a way-out of the George dilemma.

3.5.4 Citadel principle

It was the aftermath of the 9/11 terrorist attacks in the USA that created a mental shift in the Netherlands and elsewhere regarding the protection of risk sensitive systems. Especially in the Netherlands risk management based on quantitative risk assessment techniques had become the dominating policy. At the same time it created vulnerabilities because QRA's failed to answer the predictability question (when will it fail) and the consequence question (what if the unwanted event occurs).
In a way a QRA can be somewhat fatalistic in its approach. The probability of an unwanted event to happen is small, yet sooner or later it can happen and that has to be accepted by society. There are risks that are apparently not acceptable to society never mind the low probability of occurring. If that is the case what can we do about it? Is it possible to at least contain the problem if disaster strikes, thus reinforcing a QRA or other risk management policies?
An alternative approach is possible as Beukenkamp has shown[56] and put into practice several times. This is called the 'Citadel principle', based on fundamental decisions and assumptions at a strategic level (design phase, macro scale) in the DCP-diagram. These fundamental decisions and assumptions are:

1. Assumption: we don't have enough resources to secure every part of our transport system.
2. Decision: we can only allocate a limited amount of resources to the protection of our transport system.
3. Decision: we accept partial failure of the transport system; therefore we must be prepared for such a failure and the damage and casualties resulting from it.
4. Decision: apply design principles regarding graceful degradation and prevention of a progressive collapse.

Military systems show us the way a design can be made more resilient without introducing extravagant preventive measures. Battleships were specifically built for their job. They were able to give a punch and they could also survive several hits, at least that was the theory[57].

The **first step** in the evolution of their design was that ship designers in those days realised it would be impossible to protect the whole ship. It would sink upon launching under the added weight of the armour needed. Instead armour was concentrated along the most vulnerable and valuable parts of the ship, thereby creating a very strong **citadel** around the magazines, main armament, engine rooms and control towers, leaving the rest of the ship virtually unprotected.

The **second design step** was to subdivide the ship into a maze of watertight compartments. The armoured citadel in itself was a floating raft, capable of keeping the rest of the ship afloat if necessary. Flooding and counter flooding could safeguard a damaged ship against capsizing.

The **third design step** was that there was as much redundancy in the fighting system as possible. Every vital function could be operated from at least two places in the ship to ascertain graceful degradation and an operational fighting platform to the end. The outcome of this was a ship that sometimes could withstand a formidable punishment without sinking[58]. Already in those far of days communication nodes in the fire control and ships control network could be bypassed[59]. A lesson that quite often has been forgotten since (unravelling of the network).

The citadel principle is therefore characterised as follows:

1. Resources are primarily concentrated where failure is unacceptable;
2. The system is designed for graceful degradation, thus buying time to reconfigure the system and organise recovery;
3. The organisation around a risk-sensitive system is well equipped to assist in successful recovery after an accident or failure.

Time is important because in these situations there is a combination of a degradation process followed by a recovery process. The quicker the degradation process develops the more difficult it will be to stop it and turn the situation around into a recovery process. Any recovery process needs time to get organised and activated.

3.5.5 Methodology

Beukenkamp[60] applied this philosophy to the Dutch infrastructure:

1. Identify the systems of our national economy that are vital to our country.
2. Identify the infrastructure that is related to these systems.

Create the Citadel:

3. Identify the vital parts within these infrastructures, i.e. the parts that are crucial and must not be knocked out at any cost (the vital, strategic nodes). Focus on pro-action, prevention, preparation and repression.
4. Identify those parts of the infrastructure that in itself are not strategically important, yet where a progressive collapse could occur, resulting in failures of strategic parts of the system, i.e. a multiplier effect (the tactical nodes). Focus on pro-action, prevention, preparation and repression.
5. Accept that everything else is vulnerable and not vital: focus only on preparation and repression.

In step 3, targets are identified. In step 4 weapons at systems level are identified, where a multiplier effect could be used to create more havoc than initially inflicted. Everywhere else, the system must be able to survive a terrorist attack without specific advance protection other than the usual protection against everyday problems. In the Netherlands, the ‘acceptable’ amount of casualties has been established as being equal to the order of the annual number of victims in road traffic (2015: 621).

One must be careful though. Recent serious accidents in the Netherlands (Amsterdam air crash 1992, 43 casualties; Volendam pub fire 2000, 14 casualties; Enschedé fireworks disaster 2001, 23 casualties; Amsterdam Airport Detention Centre fire 2005, 11 casualties) have shown that a relative low amount of casualties can result in serious public criticism and political turmoil. Additionally normal contingency planning like quick response agreements with fire brigades, salvage contractors and the Corps of Royal Engineers of the army should deal with any catastrophe in these places.

3.5.6 Forward versus rearward defence

The Citadel principle does not mean we concentrate all our defences on specific objects. We concentrate our resources at the mission/task orientation from object to process. Defence can be both forward and rearward. An example of a forward defence is the airline industry. Naturally, it makes sense to armour cockpit doors (there are also arguments against it[61] as is shown by the German Wings air disaster[62]), but this is a last resort.

Best defence is to make sure nothing improper gets on board. This requires a forward defence on the ground. At airport level again the defence can be forward and rearward. Security checks at the gate are an example of a rearward defence. An integrated filter whereby a passenger is checked at the border control is an example of the former.
There are other examples where a rearward defence is necessary, because it is the only option left if you have more or less open borders and an open society. Control centres are strategic objects and therefore need good security and safety systems at centre level. Otherwise not only a terrorist attack but also an overheated cooling unit can destroy it, thereby immobilising the system it controls.
Such a defence can comprise of back-up units, subdivisions, manual backup operation facilities and so on. Crucial determining parameters to what is necessary are (similar to the process industry): mean time between failures (MTBF) and maximum allowed down time (MADT).

3.6 Critical infrastructures: quick results

The Citadel principle when applied to Dutch transport infrastructures, reduced the list of possible vital objects from 120 to less than 20. However, the other 100 are not ignored, they have been given a lower priority. At present, main attention is focussed on the short list. When time and resources become available, the other objects will be re-examined.
Recently the Ministry of Transport (MoT) has determined that neither the Dutch railway system as such nor most of the motorway system is considered to be vital, the former because at national level its role in transport is limited[63], the latter because the network as a whole is important, but it has a lot of redundancy (dense network).
Furthermore, the MoT has established that there are nodes in these systems that are vital, either because of the earlier mentioned multiplier effect or because of the concentration of people (soft targets). The inland waterway system is considered to be vital, not from the transportation point of view, but because it plays a role in the drainage of the lower areas[64].
Problem is that all these systems depend on other infrastructures not under the control of the MoT, like the energy grid and the ICT network which are the responsibility of the Ministry of Economic Affairs.
The Dutch government has appointed a national security coordinator to make sure that this multiform security arena does not turn into an unworkable swamp. If organisation and coordination are fundamental in the way a system operates, then policymaking must pay attention to these items. They are the cement between the stones, binding the system and its objects together.

3.6.1 Putting the Citadel principle into perspective

The Citadel principle does not replace other risk analysis methodologies; it is complementary to them as shown in figure 21:

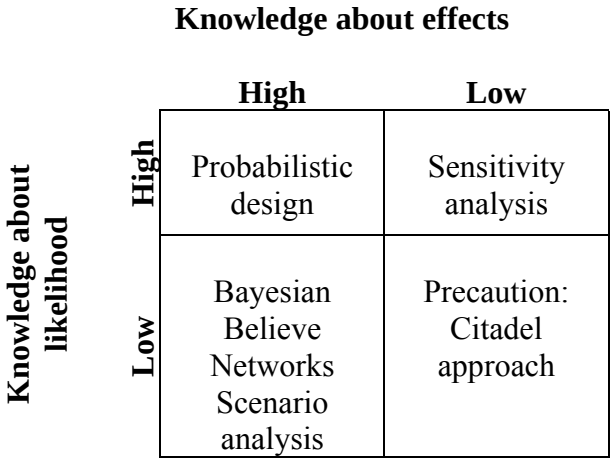

Figure 21. Positioning of various risk analysis methodologies, Beukenkamp 2005

In 2002 David Snowden introduced a new conceptual framework for decision making, called the Cynefin model (figure 22).

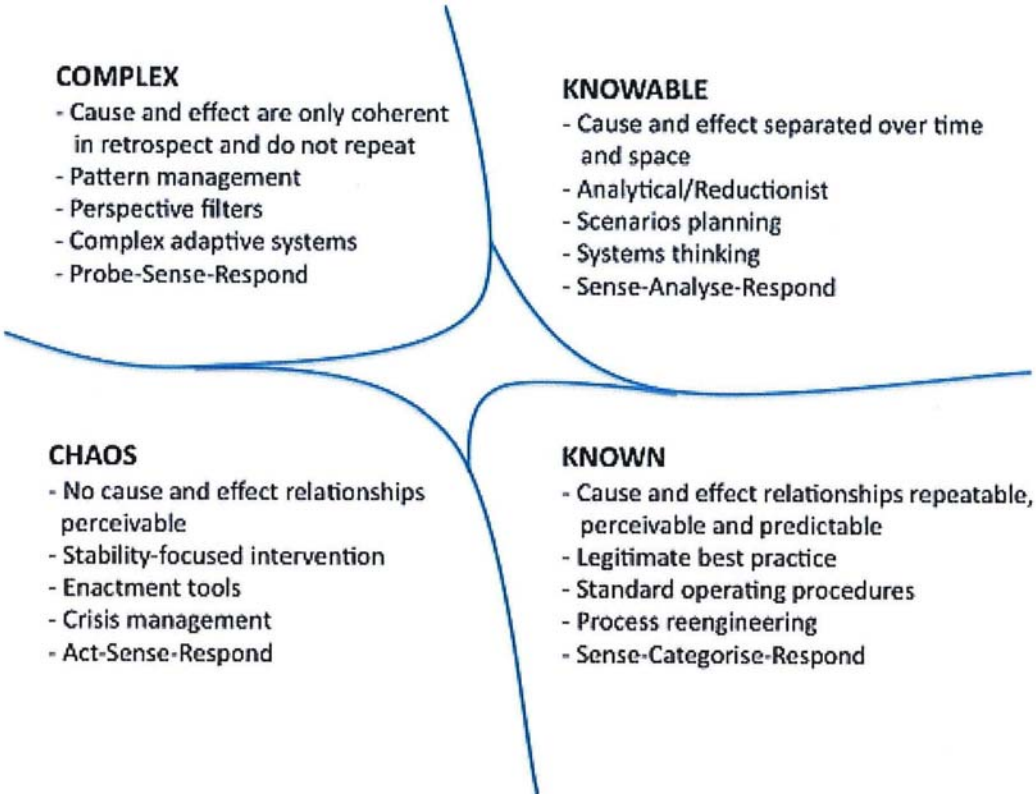

Figure 22. Cynefin model of decision making in complex situations, Snowden 2002

The Citadel approach as proposed by the author fits in well in the 'Chaos' quadrant of the Cynefin model, because it creates new certainties where they cease exist operationally. In 2013 French[65] expanded Snowden's Cynefin model to explain decision making in complex space. French explains in his paper that there is a relationship between the perspectives offered by the strategy pyramid and Cynefin.

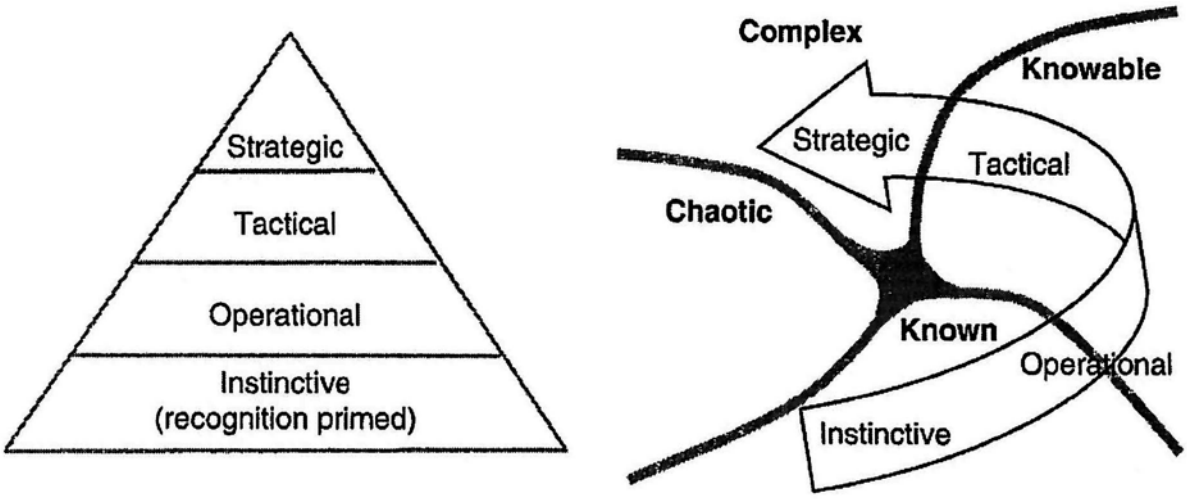

Figure 23. Relationship between the perspectives offered by the strategy pyramid and Cynefin. French, 2013

French[66] recognises three phases in the decision analysis cycle:

- '*Formulation or sense-making phase*, during which the problem, issues, objectives uncertainties and options are identified and formulated. This phase is much more visible in the knowable and complex space. In the known space the problems repeat so often that they were formulated long ago and sense-making becomes a matter of recognition, as acknowledged in the term 'recognition-primed decision making'.
- *Analysis phase*, during which the issues, objectives, uncertainties and options are modelled and analysed. According to French this involves predicting the consequences of each possible option in terms of its success in achieving the decision makers' objectives, taking account of the uncertainties in the prediction. Thus the analysis offers guidance towards options that promise to achieve their objectives. The analysis itself may be formalised as quantitative techniques of risk analysis' (note: as is common practice in the Netherlands when dealing with external risk). 'Or it may be much more informal and qualitative. Moreover there may be more than one strand of analysis, each representing a different perspective on the problem.
- *Appraisal and decision phase*, during which the decision makers decide which option to implement or whether more analysis is needed. Since any model is a simplification of the real world, there will be a need to reflect on the recommendation and determine whether it makes sense once the complexity of reality re-enters the discussion. Has the analysis brought enough understanding to make the decision? Is it requisite? If so decide and implement; if not, introduce further issues into the formulation and e-analyse'.

A classic risk approach determined by a more or less random distribution of incidents, will fail because the probability of for example a terrorist attack is directly linked to the properties (vulnerabilities) of that object and is not stochastic distributed. It is as if a fire is deliberately creeping towards the weakest petrol car in a train.

Terrorism at systems level is specifically aimed at the vulnerable aspects of the system, increasing already existing instabilities (both known and unknown) to such an extent, that a collapse is inevitable. This makes both the likelihood and the effects unpredictable, because any action to mitigate these problems results in a strategic counter move by the terrorist, attacking the next weak link in the chain. The chaos itself is the aim of the terrorists. Using game theories in combination with a Citadel approach is more likely to have effect when dealing with terrorism, because it aims at constraining the chaos.

3.6.2 Reliability paradox

A basic requirement for a successful security policy of the transportation system is control of the network, which is recognised by the Dutch government as crucial to a successful (transport) security policy. Terrorism is no longer seen as a technical problem at object level. Instead it is well recognised that at systems level terrorism is foremost a control and management problem.
TNO research indicated that at present the Netherlands is vulnerable to terrorist attacks[67] because of inherent weaknesses in the way its critical infrastructures are designed. Dutch society is not used to failures of its water supply, electricity mains or telecommunications according to this research.
A paradox exists because on safety grounds the proven high level of reliability of the technical design results in the absence of an economic justification for a more resilient design, making these systems extra vulnerable to terrorism. Not the state of a system is important, it is the transitions that make it vulnerable.
The other possible weakness is that 50% of the vital infrastructure is in private hands. These actors should realise that they are part of a complex tightly coupled system and therefore share responsibility for the whole system and not just their own part. One of the measures considered by the government is to renationalise the national power grid.
Recent events in the US (massive power failure in the north-east and Canada) have contributed to this consideration. Is the national interest so important that it justifies bringing the control of national infrastructures back in one hand? Which function is in which state of the system dominant? It is the struggle between monofunctional versus multifunctional thinking that in fact helps to create the George dilemma, see figure 20 §3.5.3.

3.6.3 Spin-off

The spin-off of the Citadel principle is that the transport system becomes more resilient. This is not only towards terrorism and other intentional criminal acts, but also when dealing with common accidents, the ‘normal accidents’ according to Perrow[68]. The Citadel way of thinking shows that some of these normal accidents are possibly serious as accidents, but not catastrophes at regional or even worse national level. One of the key recommendations is to design systems to become less complicated and interdependent. It is easier to make a linear loose-coupled system robust than a tight-coupled complex system as Perrow has shown.
The Citadel way of thinking helps to design and control systems away from these Perrow traps. In order to achieve a balanced policy to protect society against these sorts of threats, the systems approach indicates that the main policy should be aimed at coordination of the system as a whole. Until recently policy making appears to be primarily focussed on local problems or individual problems of various components thereby overlooking consequences outside the failed object or part of the system.

3.6.4 Results: expected and unexpected vulnerabilities

The outcome of the Ministry of Transport research was integrated with similar reports from other departments into a national report on critical infrastructures. In July 2005, the Minister of Internal Affairs presented this to Parliament[69]. In general the transport infrastructure was thought of as being reasonably resilient regarding a number of threats including terrorism. However, it is possible to identify specific parts of the system or objects which, when put out of action, could lead to serious disruption of the transport system or a large amount of casualties. Some parts of the transport system proved to be much more vulnerable than expected. The reason for this was that in most of these cases objects like tunnels provided facilities for other infrastructures, itself more vital than the contemplated infrastructure.

An investigated example shows that from the transport point of view (actor to function), the system is not vital. This changes when looked at from another systems point of view, because it is the latter system that could be seriously disrupted if the first system fails in a specific way, a form of a multiplier (regional) relation between a non-critical and a critical system. In another example disruption in the transport system not only leads to a serious malfunctioning in the transport system itself but also in another vital system, a multiplier (functional) relation between two critical systems, see chapter 6.

These cases show that system boundaries should not be taken too tight. However, when boundaries are too wide, the system runs the risk of becoming uncontrollable. In some cases vital infrastructures were vulnerable because of dependencies on other infrastructures, chiefly ICT and energy supply.

It is remarkable but not unexpected that elderly system designs proved to be more resilient than more recent designs. This is not because the older systems were over engineered, but because their (ICT) control systems were cruder, with many opportunities for manual operation in case of partial or complete failure of the control system.

Access control in transport systems, both physical and virtual, proved to be a general weak characteristic, almost inevitable given its main function and the requirement for low accessibility thresholds. The whole culture of the staff dealing with these objects is one of openness and pride.

This extends so far that internet is used for PR of these systems and its components. This is done in such a way that not only the function of some systems is shown but also the way in which they can fail. This makes very interesting reading for potential terrorists indeed. Added to that is the situation that many operational functions, chiefly day-to-day maintenance, has been outsourced to contractors without proper security screening of their staff.

Another problem arising with the use of the Internet is the risk of hacking and virus attacks. Every system that communicates via the Internet is vulnerable regarding these problems. Although at present there are no known cases of serious attacks on strategic systems, the risk of this problem cannot be ignored given the widespread character of it.

A further example of an unexpected vulnerability is a case whereby the characteristics of the system make it vital yet invulnerable. E.g. during normal operation the actual use of the system depends on extreme meteorological conditions, which are completely unpredictable for terrorists, thereby making it a very unattractive target.

This changes fundamentally once the system is being tested. The test in itself creates a much-increased exposure and the possibility of a progressive collapse of other systems. This is mainly caused by the circumstance that the test is to a large extend predictable, being announced on Internet month before in sufficient detail. Given the fact that such a real time test is very spectacular to watch, hundreds if not thousands of spectators gather nearby, creating all the ingredients to make it a very attractive target.

Finally human resource management proved to be a potential Achilles' heel. As mentioned earlier in this thesis one object supervisor stated that he felt 'like a tourist on his own object'. Erosion of object and systems knowledge within the organisation is already showing signs of becoming a very important hazard. Again, this is caused by the general policy of outsourcing as much as possible, without defining the acceptable minimum of knowledge (strategic, tactical and operational) within the parent organisation.

3.7 Conclusion

When dealing with problems, experts have a tendency to delimit their scope to what they are normally involved in. Thinking outside the box does not come naturally. With regard to transport and traffic related problems, the Pizza model can help to detect causes and additional options for interventions. The effectiveness of the idea was illustrated by looking at problems relating with two kinds of ageing: ageing of the population and ageing of design and technical structures.

Ageing is an inherent property of transport systems. It could be a problem if the threats of this aspect are not recognised in time. On the other hand, ageing in dynamic systems is a natural process, which can be controlled. The answer to ageing problems does not lie in finding just any solutions but finding the effective and efficient ones. What is required is a shift from looking at the explaining variables to looking at the steering variables.

The Pizza-model helps putting a problem in a broader context, finding new lines of approach and generating new solutions that could be more effective and efficient than the solutions that seem obvious at first sight. The Pizza-model is foremost a map necessary to find the way out of trouble rather than the road to safety itself.

The Citadel principle studies multiple roads to possible solutions. It not only focuses on the analysis and barriers that are already designed into the system. It also focuses on the possible or viable solutions. Above all the envisaged effect of the Citadel principle is slowing down the degradation of the system, thereby introducing the notion of time dynamics. The importance of this will be shown in chapter 6.

The conclusion from these observations is that it is necessary to view safety critical systems from a third perspective by looking more closely at their control variables. The next chapter takes a look at what happens in major projects, their protocols and procedures. How do we deal with them at present? And above all: is that view restricting us in way that can hide safety criticality in such a way that it only becomes an emerging (hidden) property much later?

Research question 2: *What roles do safety and security issues play in the decision-making processes regarding large scale infrastructures in the Netherlands*? Can be answered as follows. Safety and security issues play an important part in decision-making processes regarding large scale infrastructures in the Netherlands. However, they must compete for funding with environmental and economic issues.

Also the view regarding safety and security is an ex ante view. Once construction has started and later when in use changes both within and outside the system that influence it are not always understood. During design and construction managing the process (often dominated by the necessity to control budget) sometimes tends to be dominant over managing the contents and the envisaged outcome. If process and contents do not converge at some point in the process, the outcome can be missing the original goal completely. This can result into drift into failure when the importance of modelling time as a dominating factor is not understood.

Notes

[1] Nowadays operating as RWS-WVL
[2] Ref. Perrow, 1999
[3] Ref. George, 1980
[4] Ref. Petroski, 1992
[5] Ref. Algemeen Dagblad, 11-02-2006
[6] Ref. Algemeen Dagblad, 21-02-2006
[7] Ref. Algemeen Dagblad, 21-02-2006
[8] Ref. IJsselstein et al, 2006
[9] Ref. Interview, 2004
[10] Ref. Donald Rumsfeld, Secretary of US Department of Defence, February 12, 2002
[11] Ref. RIVM, 2003
[12] Ref. Stirling, 1999
[13] Ref. Donald Rumsfeld, Secretary of US Department of Defence, February 12, 2002
[14] Ref. Beukenkamp et al, 2003
[15] Ref. RIVM, 2003
[16] Ref. Projectteam Tunnelveiligheid, 2003
[17] Ref. Commissie Duijvestein, 2004
[18] Ref. Hendrickx, 1991
[19] Ref. Stoop et al, 2003
[20] Ref. AD, 2002
[21] Ref. Petroski, 1992
[22] Ref. Methorst, 2003
[23] Ref. Beukenkamp, 2006
[24] Ref. Methorst, 2000
[25] In 1996, TWA flight 800 crashed of Long Island because of power cables igniting fuel damps. The cause of this was found to be aged insulation of the power cables.
[26] Ref. Government of Estonia, 1997
[27] Ref. Government of Estonia, 1997 §3.1
[28] An infamous example that caused a major rethinking in structural engineering is the Ronan Point disaster. Ronan Point was a 23-storey tower block in Newham, East London, which suffered a fatal partial collapse due to a natural gas explosion on May 16, 1968. Ronan Point was part of the wave of tower blocks built in the 1960s as cheap, affordable prefabricated housing for inhabitants of the West Ham region of London. The tower was built by Taylor Woodrow Anglian, using a technique known as Large Panel System building or LPS. This involved casting large concrete prefabricated sections off-site, then bolting them together to construct the building. Only a few weeks after the occupants had moved in, a gas explosion demolished a load bearing wall, causing the collapse of one entire corner of the building. Four people were killed in the collapse, and seventeen were injured.
[29] Ladbroke Grove, 1999
[30] Eschede, 1998
[31] Amsterdam CS collision, 2004
[32] According to an estimate by the International Data Corp, a total of USD 297 bln had to be spend worldwide to fix the Y2K bugs in computer systems. The cost of the 9-11 attack was in the order of USD 20 bln, according to the official US reports.
[33] Ref. Perrow, 1999
[34] Ref. Centraal Bureau voor de Statistiek (CBS) data, 2012
[35] Ref. Centraal Bureau voor de Statistiek (CBS) data, 2012
[36] Ref. IVW veiligheidsbalans 2008
[37] At present, two railway acts are operational in the Netherlands. The new 2005 act applies to main line railways, being part of the European network. The original 1875 act deals with light railways (metro's) and tramways.

[38] The introduction of pressurised cabins in jet liners is an example. This innovation introduced the problem of fatigue in the airline industry, shown by the problems with the development of the British build De Havilland Comet.
[39] Ref. IVW RV-04U0008, 2004
[40] Ref. IVW RV-04U0008, 2004, Raad voor de Transportveiligheid, 2005
[41] A good example is the collision between a tram and a bus in Amstelveen near Amsterdam, October 17, 2008. The tram driver ignored a red traffic light and caused the accident. The dominating problem according to the investigators was that this road crossing was disaster waiting to happen, being a complex traffic junction with heavy traffic flows (trams, buses, motorcars and cyclists). (IVW RV-08U0831).
[42] Ref. IVW RV-04U0008, 2004
[43] Rotterdam (2005), Utrecht Lunetten (2005), Arnhem (2006), Rotterdam (2006), Amsterdam Muiderpoort (2007), Weesp (2007)
[44] SPAD = Signal Passed At Danger; a train running unauthorised through a signal that shows a 'stop' indication (usually red).
[45] IVW report RV-04U008, 2004 stated that although the driver of the train in question caused a SPAD resulting in the frontal collision with an approaching intercity, he was not to be blamed for this.
[46] Recently, two serious derailments of freight trains occurred in the Netherlands through axle failure, one in December 2008 between Amsterdam Central Station and Muiderpoort station and another in March 2009 between Harmelen and Vleuten west of Utrecht. In case of the Amsterdam derailment, four tracks and a canal bridge were damaged, disrupting rail traffic for a week. A collision with two NS passenger trains was only narrowly avoided, whilst a Frankfurt bound ICE had just passed the offending train.
[47] Such as DD-AR and VIRM type rolling stock as operated by NSR
[48] Such as the Sprinters and the new SLT's as operated by NSR
[49] The Dutch railway inspectorate IVW investigated the crashworthiness of the VIRM design (IVW RV-05U0026 p. 28-30).
[50] BLEVE: Boiling Liquid Expanding Vapour Explosion, the explosion resulting from the uncontrolled escape of a pressurised gas or vapour. A BLEVE can either be hot or cold. In a cold BLEVE, a pressure vessel fails either through being punctured or because of some form of mechanical weakness of the vessel itself. The escaping gas or vapour expands adiabatically (no energy being transferred from outside the vessel to its contents), resulting in the cooling down of the mixture in the vessel. In a hot BLEVE, heat is transferred (e.g. as a result of a fire) from the outside the vessel to its contents. This results in a boiling process of the liquid inside, increasing the pressure in the vessel. This process continues until the vessel fails through overpressure, when the content escapes. This is the classic steam boiler explosion.
[51] Ref. Perrow, 1999
[52] Ref. AVV, 2003
[53] Ref. Stoop (1990), Toft et al (1994), van Duin (1992), Petroski (1992) and van Poortvliet (1999)
[54] Ref. George, 1980
[55] Ibidem
[56] Ref. Beukenkamp, 2004
[57] Many books have been written about the development of battleship design. One of the classic ones is Dr. Oscar Parkes O.B.E. A.I.N.A. 'British Battleships: A history of Design, Construction and Armament'.
[58] During the Battle of Jutland in 1916, SMS Seydlitz, a battle cruiser of the German High Seas Fleet, received 23 hits; she nearly sank, yet managed to reach the naval base at Kiel through successful damage control efforts requiring flooding and counter-flooding to prevent her from capsizing. When the Seydlitz entered port her forecastle was awash right up to the first barbette (gun turret). During the same battle, the British Grand Fleet lost three battle cruisers in quick succession after receiving single hits, resulting in exploding magazines because of poor internal protection and poor handling

procedures. Afterwards Admiral Beatty, commander of the Battle Cruiser Squadron, made his famous remark: 'There seems to be something wrong with our ships today.'

[59] Ref. Parkes, 1957.

[60] Ref. Beukenkamp, 2004

[61] One of the arguments against it is, that cabin staff is no longer capable of entering the cockpit in case of problems in the cockpit, such as ill pilots.

[62] Germanwings Flight 9525 was a scheduled international passenger flight from Barcelona–El Prat Airport in Spain to Düsseldorf Airport in Germany. The flight was operated by Germanwings, a low-cost carrier owned by the German airline Lufthansa. On 24 March 2015, the aircraft, an Airbus A320-200, crashed 100 kilometres (62 mi) north-west of Nice in the French Alps after a constant descent that began one minute after the last routine contact with air traffic control and shortly after it had reached its assigned cruising altitude. All 144 passengers and six crew members were killed. It was Germanwings' first fatal accident in the 18-year history of the company.
The crash was deliberately caused by the co-pilot Andreas Lubitz, who had previously been treated for suicidal tendencies and been declared "unfit to work" by a doctor. Lubitz kept this information from his employer and reported for duty. During the flight, he locked the pilot out of the aircraft's cockpit before initiating a descent that caused the aircraft to crash into a mountain.

[63] To nuance this: in general this is true, however 35% of the Amsterdam commuters travel by train; a failure of the rail system around Amsterdam would create serious transport problems in the entire western part of the Netherlands, including Amsterdam Airport Schiphol, as recent railway accidents around Amsterdam have shown.

[64] Most of the Netherlands is located below sea level or below the level of the main the rivers Rhine, Waal and Meuse, creating the need for an adequate regional or sometimes even national drainage system. This system is also very important for the supply of fresh water.

[65] Ref. French 2013

[66] Ibidem

[67] Ref. Algemeen Dagblad March 13, 2004

[68] Ref. Perrow, 1984

[69] Ref. MinBZK, 2005

4. Introducing a third perspective: large projects

4.1 Introduction

The previous chapter showed the necessity to view safety critical systems from a third perspective by looking more closely at their steering variables. This chapter takes a look at what happens in major projects, their protocols and procedures. How do we deal with them at present? And above all: is that view restricting us in ways that can hide safety criticality such that it only becomes an emerging (hidden) property much later?

Large projects take a long time before they become operational. At the start assumptions are necessary regarding their societal and environmental effects plus their economic consequences. Detailed studies using established protocols and procedures are necessary to prove the correctness of these assumptions and compare the various alternatives. In the end a preferred option emerges that serves as the basis for a more detailed design that forms the basis for the project itself. However, by that time the whole system influenced by its surroundings (such as societal and technical developments) can have changed considerably, thus undermining some of the original assumptions and estimates.

The previous chapter showed the role that safety and security issues play in the decision-making processes regarding large scale infrastructures in the Netherlands. This chapter deals with research question 3: *If this role is insufficient, what are the causes of this?*

As the previous chapter showed a too static approach can introduce hidden properties and hidden dangers. This chapter takes a look at these large projects and their established protocols and procedures. How is safeguarded that the system over time will not drift away from its original development envelop (such as represented by the quadrants of Slovic/Stirling)?

4.2 Types of safety related to transport systems

In general, the following safety aspects are relevant to the decision-making processes regarding infrastructures and transport systems:

- Internal safety;
- External safety;
- Social safety.

Traffic safety deals with the consequences of traffic for its road users. Traffic safety can be expressed in terms of number of accidents, number of casualties or number of fatal injuries resulting from traffic accidents. AVV/Transport Research Centre (1999)[1] defined a traffic accident as 'an event on a public road, related to traffic, whereby at least one vehicle in motion is involved and resulting from which one or more road users have been killed and/or have been wounded and/or material damage has occurred'.
Transport safety encompasses road safety, railway safety, air safety, maritime safety, safety on rivers and canals. A traffic accident within transport safety is defined by AVV/Transport Research Centre as[2] 'an accident, related to traffic by means of transport on public roads, trains, ships and/or aircraft, whereby at least one moving craft is involved and resulting from which one or more system users have been killed and/or have been wounded and/or material damage has occurred'.
External safety deals with the consequences of traffic and transport for the safety of third parties, those not directly involved with the transport system. According to AVV external safety risks are[3] 'risks to the environment caused by the production, storage, transport and use of hazardous materials'. In the Netherlands, the risk resulting from flooding is seen as part external and part internal. The risk resulting from aircraft crashing in populated areas is seen as having both an internal and an external component. The same applies to derailed trains. The above-mentioned definition of external safety as used by AVV is therefore too narrow and focuses only on dangerous goods[4].
Social safety is according to AVV[5] determined by the extent of criminality and the perception of (un)safety in the public space. Social safety is determined by an objective and a subjective component. The objective component indicates the number of registered incidents related to criminality in the public space. The subjective component shows the extent of safety as experienced by the public.
One way or another all these aspects play a role in the decision-making processes related to transport systems. Some of them are covered by formal procedures; others are more internal (non-explicit) in the processes. As will be shown further on in this thesis it is the latter aspect that runs every risk of being overlooked.

4.3 OEI, MER, VER and the SEE-framework

In the Netherlands decision-making regarding infrastructures at strategic level is dominated by two studies. The first one is an (economic) cost-benefit analysis, called OEI[6]. The second one is the legally required environmental effect study MER[7]. In both studies safety is incorporated as one of the issues to be addressed by the study.
Recent research[8] has shown that in practice, safety requires a separate study, the safety effect report VER[9]. The latter is a relative new instrument that is not formally required, but used in an increasing number of projects regarding infrastructures. OEI, MER and VER have one thing in common, i.e. the decision-making dilemma, whereby interests regarding safety have to compete with economy and environment, the so-called SEE-framework[10], see §4.3.4.

4.3.1 OEI (Research into the effects of infrastructures)

The design and construction of the freight railway from Rotterdam to Germany, the so-called Betuweroute, showed that a structured cost-benefit analysis was necessary. The main problem was that at the time of construction of the Betuweroute serious doubts existed regarding its environmental benefits[11], the way it would counter traffic congestion on motorways[12], and the economic costs that would far outstretch its proposed benefits[13].
Therefore the Ministry of Transport en Water management decided that a manual needed to be developed for a structured and documented guideline to assess the viability and necessity of major infrastructure projects.

This became the OEI manual, although at first it was known as OEEI[14], because initially it focussed chiefly on the economic costs and benefits of these projects. Later on it became possible to quantify other effects as well, such as safety, environment and social effects. Since then, the cost-benefit analysis has become standard in the assessment of such projects.
The essence of the OEI assessment is that all benefits and detriments of a project are examined. Each one of them is quantified and translated into a financial value. The basic idea behind the cost-benefit analysis is that consumer preferences must be the dominating guideline for the appraisal within the governmental policy regarding a proposed project. The willingness for a consumer to pay for an envisioned benefit against the cost of the investment by the government is the core of the discussion. It is not possible to translate each and every one of the costs and benefits into money. Still they are taken into account but as a p.m. post. Adding and subtracting the costs and benefits gives a balance, which can be either positive or negative.
Building an infrastructure precedes its use. In order to compare costs and benefits it is therefore necessary to use a discount rate, a fixed percentage to translate future values into present values. Usually the horizon of a costs-benefit analysis is 30 years or more. The value at the end of the period, the residual value, is often incorporated as well.
Problems arise for effects for which no economical market exists (environmental effects) or where the market fails, because the consumers don't have the proper information to assess the costs and benefits[15]. More recently transport topics have shifted to the issue of gaining time. This gain is not easily translatable into quantifiable economic benefits. The latest development is the issue of reliability of transport systems. Again this aspect is not easily translatable into quantifiable economic benefits and is in the forefront of scientific and social studies.
One of the inherent weaknesses of the OEI research is its timing. The OEI research takes place at a very early stage in the decision making process, when the problem is clear but where major uncertainties exist regarding the possible solutions and their side effects such as environmental impact. These side effects need to be addressed to satisfy other stakeholders. Therefore this process uncertainty translates into economic uncertainty. This weakness was recognized by the Parliamentary Enquiry Committee when they investigated the problems regarding major Dutch transport infrastructure projects[16].

4.3.2 MER (Environment Impact Assesment)

The M.E.R.-report is legally required as part of the planning process for major infrastructural projects. The procedure investigates the environmental effects of a proposed project and is as such the implementation of European Guidelines 85/337/EEC, 97/11/EU and 2003/35/EU. Safety is one of the aspects covered by the report. Given its aim (environmental effects) the focus of the report is external safety, not internal safety.
The MER dictates a choice between three basic alternatives:

- Zero-option/autonomous development. What would happen if the present situation including a foreseen development of the use of existing infrastructures would continue for the foreseeable future? In other words, the option nobody really wants.
- The environmentally friendliest alternative: what alternative exists for the planned infrastructure (change) that is most friendly towards the environment? This is the option that satisfies one party and disappoints all the others.
- The planned alternative: what would the effect be of the planned infrastructure (change)? This option gives everybody something, but is usually best described as the least unfavourable alternative, which does not satisfy anybody, and deviates from the original reason for the project, the problem that needs to be solved.

Often the outcome of the MER procedure is that the planned alternative appears to be the best (or least worst) compromise. This is underpinned by sometimes thousands of pages of studies, leaving little room for further research and identifying knowledge gaps. Indeed the impression exists as if these knowledge gaps don't exist at all. Stoop[17] claims that the aim of this process is to achieve consensus on the middle alternative: the planned alternative as presented by the initiator, using the famous Dutch 'Polder Model[18]' as management instrument. The plans are presented in such a way that the discussion focuses on the procedure, not the contents, which have been worked out in advance in great detail and leave little room for change. As Stoop puts it: the MER results in three options, none of which are really satisfactory.
The fact that the MER results in compromises does not mean that the struggle is over after the MER phase of a project. The inherent shortcomings of the MER often results in further struggles and enduring legal battles, instead of consensus on rational foundations for decisions, addressing first of all the raison d'être for the project: the original problem that needs to be solved. The recent conflict between the Netherlands and Belgium about the deepening of the Westerschelde river leading to Antwerp is a clear example of this problem.
The other weakness of the MER is that it focuses on external effects, stimulating a tradeoff between internal and external safety to the benefit of the latter. In a densely populated country like the Netherlands where space is at a premium, quite often the only way to satisfy negative effects to the environment is to construct a tunnel. This reduces to external risk to virtually nil, but increases the internal risk considerably. Since there is no requirement within the MER to address the problems of internal safety, this problem is carried forward to the design and building phase, when few alternatives exist to solve these problems. After all, a tunnel is a tunnel with all its safety limitations. The risk for the traffic through a tunnel (internal risk) is always higher than the internal risk for a surface solution (embankment, viaduct).
It appears that in these cases safety seems to be regarded as something to be solved by engineers, instead of being the responsibility of the original decision makers[19]. The MER shows a clear tension between safety and the environment, a tension that often exists and in many cases incorporates a third element as well, the cost of the various alternatives, the economic viability. This aspect will be shown in §4.3.4 about the SEE-framework.
It is unavoidable to go through the MER procedure, yet the outcome of it must be regarded with precaution. The MER gives a direction towards a possible outcome, but has its limitations. One of the challenges is to restore the balance between internal safety, external safety and economy. Another instrument is needed to achieve this and that instrument exists since the beginning of this century under the name of the VER, the safety impact assessment.

4.3.3 VER (Safety Impact Assessment)

It became apparent during the last decade of the 20th century that something was missing in the approach of safety during major infrastructure projects. The construction of the infrastructure was dominant, followed by its environmental impact, as shown in the previous paragraph. Safety related problems only became clear when the new system was about to be commissioned. An example is the case of the tunnels in the Betuweroute freight railway from Rotterdam to Germany, where the discussion between the emergency services (fire brigades) and the project management about the necessary fire repression systems started very late in the project, when the tunnels and rail infrastructure were almost ready for use. Another example is the change in the layout of Schiphol Airport (new runway, new ATM system).

This awareness in a late stage of the project that safety was not addressed properly made it very difficult to implement necessary retrospective changes, not only for the project management but for other stakeholders as well. A cautionary approach by these external stakeholders was sometimes regarded by the initiators as 'over cautious' or even 'obstructive'[20]. In this way LVNL (ATM Netherlands) conflicted with Schiphol about the above-mentioned changes in airport configuration, initiated by Schiphol on grounds of capacity.
Following the safety problems that arose from amongst others the Betuweroute, a new instrument was proposed, being the Safety Impact Assessment or VER. The VER is a process instrument that focuses on safety issues, not at the end of a project but right from the start of it. The aim of the VER is to achieve process transparency regarding safety risks and safety related problems as indicated or expected by stakeholders and how they can be dealt with or how they can be avoided. The results of the VER can be used when the safety case is written, because if the VER does its job well every safety case issue that is relevant for the safety case will be indicated and specified during the VER phase. The VER does not focus on solutions; it focuses on risks and accompanying preconditions by the key stakeholders.
Important for the VER is, that contradicting interests or opinions regarding possible risks are identified early in the project. Each stakeholder identifies his safety preconditions and makes them known to all the other stakeholders. The VER is not a single phase (round) in the project, but a continuous process of identifying risks and ways of reducing them. It forms an integral part of the project and runs parallel to it. It is possible to use the VER to research the safety consequences of changes in the project, such as the replacement of a proposed bridge by a tunnel alternative for example during the MER phase.
The weakness of the VER is that it can be used to impede the progress of the project by forcing the project management to address each and every safety issue before the next phase of the project can start and then repeat the whole process during that phase. Such a use is detrimental for the VER as a policy instrument. If that happens it is very likely that the VER will be killed-off in the force field between government, emergency services and private parties[21]. The VER has never been legally recognised nor implemented on a wider scale because of this inherent weakness.

4.3.4 SEE-framework

The final stage of the process of integrating economics, environment, internal and external safety was the introduction of the SEE framework (VEM-raamwerk) at the end of the last century. SEE stands for safety, economics and environment. As mentioned in the previous paragraph, a conflict arose between Schiphol Airport and Air Traffic Control Netherlands about the safety consequences of the proposed changes in runway and air traffic management configuration of the airport. This stimulated ATC Netherlands to develop the SEE framework as a policy instrument to balance the dilemmas of safety, environment and economics (efficiency)[22].
In 1999, a project was started to develop the possibility of landing on converging runways outside the Universal Daylight Period (the so-called UDP project). The first application of the SEE framework on this project took place in 2001. The risk of a collision was investigated between two aircraft simultaneously executing a missed approach procedure on converging runways.
The SEE framework aims to explain the operational requirements by Schiphol to the air traffic controllers within ATM Netherlands. Furthermore the framework aims to justify the capacity limits and matching mitigating measures to external stakeholders (external from the point of view of ATC Netherlands).

In other words: the framework is the instrument used by ATC Netherlands to guarantee that external forces to increase capacity and reduce noise are counter balanced by sufficient attention to the safety implications of these proposed or required changes.
It offers a framework to take decisions about the required level of safety of the ATM system. Also it answers the question of whether the impact on the system of the identified risks resulting from the proposed changes (both individual and compound changes) is small enough to be regarded as acceptable. ATC Netherlands integrated the SEE framework into an effect report: the VEMER (SEE Effect Report)

The VEMER process (figure 24) is structured as follows:

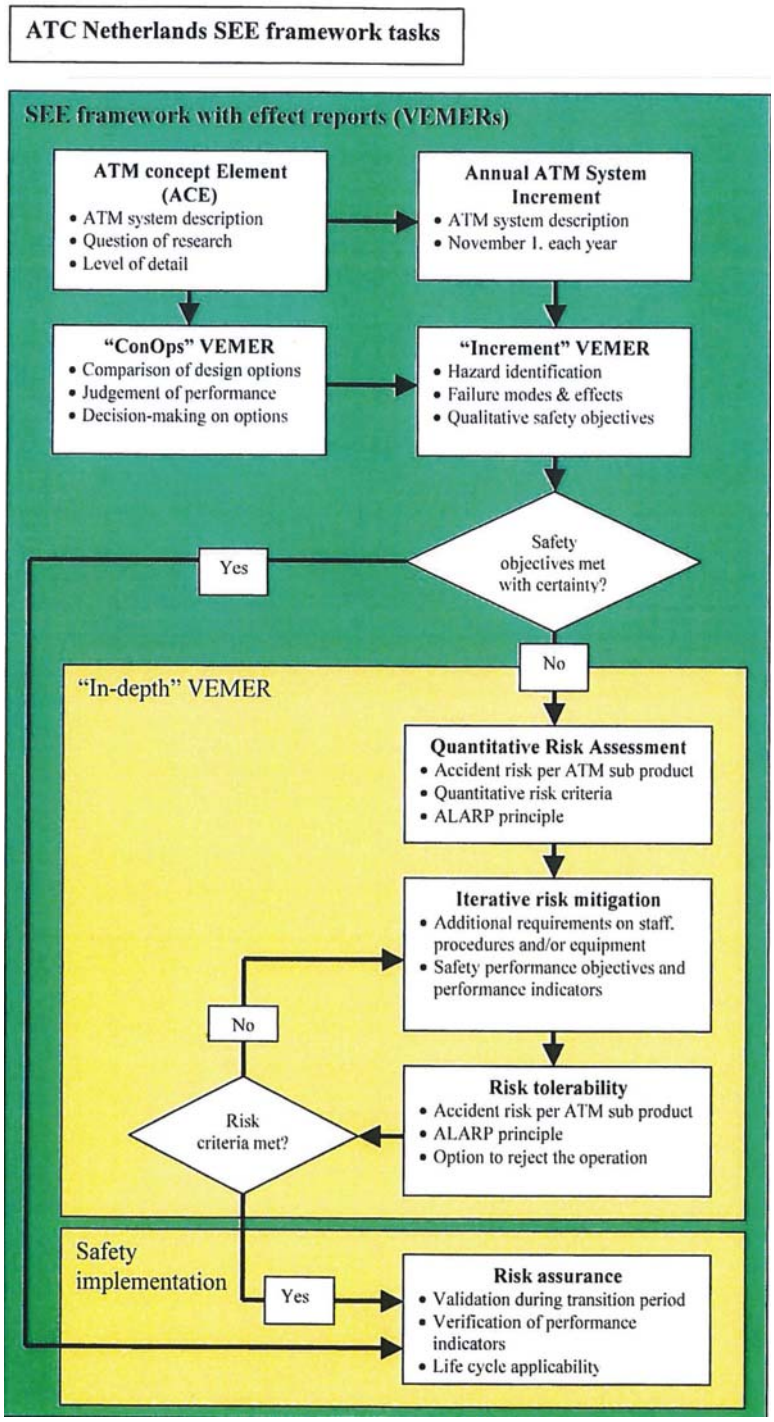

Figure 24. SEE framework tasks

4.4 Monitoring safety in design and construct; the HSL-Zuid safety process[23]

4.4.1 Introduction

Until fairly recently in the Netherlands safety aspects during design and construct of major infrastructure projects were assumed to be covered by existing formal environmental impact assessment procedures such as the OEI and MER procedures as shown in the previous chapter. In environmental impact assessment studies, conventionally a safety focus is restricted to external safety aspects, setting standards for individual safety and societal risk exposure (group risk as it was known previously).
These standards are derived by quantitative risk assessment techniques from accident data. Since transportation of hazardous materials was excluded from the HSL-Zuid concept, at first the railway was considered inherent safe'. This assumption was based on the track record of the existing railways in the Netherlands, which was at the time operating without a single casualty amongst passengers on the train since 1993, a track record which ranks amongst the best performing railway systems in the world[24].
Such an assumption (approach) however does not fully take into account the different characteristics and context of a high-speed passenger railway transport system, nor does it consider additional measures to be taken to prevent accidents and to optimise rescue and emergency procedures after a railway disaster on such lines. Empirical evidence has demonstrated that an explicit and more encompassing safety focus could be beneficial to incorporate safety aspects in the project management and design of these innovative projects.
A pilot study performed over a number of years by Delft University of Technology served as a monitoring agent to assess and evaluate the development of a new safety approach, concurrent with the HSL-Zuid project development[25].

4.4.2 Prototyping safety

Like any prototyping rather than compliance with expectations, lessons can be learned from deviations in a planned process. The nature of a prototype is explorative and empirical and is characterized by its cyclic and iterative approach, dealing with ongoing adaptations and modifications. The most important question therefore is whether actors are prepared to learn rather than allocate blame and responsibility for failure (preferably to somebody else).

New actors and notions

To accommodate synchronization with development of the HSL-Zuid project itself, the prototype applied a systems approach and a top-down organization structure. Safety has been considered integral, including internal and external safety, working conditions, rescue and emergency operations and social safety aspects. The scope of the consequences was expanded from fatalities only to injuries[26] and the population at risk as a performance indicator for the rescue and emergency aspects. This focus introduced a new category of actors in emergency management and regional administration. Two major categories of actors proved to apply different notions on risk: the HSL-Zuid project organization based its safety critical decisions on probabilistic notions, while rescue and emergency services fundamentally applied deterministic notions.
Although they seemed incompatible, these two notions proved to be complementary in practice. Eventually the consensus on equivalence of notions increased the commitment of the rescue and emergency community and reinforced the public support for the project. In addition, attempts were made to apply and integrate the various notions of the stakeholders. Abstract risk level standards were translated into realistic accident end emergency scenarios, which were made fit for design assessment by defining critical size events.

Shift in focus

The 'Projectgroep HSL-Zuid' (project team HSL-Zuid) started in 1995, composed of representatives of various governmental departments, the HSL-Zuid project organization[27], local and regional rescue en emergency services, hospital trauma care specialists, regional police forces and an independent safety consultant. The centralized organization which initially was favoured to maintain oversight over the project, soon evolved into a more fragmented approach, devoting attention to specific issues, some of them local.

Due to planning and time schedule constraints, the safety project followed the development of the design and construction process of the infrastructure. Specific working groups were established to deal with accident scenario definition, tunnel safety or emergency procedures and operations. However, major subsystems or aspects such as junctions with other railway networks[28], combined corridors with existing railways[29] and motorways[30] and the combined use of major railway hubs with the existing conventional railway system[31] were not incorporated in the safety analysis.

Consequently a loss of system coherence occurred, which could not be restored afterwards. The safety process drifted into fragmentation and became more and more interrupt driven as and when problems were encountered[32]. The design started as a railway-engineering project in which the conventional railway concept was stretched to its limits regarding speed, track and services rendered. The HSL-Zuid gradually evolved into a new railway concept, incorporating new tunnelling technology[33], new techniques for building the permanent way[34], new signalling systems including a new ATP system[35], new power supply systems[36], maintenance contracting and public private partnership cooperation[37].

External influences

In addition, the process was influenced by major external events in other European countries. The ICE derailment near Eschede in Germany[38] and several tunnel fires in the Alps region[39] had their influence on the design agenda and occasionally dominated the analysis. Due to these external influences specific measures to prevent derailments, fire safety measures and emergency handling strategies had to be developed.

Consequently during the project a shift in focus emerged from a traditional yet enhanced railway design into fire resistance of rolling stock, disaster management and emergency handling in long tunnels, accessibility of the permanent way for emergency services and self-reliance of passengers[40]. Although a process approach was favoured, the need to proceed with crucial design and construction decisions forced the safety project organization to intervene in substantive issues as they occurred.

Role of actors

The HSL-Zuid project organization played a dominant role in the safety project, as could be expected. This influence was caused by its specific engineering knowledge and past performance with major projects as well as its high interest in the need to accomplish the project within time and budget constraints. This position and the accompanying constraints put pressure on the participation and emancipation of the other participants in the project. During the process two major conditions have been identified as critical success factors for cooperation between actors.

1. creating and assuring mutual confidence between actors;
2. design and control of decision-making and cooperation processes.

During the process various documents were passed to establish safety references and to assure critical safety decision. A first 'Integral Safety Plan[41]' was followed by a generic concept and several specific safety concepts. During the project dedicated new entities were established. On a central level a safety committee performed the task of independent safety assessor (ISA) on substantive issues such as tunnel safety, social safety at stations or other relevant issues. When engineering detailing issues became relevant at a local level, a process manager was appointed to facilitate the safety process.

4.4.3 Lessons learned

The pilot study concluded that valuable lessons could be drawn from the HSL-Zuid safety project:

- Without the safety project the HSL-Zuid would have been less safe. Apart from the Channel Tunnel this approach may be considered unique, because from the start of the project safety has formed an integral and explicit part of the design process, incorporating all relevant actors and stakeholders into the project.
- After a central start the process fragmented resulting in a loss of efficiency. However, the process was overall effective and was dictated by the time schedule and planning of the design and construction processes. External influences were handled piecemeal as they occurred, such as the ICE train crash and the tunnel fires in the Alps.
- The status of the safety project organization remained unclear, due to the fact that it lacked a starting document, containing mission statement, control instruments and feedback loops with respect to quality and safety assurances.
- The dominance of the HSL-Zuid project organization over the other actors remained clear throughout the process. Differences in risk perception and acceptance were inevitable and can be explained by process and actor characteristics.
- Divergence and fragmentation was inevitable due to deficiencies in the process design, lack of decision making instruments, absence of a central as well as local process manager and existence of formal authorization capabilities and instruments exclusively for the final stages of the engineering design and construction phase.
- At the beginning of the project decision support tools were non-existent at a central level of the organization and had to be developed during the project. A need for a consensus document at the start of the project emerged, containing a description of the scope of the safety project, its performance indicators, involvement of categories of actors, their specific safety requirements and synchronization of safety critical decisions with principal decisions concerning the overall project.

4.4.4 Theoretical considerations

Several theoretical notions can benchmark the initial safety concept and the role of the project group. The evaluation will focus on the systems concept, the process approach and substantive results. Initially the systems concept of the HSL-Zuid could be defined as a linear system with loose couplings[42]. It was considered to be independent of other railway operations by way of its dedicated permanent way and exclusive operation of high-speed passenger services (the HSL-Zuid was never meant nor designed for freight operation).
Components were supposed to be designed and constructed independently in which a linear production sequence could be applied. Much attention was paid to the application of proven technology and public-private partnership configurations to achieve practical and pragmatic improvements. During the process its complex and interactive nature became apparent, requiring a moiré integral approach in which safety became a critical design issue, such as regarding tunnelling, working conditions, derailment prevention and retention and disaster management.

At first the process approach favoured a linear, step-by-step decision making process to guarantee the position of actors and interests. In this process critical decisions are positioned as late and low as possible in time and project hierarchy in order not to obstruct the bargaining position of the actors involved and to stimulate consensus and support[43]. Therefore major decisions were fragmented and allocated at a local level during the phase of the detailed design of components.
This process created dilemmas for the HSL-Zuid project organisation because critical decisions should have been made as timely and as conceptual as possible in order not to frustrate the design and engineering time schedules. Actors opposing such decisions were forced to apply their 'obstructive power[44]' during final project phases because their legal instruments such as participation in the building licenses processes and the operational licenses processes are limited these phases. They lack safety criteria in earlier phases of design and construction.
Substantive safety results were dominated by the influence of civil engineering and its design aspects, which remained dominant over the life cycle of the project itself, until de civil engineering part was delivered and the operation was prepared, when the signalling system ERTMS/ETCS became the dominant issue. Applying conventional railway engineering approaches tend to focus and detailing levels and components design, because the railway system as a whole tends to be regarded as proven technology.
Unfortunately innovative aspects which were incorporated during the design process had a major influence on the safety performance of the HSL-Zuid at systems level. Although hard to prove in a quantitative manner, the Green Heart tunnel, drilled as a large diameter single bore tunnel in soft soil, is a prominent example of innovative design with major safety benefits. The original design envisaged a traditional twin-bore tunnel. After elaborate debate a cost efficiency optimum was established for this (twin bore) design for escape intersections at regular intervals, complying marginally with safety standards for emergencies. The private consortium that came up with the alternative design applied a different concept with a single bore tunnel of a much larger diameter with an internal partition wall, facilitating all demands of the emergency services[45]. Technological innovation proved to serve the safety issue as well.

4.4.5 Common concerns and similarities

In the Netherlands the HSL-Zuid project is not unique. Several major infrastructure projects have been realized. The issue of underground structures and the multiple land use is rapidly developing[46]. Common concerns and similarities may occur across the projects with respect to safety issues.

Common concerns
In order to improve the advisory role of the fire brigades as a participatory organisation in design and construct, a series of major infrastructure projects was analysed regarding safety[47]. This analysis focussed on the responsibility and authority of each actor. It revealed a patchwork of safety notions, lack of consensus on acceptable standards, lack of structure in the decision making process and clarification of safety resource allocation and a considerable unawareness of the public with respect to residual risks in the operational phase.
Recommendations were drawn up to cope with the three major issues[48]:

- A lack of an adequate frame of reference and uniformity in risk assessment;
- An ad-hoc structure of decision making processes;
- A lack of advisor knowledge within the rescue services beyond the level of individual expertise to support major infrastructure organisations.

Safety issues in the HSL-Zuid project are part of more common concerns in infrastructure projects. Leeuwendaal recommended supplementing the assessment framework of these projects. Leeuwendaal acknowledged that given the character of such projects (unique, complex, innovative, 'design and construct') a general assessment framework regarding safety is not possible. Such a framework can only be accomplished in phases, linking up with the phasing of the development of each project.
Leeuwendaal identified four phases[49]:

1. A safety effect report (VER)[50] should be written as part of the legally required environmental effect study[51] (MER) or as an autonomous report when the MER is not required.
2. The safety paragraph of the MER or the VER will result in an integral safety plan[52] (IVP), in which de general philosophy towards safety and its point of departure is laid down.
3. Based on the IVP in the next phase a safety concept A is developed, in which safety requirements and measures are crystallized for the project as a whole.
4. Finally, for each part of the project (bridges, tunnels etc.) a safety concept B has to be developed, in which safety requirements and measures for that specific issue are to be finalised. These safety concepts have to deal with the construction phase as well as the operational phase.

Similarities
Even more in general, safety issues of the HSL-Zuid encountered similarities with the successful implementation and social acceptance of other major Dutch projects regarding road transportation and transport innovation[53]. Rather than applying proven technology and pragmatic improvements on a detailing level, a 'system shift' may be necessary to overcome constraints in system development[54]. Major issues in various transport systems have led to such high system pressure that fundamental changes are required:

- The integral safety plan IVP is a must for all future projects;
- Projects should be safeguarded against fragmentation of safety issues.
- Right from the start of a project a subproject should be started regarding safety, in order to identify safety critical issues;
- In future plans as designed by the Ministry of Transport should no longer be judged by the Ministry itself, but by an independent outside expert(group), such as a safety committee or an equivalent of the existing MER-committee;
- Each participating actor should ensure that its representatives have the necessary (expert) knowledge to advise the project organisation;
- Independent process managers at project level should control the process at project level and at local level in order to achieve mutual trust and commitment between actors.
- There is a need for a consensus document wherein at the start of the project each and every actor writes down his or her safety requirements and preconditions.

These changes may be achieved through conceptual change in areas such as inland shipping logistics, dedicated terminals and reversed container logistics in ports, spatial planning and urban development with respect to underground structures and multiple land use. To incorporate safety in these conceptual changes, it may become necessary to transform safety from an operational cost into a strategic policy making issue[55].

4.5 Conclusion

Lessons learned from the HSL-Zuid project can be put in a wider perspective. Common concerns and similarities with other infrastructure projects can be identified. Such concerns can be expected in view of theoretical considerations regarding a systems approach, the decision-making process and substantive aspects. Integrating safety into the technical design and construct process can be realized, but it requires a different notion of safety.
Also a relation can be established with the control and management processes of the project. Together these accomplishments constitute a safety prototype along the lines of the DCP-diagram[56], which has a wider applicability for underground structures. A proof of success is difficult; especially since safety performance parameters and supporting instruments are still under development. Innovative solutions such as the single bore tunnel under the Green Heart have contributed to a significant increase in safety levels.
The outcome of chapters 3 and 4 answers **research question 2 and 3**: *What role do safety and security issues play in the decision-making processes regarding large scale infrastructures in the Netherlands*? *If this role is insufficient, what are the causes of this?* The examples in this chapter prove that despite the fact that safety and security play a major role in these projects, something is missing in general, which is a more dynamic way of modelling risk. Procedures such as the safety impact assessment VER have never been implemented. The independent safety assessor is sometimes used, but not on a general base. It is not just the models that fail, also the procedures fail to explain the situation in practice. This makes it necessary to have an empirical view at this practice.
One of the missing dimensions appears to be the time factor. The next chapter will show how important time is as a hidden property of safety critical systems, by introducing the notion of resilience time.

Notes

[1] Ref. AVV, 2006 p. 9
[2] Ref. AVV, 2006 p. 10
[3] Ref. AVV, 2006 p. 10
[4] As is shown by the Amsterdam Air Crash in 1992, when an El-Al Boeing 747 crashed into an apartment building in Amsterdam, resulting in 43 fatalities, plus a large amount of material damage on the ground. Another example of an external risk resulting from transport other than that of hazardous materials is the Osaka train crash in 2005, when a train got derailed and crashed into a building, killing 50 people.
[5] Ref. AVV, 2006 p. 10
[6] OEI = Onderzoek Effecten Infrastructuren (examination of the effects of infrastructures).
[7] MER = Milieu Effect Rapportage
[8] Ref. Leeuwendaal 2001, p. 4; Tweede Kamer 2004-2005, p. 128
[9] VER = Veiligheidseffectrapportage
[10] VEM-raamwerk: veiligheid, economie & milieu
[11] Ref. Van Wee et al 1994, p. 20
[12] Ref. Janse et al 2000, p. 5
[13] Ref. CPB 1995, p. 20-22
[14] OEEI = Onderzoek Economische Effecten Infrastructuren (Examination of economical effects of infrastructures)
[15] A good example is the willingness to reduce CO_2 emissions
[16] Ref. Duivesteijn Committee chapter 10
[17] Stoop 2004: *Een m.e.r. a boire of een stap te v.e.r.*; working document (never published)

[18] http://en.wikipedia.org/wiki/Polder_Model*: The Polder Model is a term with uncertain origin that was first used to describe the internationally acclaimed Dutch version of consensus policy in economics, specifically in the 1980s and 1990s. However, the term was quickly adopted for a much wider meaning, for similar cases of consensus decision-making, which are supposedly typically Dutch. It is described with phrases like 'a pragmatic recognition of pluriformity' and 'cooperation despite differences'. A popular explanation of both the term and the reason this decision-making style works so well in the Netherlands is the unique situation created by the fact that a large part of the country consists of polders below sea-level. Ever since the Middle Ages, competing or even warring cities in the same polder were forced to set aside their differences to maintain the polders, lest they both be flooded.*

[19] This can be illustrated by the case of Betuweroute freight railway from Rotterdam to Germany. In order to satisfy the environment of conurbations along the route, a considerable length of it was constructed in tunnels, without specifying the required safety regime. After the tunnels were constructed, indeed when the railway as such was ready, there emerged a disagreement with the local fire brigades about the measures required to contain and suppress fires in these tunnels. This discussion delayed the opening of the railway considerably. In the end, sprinklers were installed, which were deemed necessary by the fire brigades but were seen as a waste of money by other experts, given the fact that the railway was not designed for nor will it ever carry passenger trains.

[20] Ref. K+V, p. 1

[21] Ref. Wever 2002, p. 2

[22] Ref. K+V, p. 5

[23] The HSL-Zuid is the name of the project aimed at building a new high-speed railway from Amsterdam to Antwerp and Brussels, to link up with the new high-speed railways to Paris and Cologne and to London. It was finally opened between Amsterdam and Rotterdam in September 2009 after many problems with the signalling systems and rolling stock. The entire railway to Antwerp will be put into operation sometime in 2010.

[24] The only fatal injury amongst staff on board a train since 1993 occurred during a collision near Roermond in 2003. However, up to the present day, it is unclear whether the driver involved died before the accident as a result of heart failure (and was the cause of the collision) or that the heart failure occurred after the accident, see IVW DR-03U005.

[25] Ref. Beukenkamp et al, 2002

[26] This was unavoidable, given the fact that fatalities hadn't occurred since 1993.

[27] The HSL-Zuid project organization was formed by staff from the Department of Public Works and Watermanagement (Rijkswaterstaat) which has been responsible for major civil engineering projects in the Netherlands since it was incorporated by the Dutch government in 1798. Through its history it engineered and build the major canals, as well as most of the Dutch railway network, the Zuiderzee works (massive land reclamation) and more recently the famous coastal defences (Deltaworks) and the Betuweroute freight railway.

[28] The most important ones are the junctions north and south of Rotterdam and at Schiphol Airport.

[29] The HSL-Zuid uses the existing railway system between Amsterdam and Hoofddorp, from Rotterdam Central Station to Rotterdam Zuid and a branch to Breda for the national high-speed services.

[30] The HSL-Zuid runs parallel to the existing A4 motorway between the Burgerveen Aqueduct and Zoeterwoude; it runs parallel to (and was actually build on part of the original embankment of) the existing A16 motorway between the Moerdijk Bridge and Antwerp North.

[31] Amsterdam Central Station, Rotterdam Central Station

[32] Minutes of meetings of the project team.

[33] The tunnel under the so-called Green Heart (Groene Harttunnel) was build using the tunnel boring technique in soft soil. When constructed, it was the largest single bore tunnel of its type in the world.

[34] The soil along most of the projected track alignment was known to be soft, as is usual in the Netherlands. Therefore settlement can be expected; in fact on some existing railway lines this is a continuous process, requiring heavy maintenance and occasional speed restrictions until the vertical

track alignment is repaired. This was deemed unacceptable on the new high-speed railway, also because the high-speed operation required very tight tolerances in the track geometry, increasing the risk of derailment from settlement. The solution was to build the permanent way as a continuous slab on thousands of concrete piles driven into a stable sand layer. On top of this slab, the track itself was also innovative, using so-called Rheda2000 track.

[35] ERTMS/ETCS

[36] The standard power supply on Dutch railway lines is 1500V DC. The HSL-Zuid uses the European standard for such lines, being 25 kV AC. The only other railway in the Netherlands that uses this system is the new Betuweroute from the port of Rotterdam to Germany.

[37] It was through this partnership that the new tunnel under the Green Heart was designed and build. A consortium of outside contractors was responsible both for the design and its construction.

[38] The Eschede train disaster was the world's most serious high-speed train accident at that time. It occurred on 3 June 1998, near the village of Eschede, Germany. 101 passengers and staff on board lost were killed and 88 were injured. It was caused by a single fatigue crack in one wheel which, when it finally failed, caused the train to derail at a set of points. The seriousness of the accident was exacerbated when the derailed section of the train crashed into a viaduct and demolished it, wrecking the rear part of the train in the process.

[39] Most importantly the fires in the Mont Blanc tunnel (March 24, 1999) in which 41 people lost their lives and the one in the Kaprun tunnel (November 9, 2000) in which 150 people perished in the blaze.

[40] Self-reliance meaning the ability of passengers to rescue themselves after an accident.

[41] Integraal Veiligheidsplan IVP.

[42] Ref. Perrow, p. 97

[43] Ref. De Bruin et al 1998, p. 94-98

[44] Ibidem, p. 110-111

[45] Such as increased number of escape doors, better access for the fire brigades and so on.

[46] Examples are the Green Heart tunnel for the HSL-Zuid, the tram tunnel in The Hague, which also serves as a parking garage and the railway tunnel in Rotterdam, on top of which a skyscraper has been build.

[47] The so-called ‘Leeuwendaal studies’, Leeuwendaal, 2001

[48] Ibidem, p. 4

[49] Ibidem

[50] Veiligheidseffectrapportage VER

[51] Milieueffectrapportage MER

[52] Integraal veiligheidsplan IVP

[53] Extension of Schiphol Airport, Maasvlakte 2 near Rotterdam, Betuweroute freight railway to Germany, expansion of the motorway network (A73, widening of the A2 and A4, A5 and second Coentunnel)

[54] Ref. Connekt 2001

[55] Ref. Stoop 2001

[56] Ref. Stoop 1990, See chapter 2.2.5 and 2.3.2

5. What is missing? Case studies

5.1 Introduction

The previous chapters showed that despite the fact of having a number of models, theories, protocols, procedures and underlying risk management techniques, the dynamic element in the design of these systems is not very well addressed. This necessitates a back-to-reality check. This chapter will show the importance of the notion of time as part of the factual behaviour of safety critical systems.

This chapter will answer research question 4: *What methodologies exist, which can be used to improve the situation?* and research question 5: *If existing methodologies are not adequate in dealing with these issues, which improvements are possible?*

The back-to-reality check as mentioned above is accomplished by studying five exemplary case studies covering the field of transportation where safety is at its most dynamic: (light) railways and general aviation. The notion of resilience time will be introduced as a hidden yet determining property of a safety critical system.

The case studies are based on the official accident investigation reports. In general the prime function of investigation reports is societal acceptance of the recommended safety enhancements above scientific purity of analysis and conclusions. The facts as presented in these reports are not put into question, although from a scientific point of view the interpretation of these facts as presented in the reports leaves room for debate. This thesis does not question these facts. It merely puts them in a different perspective.

5.2 Case studies

5.2.1 Hidden dangers: derailment of an Amsterdam metro[1]

April 7, 2008 around 16:57 hrs a metro train derailed just before the terminus at Amsterdam Central Station (metro). The derailment occurred on a scissors crossover, see figures 25 and 26. The initial investigation at the accident site found evidence that the derailment had occurred because the points 201B had changed position at the same moment that the first coach of the four car train passed over them. This surprised everybody involved because the control system was a modern system with interlocking between points and signals. The railway inspectorate had no other option than to order the shutdown of operation at the Central Station terminus until further notice.

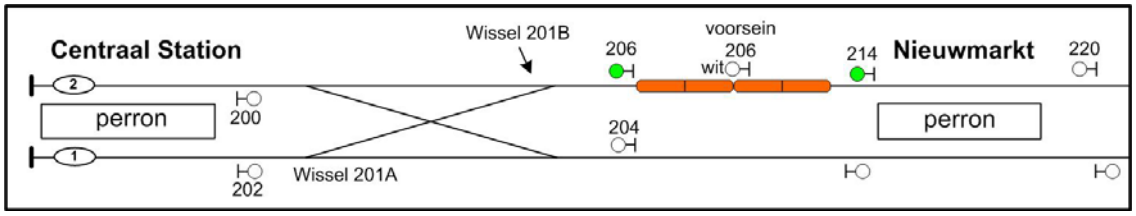

Figure 25. Situation of the accident location. The train was destined for track 2 at the terminus.

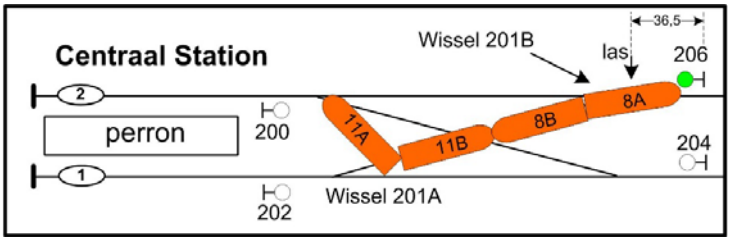

Figure 26. Situation after the accident.

Figure 27. The derailed first coach of the metro train.

Investigation into the cause of the accident by the Railway Inspectorate showed that a false train detection had occurred through stray currents resulting from a failed track section insulation in the two sections behind points 201B (two track pickup system). This immediately released the road ahead of the approaching metro train which should have been locked until that train had passed.
Crossover points 201B and 201A are no longer locked and are reset for the next train by the automatic route setting system because this system assumes that the original train has passed over the points. At the same moment that the train is over points 201B they start moving. The first bogie of the leading coach goes straight on, the rear bogie of the same coach and the rest of the train follow a path towards points 201A and track 1, see figure 26 and 27.
Further investigation showed that there was a blind spot in the system of 36.5 meters between the last signal and the insulated track joined locking the points behind it. It takes about three seconds for a metro train running at 40 kph to bridge this gap.

In these three seconds the false train detection occurred in the two sections behind points 201B without the real train being detected at the location of the points. Once the false detection had been processed by the new automatic route setting system it immediately started setting a new route for the next approaching train.
The gap between the last signal and the points had been there as a result of the signal safeguarding the crossover being moved further away from it sometime in the past. This was necessary because the train protection system ZUB could not always stop a train before a signal. In the original situation a train overrunning the home signal immediately locked the scissors crossover for every train movement including trains wanting to leave the station in the opposite direction. The relocation of the signal prevented this escalation from occurring. What was overlooked was the necessity to move the track circuit forward as well. This was left in the original location.
Two electronic systems were involved in this accident. The oldest was the points and signalling system. Because this was an older system it had a design limitation. It functioned on the basis of two track pickup. This meant that it looked at the two sections behind a set of points. If both sections had shown an occupation and subsequent release the system released itself and freed the locking of the points. This is a conventional railway system used in many places, also on main line railways. Its weakness is that it does not look at the order of the pickup and subsequent release nor the speed at which this occurs.
The other automatic system involved was the traffic management system metro. This was a fairly new system, introduced a couple of years earlier. Before this system was in use, the routes were set manually by means of a relay based entrance/exit system. Manual route setting was a slow process usually taking 5-10 seconds. This overlaps the 3 second gap in the operational system with ease. This became a different story once replaced by an automatic system using digital controllers with a clock cycle of microseconds.
Poor insulating joints can create false track occupations, sometimes resulting in a signal failure. Earlier that same day and the day before a faulty insulating joint in the scissors crossover near points 203B had created signal failures, which had cleared themselves before maintenance staff could check the situation.
When seconds before the accident a train left the terminus at the same time as the opposing train was approaching the Central Station it created a stray current through the faulty insulating joint which influenced the two sections locking the points 201B. Once passed the two offending sections returned to normal. By that time the points and signalling system had received a two track pickup signal from the two sections involved and released the route for a new route to be set by the traffic management system. Immediately a new route was set and instructions were sent to the point control system to changeover points 201B and 201A which it duly executed under the approaching metro train.
It was a freak accident yet it could have happened at other places as well because all four termini of the Amsterdam metro system were thus equipped. The root cause was twofold: there was gap in the detection of an approaching metro train and the software was not resilient enough to deal with faulty two track pickup signals. This placed the railway inspectorate for a dilemma. Would it be wise to wait until the system was reliable again? The consequence was that around 50,000 passengers per day had to be moved above ground using tram, bus and others means such as a car or a bicycle. The inevitable congestion in the Amsterdam city centre would create new risks, possibly resulting in additional road accidents.
The alternative was to accept a workaround thus eliminating the possibility of the scenario to reoccur again. This workaround was quite simple: go back to manual route setting with some additional safety procedures regarding establishing the exact location of an approaching train. Both options were analysed by the railway inspectorate. It was the latter that was reluctantly accepted.

Two days after the accident the railway inspectorate lifted the ban on operation and allowed the trains to run again. Later on the signalling system was modified to deal with faulty two track pickup signals. Also the track circuit was moved forward to cover the gap. The problem has not happened again after that.

5.2.2 Scenario's as deterministic tool: Amsterdam 2004 train collision

Introduction

In analysing complex and dynamic systems their safety performance can be assessed at several levels, based on various numerical indicators such as individual risk or societal risk. A most common and well-established tool for such assessment is the Quantitative Risk Analysis methodology. This tool gained wide application in the Netherlands in civil engineering, particular in the design, construct and operation of major transport infrastructures, flood barriers, coastal defences etc. Based on a series of experiences with tunnel fires, public governance decision-making on risk acceptance and awareness in major infrastructure and transport developments, decision makers and designers are faced with limitations of this QRA approach, such as the limited availability of reliable data and the focus on isolated causal factors.

The advocacy for applying scenarios as an additional decision-making support tool that may counter deficiencies in the QRA concept has several reasons. Recently the public governance risk policy-making strategy 'Coping rationally with risks[2]' has been developed focussing on a layered structure in decision-making. This structure recognises the need for dealing with uncertainty, not only at the level of data analysis but also at the level of scenario definition and the level of methodology. Simultaneously a parliamentary inquiry committee[3] identified several phases of policy decision-making processes that needed new policy-making support procedures and notions for strategic decision-making at a national level.

Case study: train collision at Amsterdam Central Station

The analysis of the train collision at Amsterdam Central Station on the 21st of May 2004 shows a possible scenario designed by a bottom up approach. Figure 29 contains a map of the part of Amsterdam CS where the train collision occurred. Table 1 describes the analysis of the accident chronologically[4]. Statements in italic indicate critical actions that have contributed directly to the accident.

Figure 28. Collision at Amsterdam CS, May 21, 2004. Evidence of time as a critical factor.

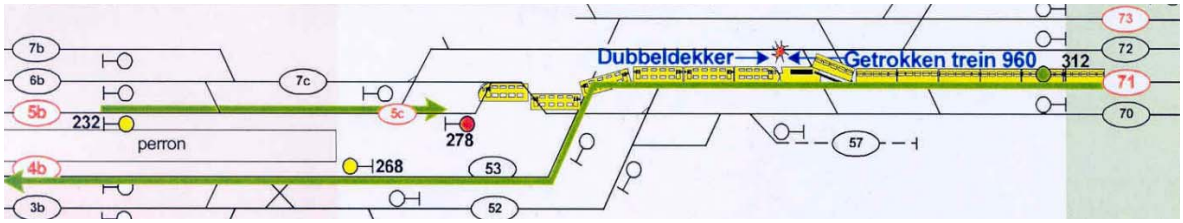

Figure 29. Map of the collision site near Amsterdam Central Station

Table 1. Chronological analysis of the train collision at Amsterdam Central Station

Time	**Intercity 960**	**Empty stock 80761**	**Train dispatcher Amsterdam CS East side**	**TNV (tracking system for trains) and ARI (automated route setting system)**
1974 (A)				***Signalling system: during modernisation at Amsterdam CS, new signal 278 is put in place. Its visibility is poor when seen from track 5c and its location is too close to preceding signal 232. Signalling system: no red-red connection (connection between two signals which are within braking distance of each other) between signals 278 and 232.***
2002 (B)		Driver train 80761 joins the railways as a trainee. ***He has never been instructed about the poor visibility of signal 278.***		
2003 (C)				***Schedule 2004 for trains 960 and 80761 is not according to rules, requiring a separation of at least 5 minutes between these two crossing trains.***
21st of May 2004 18:22 (D)		Train 3560 arrives at Amsterdam CS on track 5b. This train will be moved as empty stock train 80761 to Watergraafsmeer		

		depot.		
18:25 (E)			Train dispatcher returns from dinner break and takes over the shift from his predecessor. There are no problems. ***He omits to change train number 3560 manually into 80761 in the TNV-system.***	TNV-system: Train number 3560 has not yet been changed into 80761.
18:26 (F)	Train 960 departs on time from Amsterdam Amstel heading for Amsterdam CS.			TNV detects that train 960 is on time and forwards this information to the ARI-system.
18:29:50 (G)		Driver train 80761 reports 'ready to depart' to train dispatcher using Telerail[5] (radio system for communication between train drivers and train control centres).		TNV: because train 80761 is not fed into the TNV-system, TNV concludes train 80761 is not ready to depart. This information is forwarded to the ARI-system. ARI-system: no route is set for train 80761.
18:30:00 (H)		Scheduled departure time for train 80761.		***ARI sets a route for train 960 from track 71 (signal 312) to track 4a, using part of the original route for train 80761, which is therefore partially blocked as from now.***
18:30:02 (I)	Signal 312 comes off (shows amber or green aspect and can be passed) for train 960.			
18:31:00 (J)		Signal 232 comes off for train 80761.	Train dispatcher sets manual route for train 80761(known as *00001) from track 5c (signal 232) to track 5b (signal 278).	
18:31:29 (K)		Train 80761 departs from track 5b.		
18:31:44 (L)		Train 80761 passes signal 232 (amber aspect).		
18:31:47 (M)		Train 80761 reaches highest recorded speed: 37 km/h.		
18:31:50 (N)	Train 960 passes signal 312 (green	***Driver train 80761 fails to observe signal***		

	aspect). There are no further signals till track 4b.	***278 at danger (red aspect).***		
18:31:57 (O)		Train 80761 passes signal 278 at danger. There are no further signals till track 74 direction Watergraafsmeer. ***ATB (automatic train control system) does not stop the train because speed is less than 40 km/h.***	Train dispatcher notices SPAD (signal passed at danger) train 80761. ***Train dispatcher fails to report this SPAD to driver train 80761.***	
18:32:00 (P)	Train 960 approaches points 297a/295b.			
18:32:10 (Q)	Train 960 in path between points 283a/281 and 297a/295b.	Driver train 80761 observes train 960 approaching on the same track and applies emergency brakes.		
18:32:11 (R)	***Driver train 960 fails to notice imminent collision and instead applies normal electro-dynamic brakes on loco 1838.***	Train 80761 passes through points 295. Train 80761 in path between points 283a/281 and 297a/295b.	Train dispatcher calls driver train 80761 using Telerail because of SPAD signal 278.	
18:32:12 (S)			Train dispatcher changes train number 3560 in 80761 in TNV.	Train number *00001 changes to 80761.
18:32:13 (T)		Collision between train 80761 and train 960		

In this accident 18 people including the driver of train 960 were seriously injured. Because the collision occurred in the centre of Amsterdam, emergency services were very quick on the scene. However, damaged overhead wires caused severe safety problems resulting in a forced shutdown of the entire station area of Amsterdam CS. Most of the injured people were transported to hospital within 90 minutes of the accident. One passenger was trapped in a damaged intercity coach and could not be reached till 23:30 hrs.

Loco 1838 and the carriage next to it plus the driving power car of train 80761 (a brand new double deck train) were damaged beyond (economical) repair. The entire station of Amsterdam CS, a very busy regional hub, had to be shut down to facilitate the rescue operation, causing immense disruption on the national railway network. It took till 22:00 hrs the next evening before the damaged coaches and the loco were rerailed. Train services on the west side of Amsterdam CS could not be resumed until Saturday morning May 22, when emergency repairs to the overhead power supply system had been carried out.

It took till the morning of the 24th of May before rail traffic was back to normal on the east side of Amsterdam CS, due to the necessity of major repairs to the rail infrastructure and overhead power supply system.

Analysis of the collision
In this scenario, the earlier mentioned accelerations and decelerations can be identified:

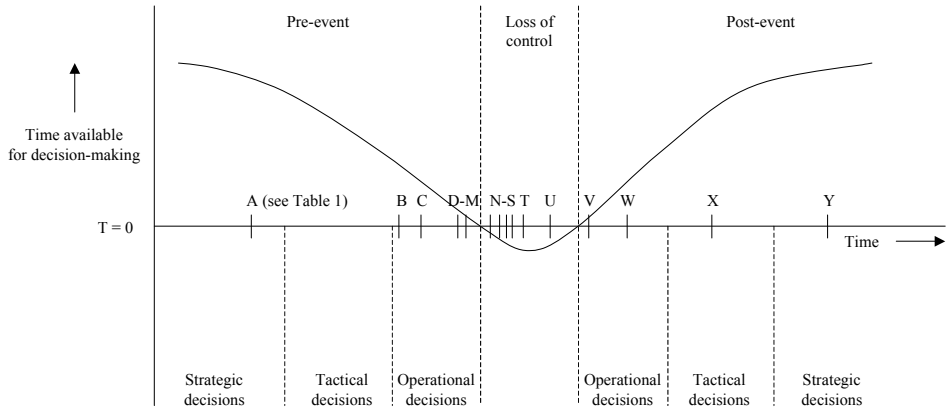

Figure 30. Time line of the train collision at Amsterdam Central Station

It took 30 years before the original design decision at strategic level to install signal 278 without changing the tracks and points resulted in an accident. It took two years before at operational level the flaw in the training of the driver regarding the instruction about the short distance and poor visibility of signal 278 related to signal 232 (figure 31) resulted in an accident.

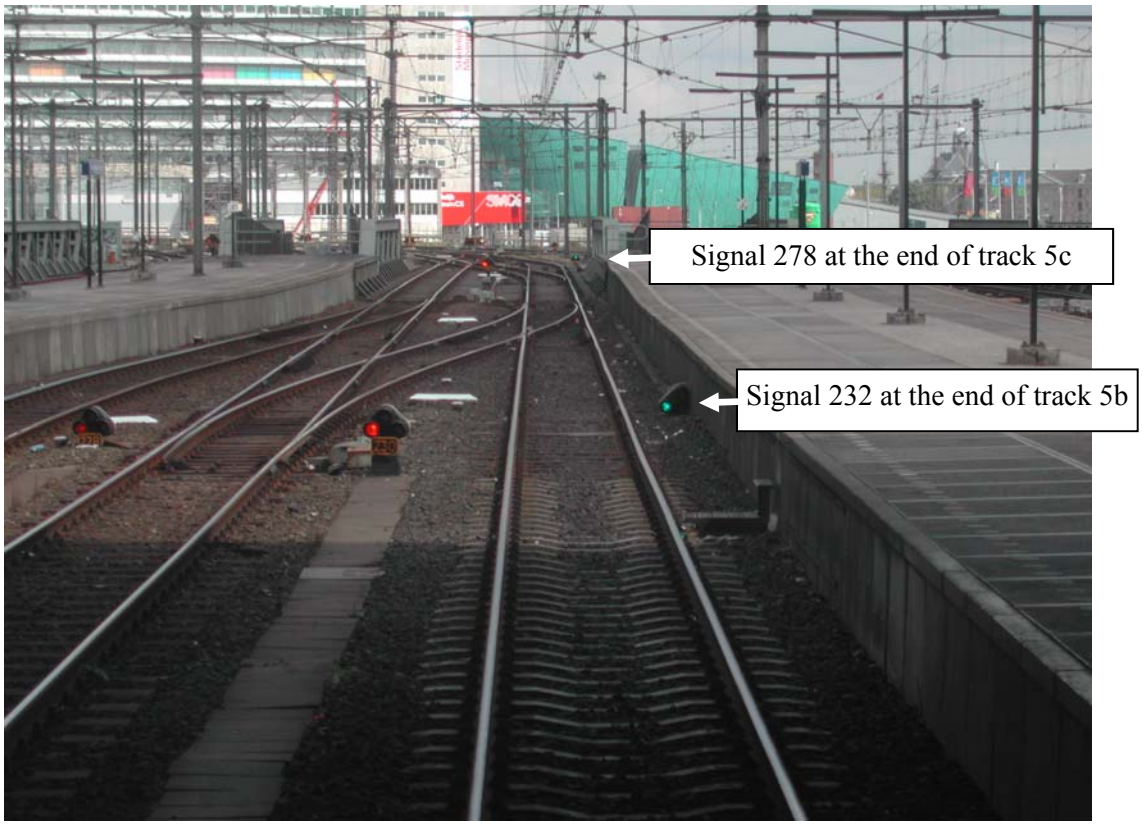

Figure 31. The short distance between signals 278 and 232

On the day of the accident events started to accelerate. The train dispatcher had 4 minutes to change the train number of train 3560 into 80761. After the scheduled departure time of train 80761 the clock started ticking in seconds to disaster. When train 80761 caused a SPAD, both the driver of this train and the train dispatcher had only 6 seconds to react (both failed to do so). After 18:32:02 the collision was inevitable, although it took 11 more seconds to occur.
In the immediate aftermath a deceleration of events is noticeable. At first events moved in seconds, ranging from the crew of both trains reporting the accident to the train dispatcher calling for help (U). The actual rescue operation took 5 hours (V), followed by the repair of the tracks and overhead, which took 3 days (W). The accident investigation at tactical level was conducted over a period of 3 months (X). The political discussions at strategic level were still going on more than a year after this event (Y).
Just after the accident, political reaction was limited at first, despite reiterated claims by the chairman of the Dutch Transport Safety Board that ATB-EG[6] (first generation) was an outmoded system and should be replaced by ATB-NG (new generation) as soon as possible. This was contrary to the policy of the Dutch Ministry of Transport that had decided not to invest any further in modernising ATB, but to replace it gradually by ERTMS/ETCS[7], the new European standard.
This accident at Amsterdam Central Station proved to be the first of a series of rail accidents in Amsterdam within a few years:

- May 21, 2004: collision of two trains at Amsterdam CS east side
- June 6, 2005: derailment of a ballast train at Amsterdam CS west side
- June 8, 2005: derailment of a coal train at Amsterdam CS west side
- August 15, 2005: derailment of an intercity at Amsterdam CS west side

These incidents combined with a head-on collision of two passenger trains near Roosendaal on September 30, 2004 and a sidelong collision between two passenger trains at Rotterdam CS on February 11, 2005 under similar conditions as the original collision at Amsterdam CS, were enough to cause severe political worries as expressed by all parties when questioning the Minister of Transport about a feared reduction in railway safety levels in the Netherlands. A parliamentary study group was established to investigate the maintenance level of the national railway network and the way its administrator, ProRail, functions[8].
By describing the scenario of the train collision at Amsterdam CS in time, the safety critical decisions made by different actors become clear. The insight in these decisions cannot only be used to intervene and prevent another accident. It can also be used to indicate the most important rationale for application of accidents scenarios: a transparency for a system intervention in deficiency identification and mitigation.

Conclusion
Deterministic scenarios prove to have a powerful potential for identifying safety critical decisions, based on the following characteristics:

- Scenarios are narrative representations of potential or actual sequences of events in time, in a specific context and operating environment;
- Scenarios gain insight into safety critical decisions at the strategic level, tactical level and operational level;
- Scenarios recognize accelerations and decelerations of decisions and events in time.

By describing deterministic scenarios in terms of accelerations and decelerations in time, safety critical decisions can be identified. The insight in the safety critical decisions can be used for prevention and system intervention. Based on figure 30, the question arises whether time can be structured as a new deciding factor in decision-making between intervention and comprehension, because tactical and strategic decision-making each have their own specific time span.

5.2.3 Second Amsterdam metro derailment: an open and shut case .... or not[9]?

General

Accidents in large transport systems such as airlines, trains, metros and trams, are always potentially serious. They attract large crowds and quite often make headline news. Transportation systems in the Netherlands are no exception to this. Because the public using these systems are not in control of it (or so they feel), the acceptable level of risk is much lower than comparable systems where they feel to be in control.

In the Netherlands traffic causes at present 750 fatal casualties per year[10]. This is regarded as a very good score, certainly compared to other countries. Indeed road safety in the Netherlands is the highest in Europe, with the exception of Malta. Traffic accidents seldom make headline news, despite the fact that sometimes three people or more die in a single accident. And despite the fact that on average 2-3 people die in traffic each day.

Our railway system on the other hand hasn't seen a single fatal accident amongst passengers since 1993[11]. The two operating metro systems in our country (Rotterdam and Amsterdam) have not seen a fatality since they were opened in 1968 and 1974 resp. Yet accidents in these systems do make headline news, even if only a handful of people get injured. A good example is the Amsterdam train crash in 2004 (18 people injured, 2 seriously wounded) and the recent derailment of an Amsterdam metro in December 2008.

It is through these accidents that the old safety paradigm becomes evident: the better you perform, the more critical the public becomes. It is a societal obligation to investigate these accidents and learn from them to make sure that they do not happen again. This paper will show that accident investigation is sometimes very complicated even when it looks at first to be a simple accident. The roots of an accident can be in place long before it happened or at a totally different location than the crash site.

Case study

Wednesday, December 3, 2008, at 19:42 hrs a metro train of GVB Amsterdam got derailed in the tunnel between Weesperplein and Wibautstraat stations. Nobody was injured, but damage to rolling stock and infrastructure was severe. Because of the serious consequences of this accident and the fact that it was the second serious derailment of an Amsterdam metro within one year the Railway Inspectorate decided to investigate it in depth. The author was the chief investigator in this investigation.

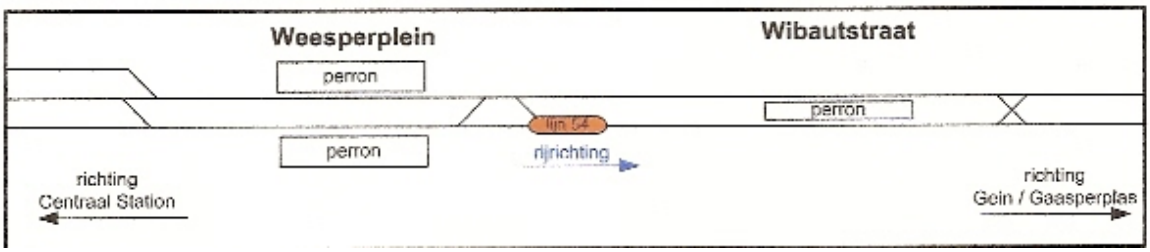

Figure 32. Track diagram of Amsterdam metro at crash site

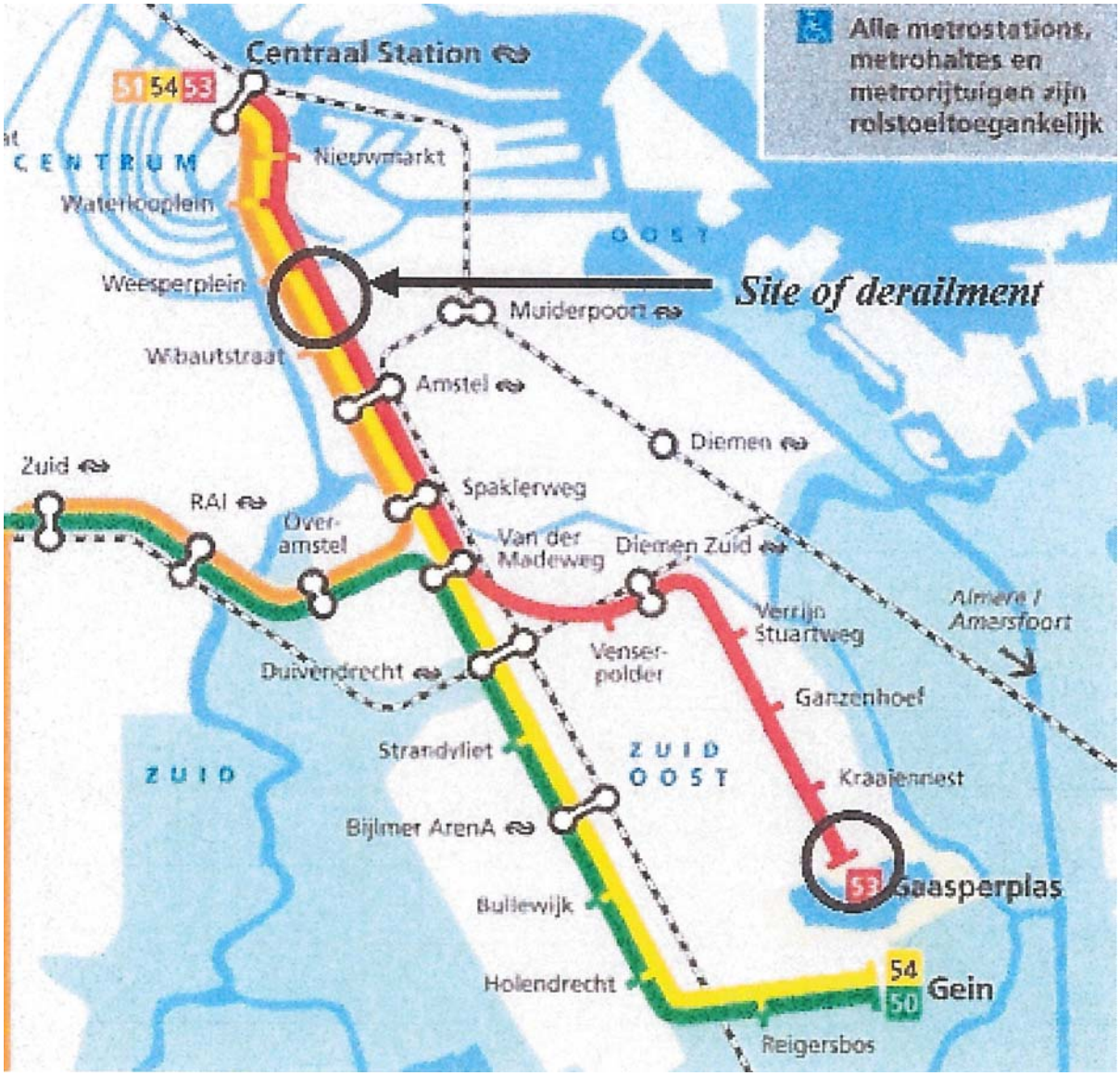

Figure 33. The Amsterdam metro system

During the recent renovation of the infrastructure, guide rails had been inserted in the tunnel section. Because of this the derailed train was held more or less in line, preventing the train from slewing broadside in this wide tunnel as happened in a derailment at Central Station in April 2008. Nobody was injured and all the passengers were quickly evacuated after the power supply had been switched off and the conductor rails had been earthed.

Figure 34. The derailed and damaged front (left) and rear (right) part of the metro

This was the second derailment of an Amsterdam metro in short time. On April 7, 2008, a metro got derailed at Central Station[12] because of a fault in the route setting software, causing points to move under an approaching train. Since then, the entire tunnel section of routes 51, 53 and 54 from Central Station to Amstel Station had been overhauled, including replacement of ballast, track, conductor rails, signalling systems and power supply.
Improvements to emergency systems were introduced as well, such as escape routes with guide lights, fire suppression systems, remote grounding of the power supply and so on. After this second derailment in a year everybody involved was worried. How could this have happened? Was there a design problem? Were maintenance and operating standards not sufficient?
The Dutch Railway Inspectorate was immediately informed of this accident. Two inspectors and the author in his capacity as senior inspector[13] went to the scene. They noticed damage to the track and conductor rails, all probably caused by the derailed train. The train itself showed damage to both front catchers, which were separated from the bogie (figure 35). Furthermore there was damage to the transfer drive between the central motor and the leading axles. Indeed, on the first axle this transfer drive had disintegrated (figure 37).

Figure 35. The dropped right-hand catcher as found (left) and as normally mounted (right)

Figure 36. The dropped right-hand catcher striking a check rail (reconstruction)

Figure 37. The disintegrated elastic transfer drive on the front axle

When interviewed immediately after the accident the driver of the derailed train stated that he felt nothing wrong with his train when he departed from Weesperplein station. His train accelerated normally, until at a speed of around 70 km/hrs. the driver heard a loud bang, followed by a severe shaking of the front section of the train. He also noticed sparks and fire. He was unaware that his train had derailed and thought part of his train had caught fire.
It didn't take long for the inspectors to determine what had happened. A catcher on the front bogie had worked loose and had dropped on the railhead. When it struck a checkrail in a set of points, it deformed in such a way that it obstructed the leading right-hand wheel, causing it to derail. Failure of detecting the lose bolts in the catchers' mounting bracket during routine maintenance was the most obvious cause of this derailment. It seemed like an open and shut case to the inspecting officers. Or was it?
It was clear what had happened, but not why it had happened. These catchers were mounted on the bogie frames using heavy duty bolts with self-locking nuts. Even if for some reason a nut had turned a couple of times, it could not have worked loose. And in the unlikely event of a loose fastening bolt dropping out of the mounting, the catcher would have dropped on the railhead without obstructing the checkrail. The damage to the right-hand catcher indicated an earlier mishap, causing it to deform in such a way that when it eventually dropped down, it struck the checkrail.

The other outstanding question was: why had the transfer drive failed? This was very unusual to happen. In the entire history of these trains since 1974, there were only two earlier occasions of such a mishap to occur. Had it preceded the derailment or was it caused by the derailment? Furthermore bits and pieces were missing. Of the four bolts and nuts with which the catchers were mounted on the bogie frame, only two bolts could be recovered at the scene of the accident. The others were missing. The ballast was fresh, so it was not too difficult to find even smaller parts. Despite an intensive search, the missing bits could not be found in the tunnel.
The only way to find out what had caused this accident was working backwards step by step. This is known as the Achilles method, reconstructing the preceding events, the underlying causes and the circumstantial factors. The other step taken by the inspectors was to reconstruct the failed bogie, in order again to decompose the technical failure mechanism. This is known as forensic engineering. At that time it was unknown if the derailment and the failure of the transfer drive were related or not. It could just as well be two non-related incidents, which happened within short time of each other. Or the derailment could have caused the failure of the drive or vice versa.
An inspection on foot through the entire tunnel section preceding the accident by an inspector and a safety officer of GVB showed no sign of a possible obstacle that could have struck the catcher and cause it to deform as it was found. As a precaution, the Railway inspectors ordered GVB to check the mounting of al catchers on this type of metro stock. No problems were found on the cars thus inspected.
Two days later the train was inspected in the central works of GVB. The inspectors decided first to reconstruct the train after thorough inspection and fact finding. It became clear that the damage to the underside of the front bogie was far more severe than originally thought. This damage could not be explained by the derailment.
Apparently some time before the accident another mishap had occurred with this train set. Either this mishap had been unnoticed or unreported. The question was: what had happened where and when? There was not a single clue that could answer that question, or were the inspectors overlooking evidence?
During the investigation in the workshop, a GVB permanent way inspector reported damage to a buffer stop at Gaasperplas terminus. Apparently an as yet unknown metro train had crashed into it, causing it to move substantially. The offending metro was nowhere to be seen, neither was it known when it had happened apart from the fact that it must have occurred since the previous inspection a couple of days earlier.

Figure 38. The damaged buffer stop at Gaasperplas terminus; notice the gap in the track

Only minutes after arrival at the scene of this (second) accident, the whole puzzle became clear to the inspectors. This was because vital clues were found: bolts and nuts matching the missing pieces of the catcher mountings and the impression made by the anti-climbing devices on the front buffer of the trains. The red colour of the wooden buffer beam matched red paint found on the front of the damaged metro car.

Figure 39. The red paint on the anti-climbers on the buffer beam and on the buffer stop

Figure 40. The gap in the track caused by the collision with the buffer stop

The sequence of events as reconstructed by the Railway inspectors was as follows. Three drivers were involved.

At 18:09 hrs, Wednesday, December 7, 2008, driver 1 arrived with his train at Gaasperplas terminus. He was requested to park his train on tail track 4 at the terminus.

At 18:11 hrs, driver 1 moved his train into this siding. He failed to stop in time and hit the buffer stop with such a speed, that the sheer bolts broke off and the whole buffer stop assembly moved over a distance of approximately 80 cm. The front bogie of the leading car was standing on the stub track connected to the buffer stop. The rest of the train was still standing on the track. Apart from the (minor) damage to the buffer stop, no real damage had occurred at that moment.
The driver then set his train back, contravening GVB regulations. During that unauthorized movement, the leading bogie had to cross the gap in the track. It was this rerailing action that caused the damage to the bogie. In order to bridge the gap, the wheels had to drop considerably. This vertical movement of the axles caused the catchers to strike the railheads. The gearboxes and transfer drives struck a concrete slab, functioning as a walk path between the tracks. Surprisingly, the metro train did not derail during this unauthorized movement. The first driver walked away without reporting this accident or his subsequent actions.

At 19:07 hrs, driver 2 was requested to bring the metro train forward to the station and hand it over to his colleague, driver 3. He duly did so, without noticing anything wrong with the train. Everything operated normally when he switched the train on. Driver 2 could not inspect his train on the outside, because of the live conductor rails at the terminus sidings.

Driver 3 left Gaasperplas at 19:12 hrs to drive as route 53 to Central Station. Nothing unusually happened during that run. At 19:36 hrs, driver 3 left Central Station as route 54 destination Gein. He arrived at Weesperplein at 19:40 hrs and left again a minute later.
When the train approached the set of points between Weesperplein station and Wibautstraat, approximately 19:42 hrs the transfer drive of the front axle failed because of the damage sustained earlier during the accident at Gaasperplas. The vibration resulting from this failure caused the remaining bolt stubs with which the catchers were still hanging from the bogie, to drop out. The catchers dropped down, causing the right hand catcher to obstruct the right front wheel, resulting in the derailment.

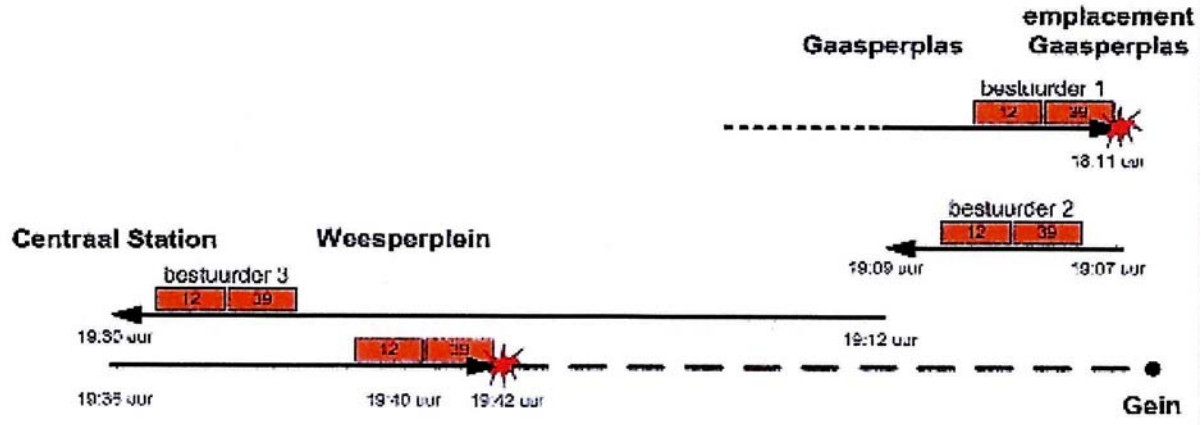

Figure 41. The sequence of events preceding the derailment

This sequence of events was corroborated by evidence from surveillance cameras at the terminus and other evidence found at the site, such as scratches on the concrete walkway which matched the damage found on the disk brakes and the transfer drive on the front bogie of the derailed metro set. The camera pictures showed the train arriving at track 4, stopping and setting back in three short moves. Two minutes later, driver 1 was seen leaving the train.

No record existed of any message or report left by him at that time or shortly afterwards, reporting the accident (hitting the buffer stop). He left the scene of an accident unauthorized. When challenged with the evidence he denied at first being involved, but later admitted that he might have had an accident with some metro-train. He was eventually accused of culpable negligence and sacked by the company.

Lessons learned from the Amsterdam metro derailment

First lesson

Several lessons have been learned from this accident. The most important lesson is that the accident showed to be far more complex than at first thought. In fact, it was a set of two accidents, with two different locations and three drivers involved, spread over nearly two hours' time. Indeed, the accident was already developing when the system seemed to be behaving normally. This is not unusual for such risk sensitive systems.

Their behaviour is shown in the following diagram as developed by Beukenkamp:

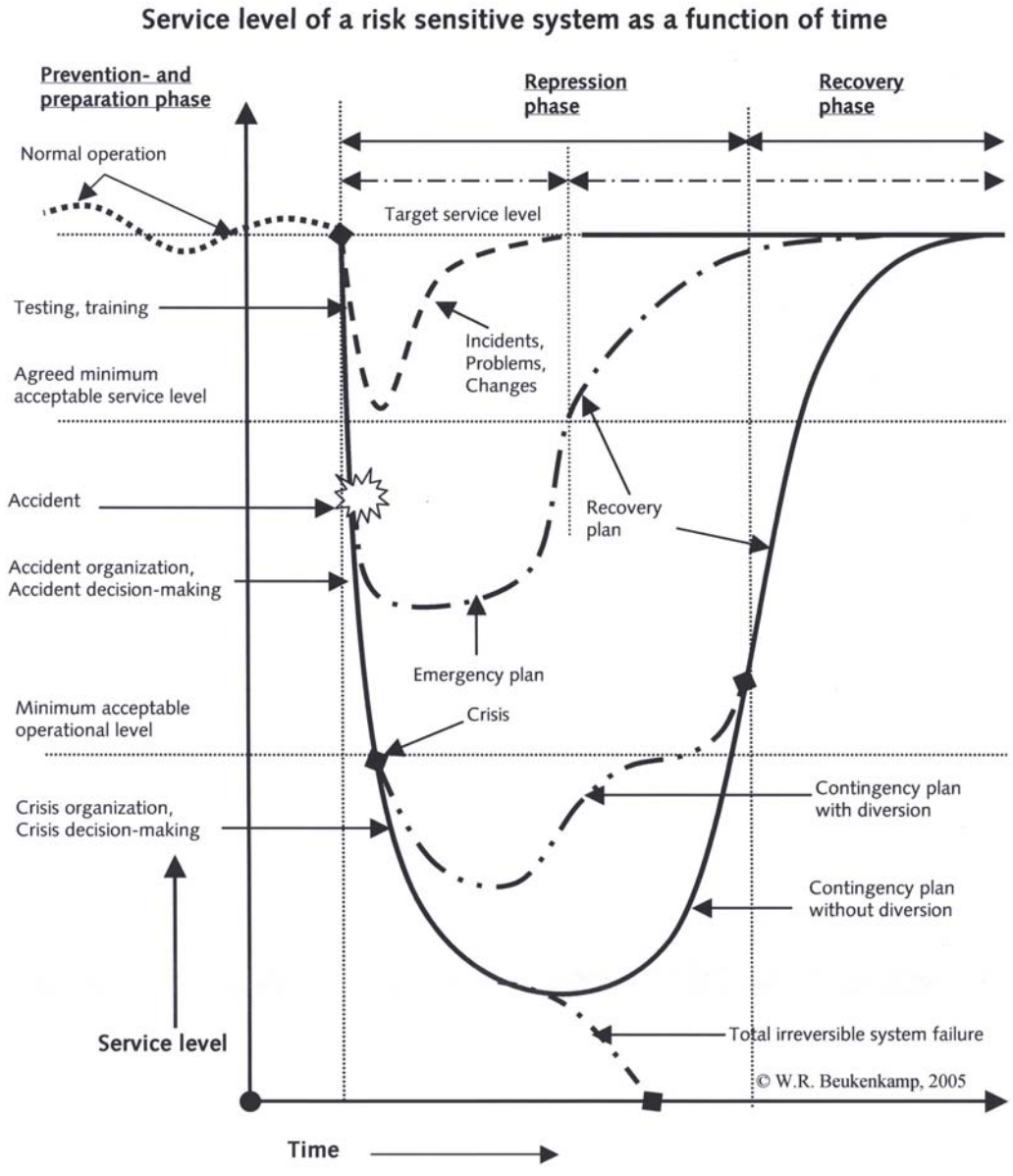

Figure 42. Behaviour of a risk sensitive system as a function of time

As happened to the Railway inspectors in this case, it is tempting to stop the investigation at the moment of the apparent accident, because at that point it is clear what has happened. It is the first moment where it is apparent that the system is behaving abnormally. Judicial enquiries are infamous for this, because it is difficult to administer individual responsibilities when a group of people is involved.
The outcome is that often the driver in the seat, who is the last in de chain of events, gets accused of wrong doing. Even if this is true, often the situation is such that he is trapped, in other words: the behaviour of the system guided him to his mistake instead of preventing this.
It is therefore necessary to go back to the last moment where the system can be proven to have behaved in a normal way. That is not the moment its performance dropped under the agreed minimum service level, but much earlier when its performance started a downward trend.
That moment could actually be at a level where a system is performing better than specified. In other words: if you don't know the origin of the accident, an investigation into its causes runs every risk of leading to wrong or insufficient answers! In this case, the investigation had to stop at the moment of the first accident, the metro hitting the buffer stop. What could not be investigated is why the metro hit the stop in the first place. Was the track slippery? Was the driver driving too fast? Was he intoxicated? Also the behaviour of the driver was unusual. Why did he run his train backwards without authorisation? Why did he not report the (minor) accident? Was he suffering from mental problems? Were there problems at home involved? All these questions remain unanswered, because the driver refused cooperation[14].

Second lesson
The second lesson: when to start the investigation at which pint in the accident process as derived from first lesson is that it is difficult to determine both the start and the end of an investigation. How far back do you go and how far back do you have to go? Do all questions need to be answered? Sometimes the factual crash site can be far larger than originally thought of. Air crashes are most of the times limited to a couple of km around the point of impact. Yet the point of origin of an accident can be located on a completely different continent.
Railway accidents show a similar picture. A clear example of this is the recent derailment of a container train west of Utrecht[15]. This train departed from Rotterdam and was travelling to Germany. At Harmelen the 12th wagon of the train derailed. In total 5 km of nearly new track (it had been relayed only last year) was destroyed, disrupting traffic for more than a week on this very important railway corridor. It is possible that the root of this accident can be found in Germany, before the train left for Rotterdam a day earlier.
A similar incident happened in Britain[16] when in 2006 a stone train left a quarry in the Mendips in the southwest and travelled to Oxford. One of the axles had two wheels with severe flats, caused by an uncontrolled wheel slip during the descent on the track leading from the quarry to the mainline. These two flats pounded 250 km of track (both rails!) to such an extent that track failures occurred immediately under the train or within hours of the train having passed, resulting from cracked rails.

Third lesson
The third lesson learned is that what looked like a technical problem (failure to secure the bolts of the catchers) turned out to be a severe case of human misbehaviour resulting from error. Some investigation methods focus on the technical behaviour of complex systems. Others turn their sight on the human factor. The method chosen by the investigators depends on such assumptions.

This case shows that an open mind, regardless of the method chosen, is necessary in order to determine the sequence of events. Indeed, in general, the subconscious assumption persists that professionals don't show such behaviour. And fortunately in most of the cases they don't! They can and do make mistakes though. They can be overwhelmed by the situation because of lack of information or training. But yes sometimes professionals can behave in a criminal way, when they put their own interests before that of the passengers entrusted to them. This puts the impartial accident investigation into a difficult position.
The main purpose of accident investigation is to learn from what happened to prevent repetition. Under Dutch law (like in many other countries) anybody involved is obliged to cooperate with the investigation. The evidence thus collected cannot be used against the witnesses (blame free investigation).
If there is even a remote possibility that the investigation is turning towards a judicial investigation, every witness must be cautioned and he or she is no longer obliged to give evidence incriminating his or her self. And this can hamper the investigation severely.
That is the main reason why the investigation into the second metro derailment had to stop at the moment the metro-train hit the buffer stop at Gaasperplas. All the evidence collected indicated the possibility of criminal action by the first driver. From that moment on he had the right to remain silent and he exercised that right. The only person who knows why the metro hit the buffer stop is this driver. And as long as he will remain silent, the riddle remains unsolved.

Conclusion
The Amsterdam metro derailment showed how a relative simple accident could turn out to be far more complex than thought at first. At the site of the crash it was unclear if the investigators were dealing with one or two incidents and what if ever their relation was. It was also surprising that the factual crash site was much larger than initially expected. It stretched over a substantial part of the metro system. And it spread over a much larger time span, involving not one but three drivers. To explain the sequence of events, the starting point of the mishap had to be found. Reversing the process and at each step asking the question why and how this could have happened, known as the Achilles method, assisted in this process. Also, reversing the technical failure process through forensic engineering proved vital in solving this case.

5.2.4 Colliding concessions in Amstelveen, 2008[17]

October 17, 2008 a GVB tram on route 5 from Amsterdam Central Station to Amstelveen ran into a Connexxion bus on route 175 from Amsterdam Bijlmer to Haarlem. The accident happened at a busy road junction in Amstelveen south of Amsterdam near the terminus of route 5. The tram derailed, the bus smashed twice into an office block, see figure 43. 13 people got injured, four of them severely including the bus driver. There was major damage to both vehicles, the road crossing and the office building. Because of the severe consequences of this accident the Railway Inspectorate decided to investigate it in depth. The author was the chief investigator in this investigation.

Figure 43. Situation in Amstelveen after the accident. (Picture Parool/©E. van der Marel)

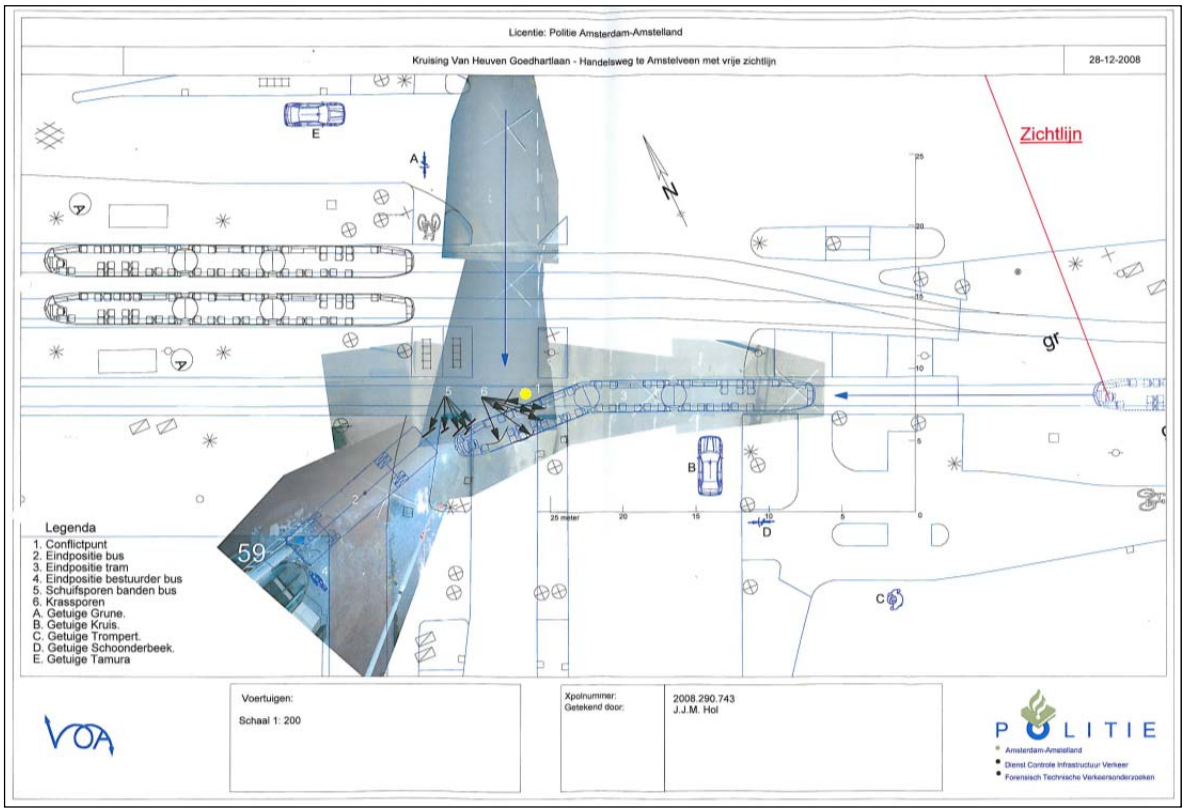

Figure 44. Position of the vehicles and their lines of movement. Courtesy Amsterdam Police

Investigation by the Railway Inspectorate showed that the accident was caused by the tram driver ignoring a red signal. The underlying causes were more interesting. The road junction was a very busy junction with priority conflicts. Tram route 5 was a part of a heavy suburban rail system having top priority at every road junction along its route. Every junction except this one, only a few meters away from its terminus just behind the junction.

The reason for this exception was that at the time this junction was also being used by the Zuidtangent (now R-Net) heavy express bus system routes 300 and 310 from Amsterdam Bijlmer to Haarlem and Nieuw Vennep respectively. On top of that the regional bus route 175 also used this junction. Only 500 meters away was the Amstelveen bus station, which served as a time check point for punctuality. The terminus of tram route 5 also served as a time check point for punctuality.
Tram route 5 was part of the regional tram and bus concession for Amsterdam and surroundings, operated by GVB. The Zuidtangent was part of a dedicated provincial concession, operated by Connexxion. Bus route 175 was part of a regional bus concession, also operated by Connexxion. Analysis of the time tables (see table 2) showed that neither of the three concessions took into account possible time table conflicts with other concessions. There was no risk analysis of the viability of the concession requirements. In fact at this location in some cases six times per hour trams and buses were approaching this junction at almost the same time fighting for priority and trying to keep time. The Railway Inspectorate concluded that it was disaster waiting to happen.

Table 2: Arrival time windows of tram route 5, bus route 175 and bus route 300 at the accident location according to schedule. A = coming down from Amsterdam; B = going towards Amsterdam.

	Tram 5A	Tram 5B	Bus 175A	Bus 175B	Zuidtangent 300A	Zuidtangent 300B
.00						
.01						
.02						
.03						
.04						
.05						
.06						
.07						
.08						
.09						
.10						
.11						
.12						
.13						
.14						
.15						
.16						
.17						
.18						
.19						
.20						
.21						
.22						
.23						
.24						
.25						
.26						
.27						
.28						
.29						
.30						

Solution was found chiefly by rerouting Zuidtangent routes 300 and 310 away from this junction. This left tram route 5 as the only top priority system which it now had full time just as on the remainder of its route. GVB paid more attention to training its tram drivers regarding this busy junction and similar junctions. The same applied to bus operator Connexxion.
There was one other noticeable aspect. For many years the standard colour of public transport vehicles in the Netherlands (trains, trams, buses and ferries) had been bright yellow, a colour that is also used for safety reasons in many situations such as safety vests. When public transport was privatised in the mid-nineties of the last century, this standard was abandoned and company liveries were reintroduced. In the course of this Amsterdam transport rolling stock became overwhelmingly white with a blue band. The office buildings south of the junction on the approach of tram route 5 were also white, thereby camouflaging the trams when they were near the junction.

Figure 45. The tram not showing much contrast (especially with an autumn sun just behind it).

5.2.5 Sliding trains in Leiden Centraal[18]

It is not enough to equip systems with a fallback option. They need time to become fully operational. If that time is not available they are of no use as this case will show. There were six train collisions at Leiden Central Station between 2008 and 2012. In each case trains of Dutch Railways (NSR) were involved:

- October 21, 2008: collision between a train and a buffer stop on track 502. No casualties, damage to rolling stock and infrastructure.
- November 23, 2008: collision between a train and a buffer stop on track 502. No casualties, damage to rolling stock, no damage to the infrastructure.
- November 1, 2010: collision between a train and a buffer stop on track 515. No casualties, damage to rolling stock and infrastructure.
- November 5, 2010: collision between a train and an empty train on track 502. Eight passengers injured, damage to rolling stock, no damage to the infrastructure.
- November 28, 2011: collision between a train and an empty train on track 502. Three passengers injured, damage to rolling stock, no damage to the infrastructure.

- April 17, 2012: collision between a train and an empty train on track 502. No casualties, damage to rolling stock, no damage to the infrastructure.

Because of the repetition of these accidents the Railway Inspectorate decided to investigate them in depth. The author was the chief investigator in this investigation.

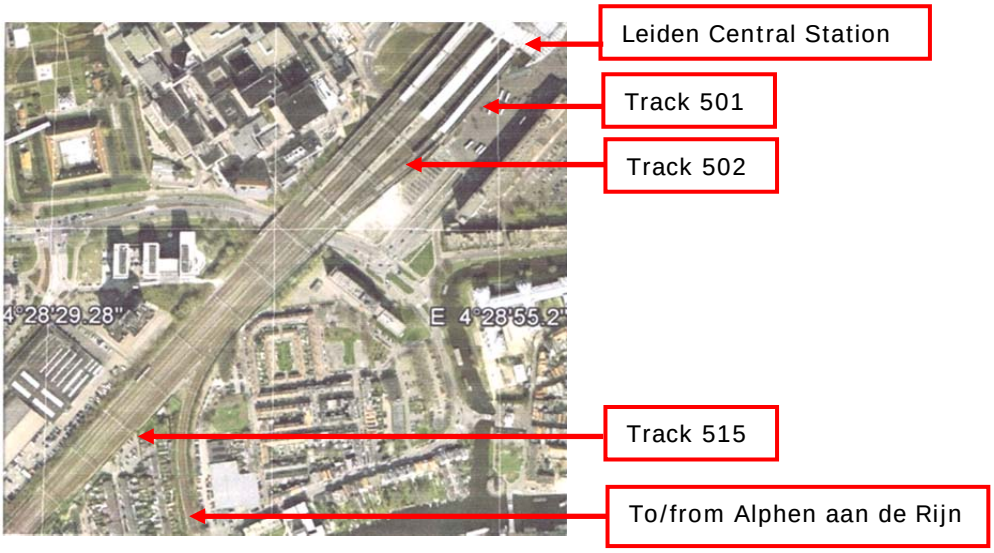

Figure 46. Situation at Leiden Central.

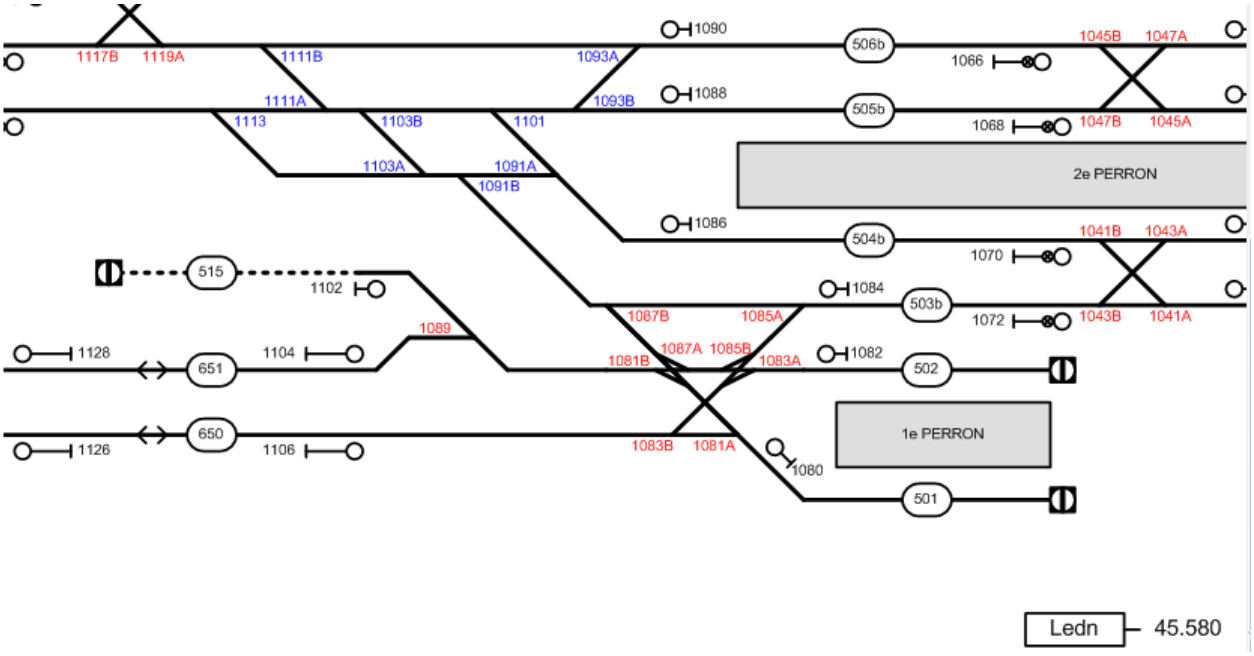

Figure 47. Track plan at Leiden Central (only the relevant part of the station is shown)

The investigation by the Railway Inspectorate into these accidents showed a number of serious deficiencies in the rail system at Leiden. The infrastructure manager ProRail failed to regularly clean the tracks which were susceptible to contamination from air pollution (soot from buses using the bus station next to the railway station) and a rail conditioner in the curves approaching Leiden from Alphen aan de Rijn. However, the main cause of the accidents was found in the design and operation of the rolling stock involved.

Except for the November 23, 2008 accident, in each case the rolling stock consisted of a first generation Sprinter class two coach electrical multiple unit (emu) type SGMm. These trains

were built between 1975 and 1980 as two car emus. In 1983 a number of them were lengthened to three car formation.
The three car sprinters were overhauled and modernized by Bombardier (Randers) between 2003 and 2006. Subsequently the two car emu's were also overhauled and modernized by Bombardier (Randers) between 2007 and 2008.

Figure 48. Sprinter type EMU class SGMm in two coach formation (SGMm-II).

From the beginning they were showing problems with braking in low adhesion conditions. As two car emu's they were equipped with motor bogies only with disk brakes. Braking could be done either using the pneumatic brake or a combination of electro-dynamic (ED) braking (using the generating force of the traction motors as brake) and pneumatic brakes at lower speeds. When a non-motored third coach was inserted as center section, this coach was equipped with pneumatic operated disk brakes only. The braking system was therefore modified in these units from electro-dynamic to electro-pneumatic (EP).
The critical point in their braking occurred around the speed of 10 kph. This is the speed where the ED-brake has to give over to the pneumatic brake to stop the train because the braking current has dropped to such a level that it is no longer slowing down the train. The activation of the disk brakes can result in a potential lock of the brakes under conditions of low adhesion. To counter this an anti-locking system has been provided that temporarily releases the brakes when a wheel lock is detected, after which the pneumatic brakes are applied again.
There have been a number of occasions where the sequence of brake application – wheel lock – brake release – brake application resulted in another wheel lock and repetition of the sequence. Or the wheels did not start to roll again after release of the brakes because the adhesion was too low to spin them up.
Earlier tests by Dutch Railways showed that the deceleration rate under conditions of full wheel lock is a factor 10 less (sliding friction) than under conditions of rolling friction[19]. The braking distance will increase by the same amount. The three car version of these emus did not suffer as badly as the two car version because the center (non-driving) coach only uses the pneumatic brake which is applied continuously, thus braking the train (even at reduced capacity) in case the motor bogies are locked.

In the Leiden collisions each time the trains started to slide at low speed at the end of the platform. Given the relative short length of the platform between tracks 501 and 502 there was simply no reaction time available to facilitate a recovery of the braking system. This became more critical when the available track length had been shorted because part of it was occupied by an empty train. Worse: analysis of the on board train monitoring recorder (ARI) showed that in at least three accidents the braking system was actually oscillating out of control: brake application – wheel lock – brake release – brake application – wheel lock – brake release et cetera.
To improve their braking characteristics in 2013 the three car SGMm sprinters were equipped with magnetic track brakes in the non-motored center bogies. Unfortunately it turned out to be very difficult to fit track brakes to power bogies.
Summary of findings:

- Difficult approach to the tracks in question, necessitating the application of power until the train is close to the platforms;
- Failure to combat pollution of the rail head;
- Maintenance problem with a nearby rail conditioner;
- Absence of magnetic brakes on the EMU's of the SGMm-II type;
- Interference by the anti-slip system of the EMU's of the SGMm-II type with the braking system during transition of electro-dynamic braking to pneumatic braking.

At present studies are still going on towards finding a solution for the SGMm-II fleet. One temporary solution is only operating them coupled to a three car sprinter when there are conditions of low adhesion. Sometimes these conditions can be predicted such as autumn leaf fall. However, Leiden showed that at other times these conditions occurred unexpectedly. These sprinter emus can become unstable and therefore risk critical under conditions where scenarios apply that result in situations where the available recovery time is less than the required recovery time as is shown in figure 41 (see below).

5.3 Time as a hidden critical factor

5.3.1 Acceleration and deceleration of decision making

Both quantitative and qualitative risk analyses contain scenarios as a tool for risk assessments. However, an important difference between the scenarios of probabilistic analyses and the scenarios of deterministic analyses is time. In a QRA the factor time is part of the stochastic distribution of events and as such cannot be influenced (dependent variable). Statistics are in fact static in time and ignore the dynamics of decision making.
The scenarios of a deterministic approach describe accident processes (loss of control) of potential or actual sequences of events in time as an independent variable, in a specific context and operating environment. Let's take a look again at the way time is a critical factor related to accidents (see §5.2.2 and §5.2.5).

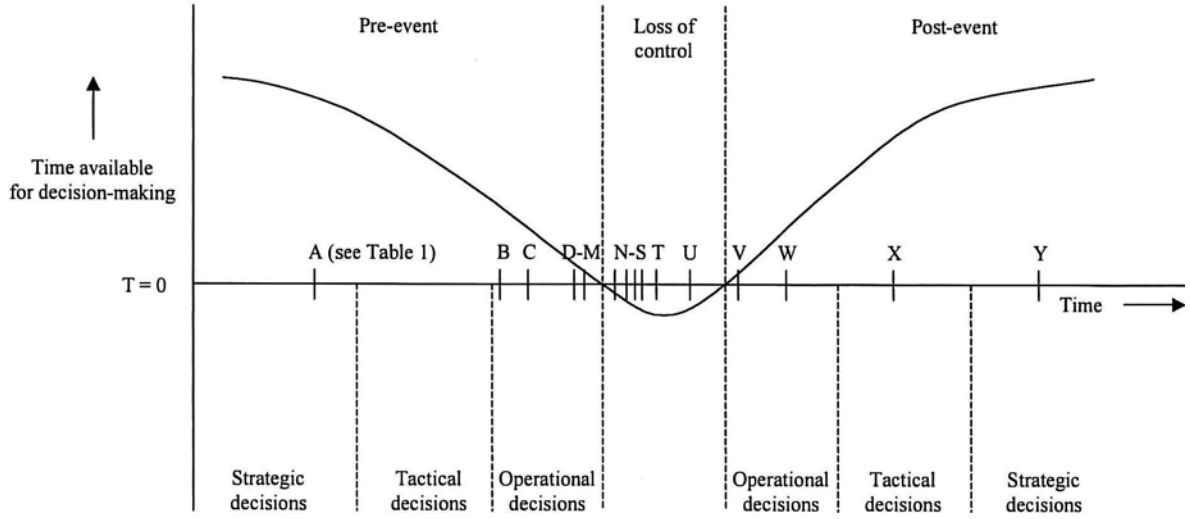

Figure 49. Time as a critical factor in relation to accidents

Figure 49 shows that pre-events and post-events are characterized respectively by accelerations and decelerations. Events before the loss of control are characterized by accelerations, which means that the time available for decision-making is shortening in time. In the loss of control situation, the time available for decision-making is less than the time required.

After the loss of control situation (sometimes culminating in an accident or near miss/near hit), the time available for decision-making lengthens. This deceleration in time will be explained in the situation of someone having a heart attack. Immediately after the heart attack (loss of control) the time available for decision-making is very short. Decisions have to take place at the operational level, because there is no time available to diagnose the problem. And they have to be made quickly because every second counts.

Examples of operational decisions are dealing with a person with acute cardiac arrest. The first action is calling the emergency services through1-1-2. After that the first aider starts applying Basic Life Support (resuscitation) to prevent the victim from dying. Resuscitation does not cure the problem, it merely helps to gain time, to postpone a total collapse of the body functions resulting in fatal damage to the vital organs and death. Sometime later the emergency services arrive. They will make decisions on a higher tactical level to make sure the patient reaches the hospital alive. When the patient arrives at the hospital, the medical staff has to make strategic decisions in the long term about the rehabilitation of the patient.

At each of these decision making levels, safety critical decisions have to be made by different actors. In the example of the heart attack, an arbitrary person can decide to resuscitate the person. In that case qualified knowledge to intervene depends on coincidental presence of experts at the accident scene, such as doctors or rescue workers. This is an event driven response instead of proactive and planned incident handling. Tactical and strategic decisions about medical assistance have to be made by medical experts. Their expertise should be incorporated in the systems design. Although decision-making takes place at different levels, the decisions do influence each other. Decisions at operational level, for example, cannot change earlier decisions made on a higher decision-making level. So decisions at strategic level do effect later decisions at lower decision-making levels.

Deterministic scenarios are time dependent and therefore capable of showing accelerations and decelerations of events. Deterministic scenarios can be designed in two different ways:

- Top down or prospective design means that the scenarios are derived from a decomposition of the system. Engineers and designers have insight into the structure and the content of the system and can define intended and foreseen complexity, interactions and interfaces. The scenarios can be used as a conceptual design tool to remove hidden deficiencies before they lead to accidents and incidents. These top down or prospective designed scenarios can be defined as a 'technical construct'.
- Bottom up or retrospective way of designing scenarios. Scenarios resulting from accident analyses of existing analogous systems are derived by this way of designing. During accident analyses learning from proven deficiencies in order to prevent their recurrence becomes possible. These bottom up or retrospective designed scenarios can be defined as a 'technical reconstruct'.

Besides these physical scenarios, accidents are also located in a policy decision-making environment constrained by the political arena. The policy decision-making environment is characterized by accelerations and decelerations as well. This became very clear during the 1992 Amsterdam Air Disaster. On the 4th of October 1992, an Israeli El Al cargo plane crashed into an apartment block in Amsterdam Bijlmer resulting in at least 43 people killed. During the following months, hundreds of people complained of health problems.
For a number of years the Dutch government kept silent about details of the crash and the contents of the cargo. However, in October 1998, after it was revealed that the crashed plane contained barrels of toxic chemicals, the Dutch House of Representatives set up an inquiry committee to investigate the crash in a broader perspective (Commissie Bijlmerramp). It was eventually determined[20] that the reported health problems were due to the airline illegally carrying dangerous chemicals as well as a large quantity of depleted uranium, the latter being legal, because depleted uranium was commonly used as balancing weight to stabilize airframes such as the 747. The policy decision-making environment finally ends in April 1999 after the report was published that resulted from parliamentary inquiry that investigated what went wrong after the accident and why[21]. The aftermath covered seven years, resulting in revisions of aircraft design, airport operations and governmental oversight over air carrier flight performance.

5.3.2 Time criticality as a hidden system property: Resilience time

As has been identified earlier in this thesis the operational necessity to changeover from normal operation to a fall back strategy (see 5.2.3 figure 42) requires a set of preconditions that needs to be incorporated into the systems design:

1. Identification of possible failure scenarios.
2. A fall back strategy for each scenario identified as high risk.
3. Competent systems control (operator, automatic) to put the fall back strategy into operation.
4. Time to identify the problem.
5. Time to select a fitting fall back strategy.
6. Time to switch over from normal operation to emergency mode.

To make the notion of time criticality more apparent it is necessary to introduce a new notion: 'Resilience time' ($T_{resilience}$). Resilience time is defined as the difference between the available reaction time and the required reaction time, see figure 49 §5.3.1:

$$T_{resilience} = T_{available} - T_{reaction}$$

Given each identified scenario the system is inherently stable when $T_{resilience} >> 0$. The system functions in a resilient state.
The system becomes increasingly vulnerable and unstable when $T_{resilience}$ approaches 0.
The system becomes critical when $T_{resilience} = 0$.
The system is out of control when $T_{resilience} < 0$.

Example: a ship equipped with lifeboats and life rafts is no good if it takes 30 minutes to deploy them if the ship can capsize within 15 minutes. On the other hand in case of a breach in the coastal defences if it takes a two days before the water level in a specific area reaches critical height and it takes less than a day to evacuate the inhabitants, there is no real safety problem.

Resilience time is amongst other things dictated by the speed at which an actor goes through his decision making processes regarding a possible recovery of a system after a mishap. This makes it necessary to go deeper into the role of decision making by human operators as explained by Rasmussen, se the next paragraph.

5.3.3 Human behaviour according to Rasmussen

In 1983 Rasmussen introduced his layered model to explain human behaviour[22].

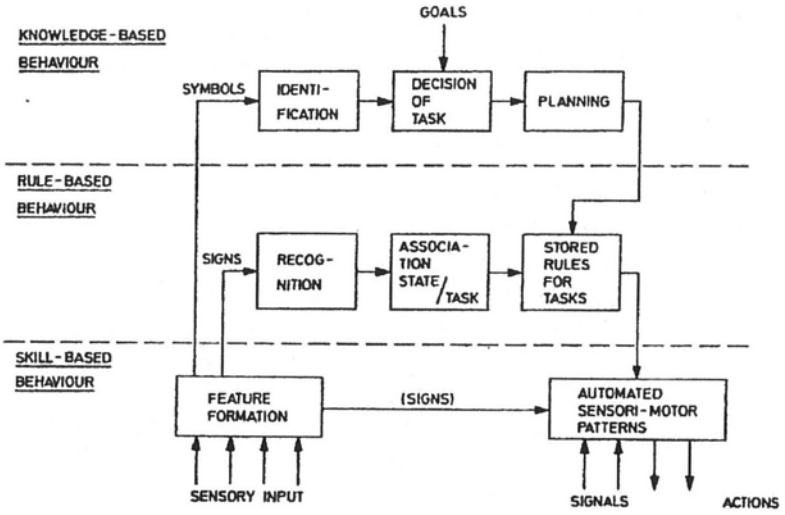

Figure 50. Rasmussen's model relating to three levels of performance of skilled human operators. Note that the levels are not alternatives but interact in a way only rudimentary represented in this figure.

Rasmussen argues that it is important that the operator acts at the correct (mental) level in order to avoid errors. Errors such as resulting from skill-based behaviour where rule-based or knowledge based behaviour should have been applied because the problem is more complex than the operators thinks. Or vice-versa knowledge based behaviour resulting in reinventing the wheel (slow reaction, wrong solution) where the problem is in fact straight forward and should have been solved at skill-based level (quick reaction).
Although the Rasmussen model appears to be dynamic, in practice it is to some extend static because it ignores time as a critical factor. If the model is combined with the notion of resilience time, it can be shown that reduction in resilience time more or less squeezes the Rasmussen model downwards, first blocking knowledge based behaviour, even if that should

have been the preferred behaviour and subsequently forcing the operator into skill based behaviour, thereby hoping that the has the right skills to save the system.
The Rasmussen model however contains a hidden time aspect. The more complex the decision making process is the more time it requires. This relationship is not linear but exponential because the number of possible strategies increases exponentially when you move from skill-based behaviour (usually one preferred action) through rule-based behaviour (finite number of pre-set strategies) to knowledge based behaviour (sometimes almost infinite number of possible strategies).

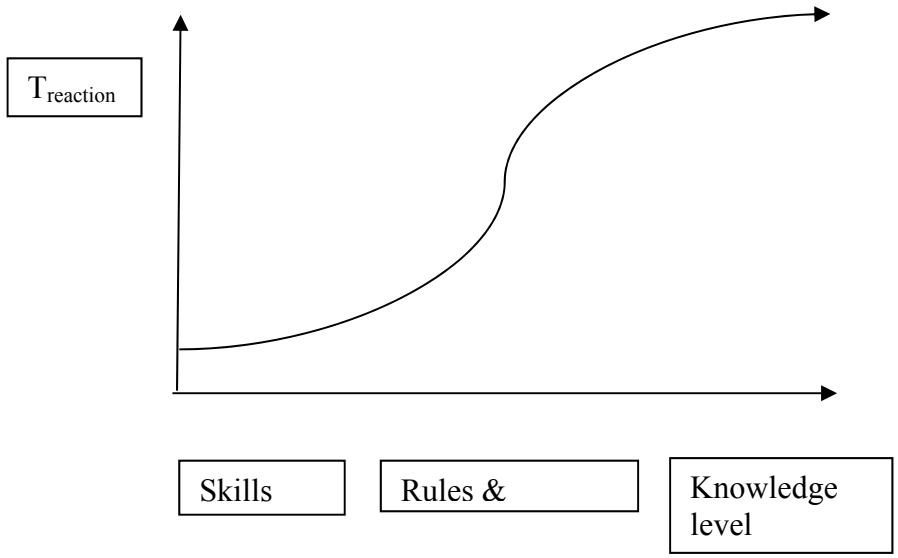

Figure 51. Relation between the reaction time and the level of decision making according to Rasmussen

The factual time depends on the level of activities at which the skilled person functions, see the AVV/WAI diagram figure 7 §2.4.3. Decision making at Macro level (policies level) varies from years to weeks and very occasionally days or hours (national or regional emergency). Decision making at Micro level (operational level) varies from hours to seconds.
The relationship between Resilience time and the Rasmussen model is not linear but exponential. This can be derived from the equation:

$$T_{resilience} = T_{available} - T_{reaction}$$

in which $T_{reaction}$ is exponential because of the accelerations en decelerations in the sequence of events (see figure 49), whereas $T_{available}$ is linear. This explains why there is an acceleration in the time it takes to come to decisions when the system is approaching its point of accident (see figure 30 §5.2.2). This acceleration in time can only occur if the process of decision making by the skilled operator is simplified thus forcing the process from knowledge based to rule based and subsequently skill based interventions.

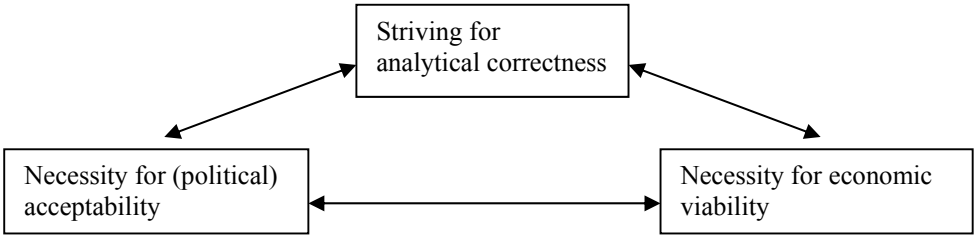

Figure 52. Decision-making dilemmas according to George

The opposite can happen as well. The George dilemma (see figure 52) occurs in situations of decision making when there is a time constraint. One way or another the person or persons involved in (policy) decision making experience a sense of urgency. There is an internal or external pressure on them to do something, yet the problem is what to do?
There is no time for analytical correctness (knowledge based) although the problem is far from clear. There is no time to implement a strategy that avoids unnecessary damage. In fact collateral damage is seen as inevitable (political acceptability) and there is certainly no time to do market research and ask for competitive tenders. If it would be possible to make the system more time resilient the George dilemma would diminish as well. Two cases illustrate this very clearly: the Qantas AQ380 engine failure incident and the Air France A330 Atlantic Ocean accident.

5.3.4 Uncontained engine failure on Qantas Flight 32

The following description has been derived from the official investigation report published by the Australian Transport Safety Board[23].

The accident
November 4, 2010 Qantas Flight 32 which was flown by a Qantas Airbus A380-842 registration VH-OQA, was on its way from Singapore to Sydney when over Batam Island (Indonesia) four minutes after departure it suffered an uncontained engine failure which crippled the aircraft. The captain decided to return to Changi Airport, Singapore where the aircraft made a successful emergency landing. The engine failure was the first serious incident involving an Airbus A380.

Figure 53. Qantas Airbus A380-842 VH-OQA. The Qantas accident was the first major accident with this type of aircraft and gave much additional insight into its behaviour under abnormal conditions

On inspection after the incident it was found that the aircraft's No.2 engine (on the port side nearest the fuselage), a Rolls-Royce Trent 900, failed because of an internal oil fire that had let to the separation of the intermediate pressure disc from its shaft. The fire had started when oil was released from a crack in the pipe that supplied oil to the high pressure/intermediate pressure (HP/IP) turbine bearing chamber.
The ATSB found that the oil pipe had cracked because it had a thin wall from a misaligned counter bore that did not conform to the design specification. The turbine disk separation resulted in damage to the nacelle, wing, fuel system, landing gear, flight controls and the controls for No. 1 engine. Furthermore it was found that unbeknown to the crew on board the plane, whilst in flight there had been an undetected fire in the left inner wing fuel tank that eventually self-extinguished.

Figure 54. Flight path during the event (ATSB report)

Sequence of events
On November 4, 2010 at 09:56 (01:56 UTC) an Airbus A380-842, registered VH-OQA and flown by Qantas as flight 32 departed from Changi Airport, Singapore for Sydney, Australia. On board were five flight crew, 24 cabin crew and 440 passengers.
At 10:01 am Singapore Standard Time (02:01 UTC), while en route over Batam Island, Indonesia, the engine was still climbing, flying at 250 knots and passing 7000 m above mean sea level, when the crew heard two almost coincident loud bangs. The captain immediately selected altitude and heading hold mode on the auto flight system control panel.
What had happened was that an uncontained failure of the port inboard (No. 2) engine had occurred. Shrapnel from the exploding engine punctured part of the wing and caused damage to the fuel system resulting in leaks and a fuel tank fire. Furthermore shrapnel disabled one hydraulic system and the anti-lock brakes and caused No.1 and No.4 engines to go into a 'degraded' mode, damaged landing flaps and the controls for the outer left No.1 engine.

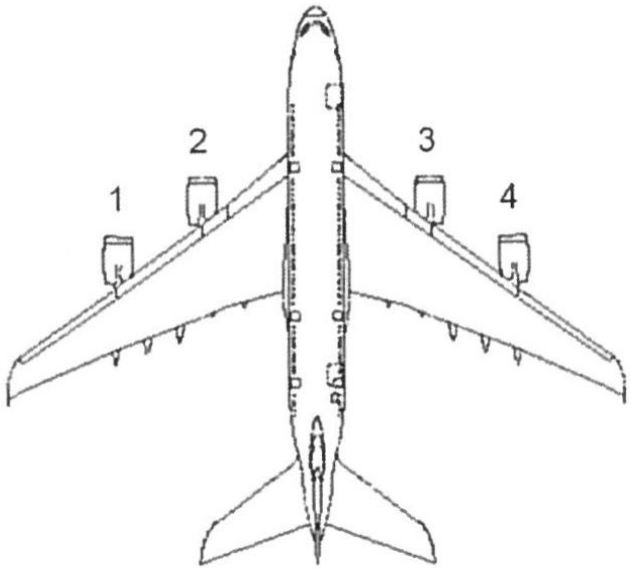

Figure 55. Engine positions (ATSB report)

The aircraft touched down at 01:46 pm Singapore Standard Time (03:46 UTC) and the captain braked the plane using both the wheel brakes and the thrust reversers. The aircraft stopped about 150 m from the end of the runway. It proved impossible to shut down No. 1 engine. The emergency services were very quick on the scene.
Disembarkation by means of moveable stairs started about 50 minutes after the aircraft had landed and took about 60 minutes. The fire-fighters decided to drown No. 1 engine with foam. Eventually three hours after the aircraft had landed, the engine was reported to have shut down.

Figure 56. Fire-fighters drowning the runaway No. 1 engine with foam (ATSB report)

Figure 57. Damaged No. 2 engine (ATSB report)

Managing the situation

At first the crew was inundated with alarms. It was therefore impossible for them to apply contingency procedures because they had no idea which one to apply! In fact they changed to knowledge based behaviour and decided to ascertain not what was wrong with the aircraft but what it was still capable of doing and work forward from that position. In other words they were quickly relearning to fly and control the aircraft in its unexpected reconfigured condition. They knew that the aircraft was equipped with failsafe fallback options such as a drop and lock landing gear capable of lowering and locking the landing gear without the help of the hydraulic system.

The crew also noticed that the aircraft was not dropping from the sky, in fact it was quite steady holding its attitude (flight angles, height and speed). In other words at that moment resilience time of the aircraft as a flight system was >> 0. There was enough time to relearn the aircraft, select a survival strategy and appropriate procedures based on the gained knowledge and if necessary change to an alternative.

As the ATSB report[24] stated 'the crew after finding the plane controllable, decided to fly a racetrack holding pattern close to Changi Airport while assessing the status of the aircraft. It took 50 minutes to complete this initial assessment. The First Officer (FO) and Supervising Check Captain (SCC) then input the plane's status to the landing distance performance application (LDPA) for a landing 50 tons over maximum landing weight at Changi. Based on these inputs the LDPA could not calculate a landing distance. Because Changi is an airport regularly experiencing heavy rains, the standard runway setting in the LDPA is for a wet runway, requiring a longer braking distance.

After discussion and weighing the options on hand the crew elected to remove inputs related to a wet runway, in the knowledge that the runway was dry. The LDPA then returned the information that the landing was feasible with 100 meters of runway remaining. The flight then returned to Singapore Changi Airport, landing safely after the crew extended the landing gear by a gravity drop emergency extension system, at 11:45 am Singapore time. As a result of the aircraft landing 35 knots faster than normal, four tires were blown'.

Upon landing the crew were unable to shut down the No.1 engine, which had to be doused by emergency crews 3 hours after landing until flameout. The pilots considered whether to evacuate the plane immediately after landing as fuel was leaking from the left wing onto the brakes, which were extremely hot from maximum braking.

The SCC pilot, David Evans, noted in an interview, '*We've got a situation where there is fuel, hot brakes and an engine that we can't shut down. And really the safest place was on board the aircraft until such time as things changed. So we had the cabin crew with an alert phase the whole time through ready to evacuate, open doors, inflate slides at any moment. As time went by, that danger abated and, thankfully, we were lucky enough to get everybody off very calmly and very methodically through one set of stairs.*'
The plane was on battery power and had to contend with only one VHF radio to coordinate emergency procedure with the local fire crew. There were no injuries reported among the 440 passengers and 29 crew on board the plane. Debris including a section of the No. 2 engine turbine disc fell on a school and houses on Batam Island also causing structural damage to a car.

Crew performance[25]
On this flight the primary flight crew (captain and first officer) was supported by an additional supporting flight crew (supervising check captain, check captain and second officer). According to the investigation report, the flight and cabin crew behaviour on this flight were consistent with the general requirements regarding crew resource management, indicating that both the flight crew and cabin crew could be classified in this instance as a team performing to the level of a competent team. The majority of skills defined were exhibited on the flight deck and in the cabin of the aircraft during the accident flight. According to the investigation report 'examples of these behaviors included:

- The captain (in conjunction with the rest of an experienced flight crew) made critical decisions regarding aircraft controllability, completion of the ECAM procedures, preparing for return and landing of the aircraft and passenger disembarkation.
- The crew service manager (purser) dealt efficiently and effectively with a minor medical issue involving a passenger and their medication, and ensured that all cabin crew were aware of the developing situation and what their duties entailed by personally visiting each station and briefing all crew.
- The crew service manager reported controlling the communications between the flight deck and cabin to maintain one point of contact.
- Communication between all crew members and between crew and the passengers was rapid, thorough and provided the necessary information to keep all fully informed.
- Flight crew and cabin crew worked very well together within and across their teams to ensure the safe outcome from an emergency situation'.

Observation
The investigation report noted that on the flight deck, the supporting flight crew provided valuable input and assistance to the primary flight crew—in terms of conducting PA announcements, liaison with the cabin crew and visual observations of damage. Although the additional flight crew were a valuable resource, had they not been available the primary flight crew would have likely responded to the situation in a similar manner. However, the gathering of information to assist in decision making would have required the use of alternative resources and methods. This may have resulted in prolonging the airborne time before landing or it is also possible that the flight crew may have shed tasks not essential to flight safety. This was unlikely to have affected the safety of the flight because the crew's training and the aircraft manufacturer's procedures required them to complete prescribed tasks before attempting to land.

5.3.5 Frozen tubes probes crash Air France Flight 447[26]

The following description has been derived from the official investigation report published by the Bureau d'Enquetês et d'Analyses pour la sécurité de l'aviation civile (BEA) of the French Ministère de l'Ecologie, du Développement durable, des Transports et du Logement.

The accident

Air France Flight 447 was a scheduled commercial flight from Galeão International Airport in Rio de Janeiro, Brazil to Charles de Gaulle International Airport in Paris, France. On 1 June 2009, the Airbus A330-203 airliner with registration F-GZCP crashed into the Atlantic Ocean, resulting in the deaths of all 216 passengers and 12 aircrew. The accident was the deadliest in the history of Air France. It was also the Airbus A330's second and deadliest fatal accident, and its first while in commercial passenger service.

Figure 58. Air France Airbus A330-203 F-GZCP

Initial investigation was hampered because authorities were unable to locate the wreckage; it was located nearly two years after the accident, and the aircraft's black boxes were finally recovered from the ocean floor, May 2011. The final report, released at a news conference on July 5, 2012, stated that the aircraft crashed after temporary inconsistencies between the airspeed measurements—likely due to the aircraft's pitot tubes being obstructed by ice crystals—caused the autopilot to disconnect, after which the crew reacted incorrectly and ultimately led the aircraft to an aerodynamic stall from which they did not recover.

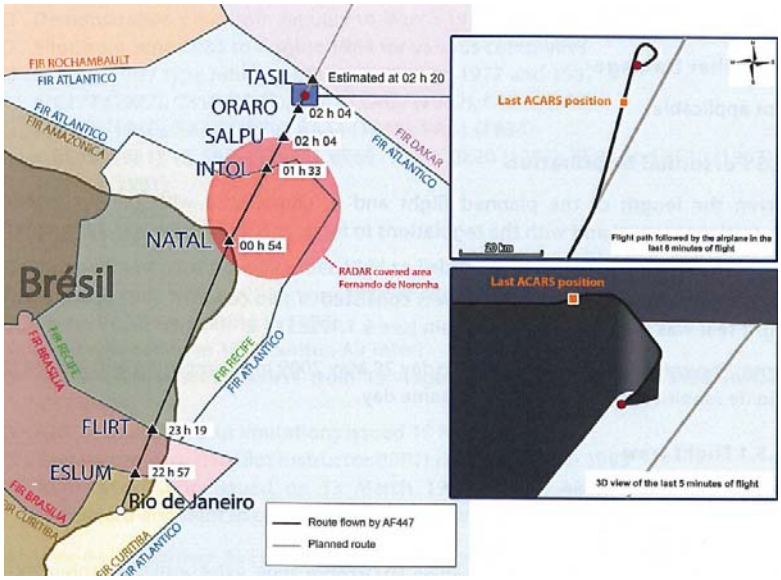

Figure 59. Flight path during the event (BEA report)

Operational control modes

The Airbus series A330 is designed and build as a so called fly by wire aircraft. The pilots operate a side stick which gives command inputs to the on board flight control system. The aim of this system is to increase the overall safety by providing direct input through electrical signals for more precise commands. In addition, the control system monitors pilot commands to ensure the aircraft is kept within a safety margin called the 'flight protection envelope'. Usually pilots can get the maximum performance out of Airbus aircraft without running the risk of exceeding these flight limits. The on-board flight control system can operate in three main modes:

- Normal law;
- Alternate law:
  - Alternate 1;
  - Alternate 2;
    - Abnormal attitudes law;
- Direct law.

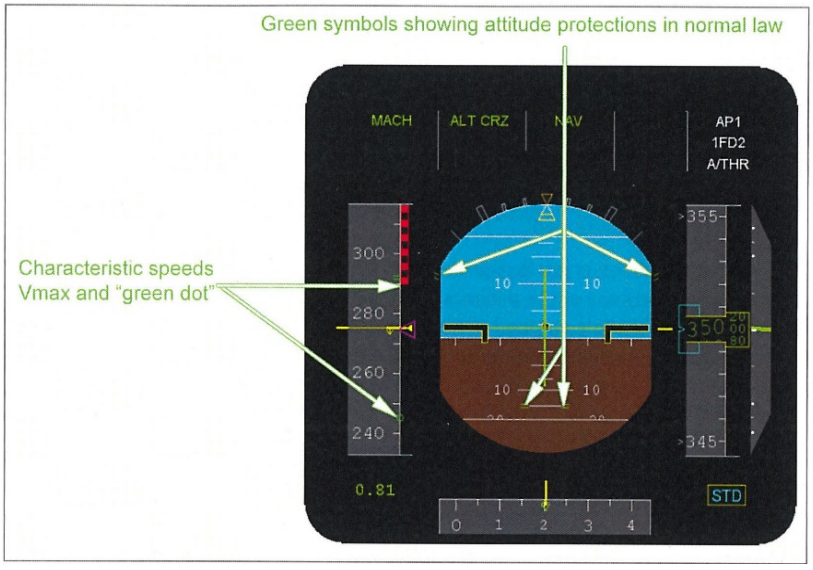

Figure 60. Primary flight display in normal law mode (BEA report)

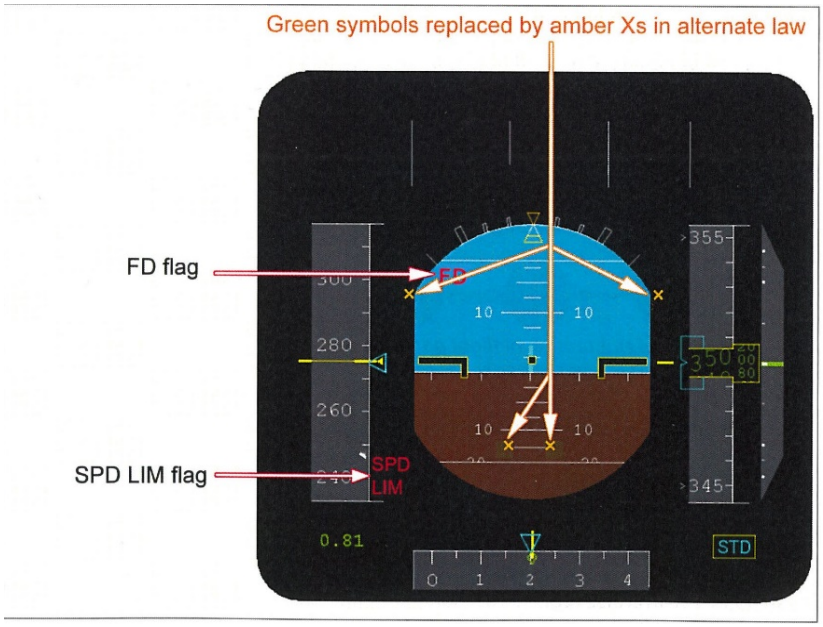

Figure 61. Primary flight display in alternate 2 law mode (BEA report)

Normal law offers complete protection of the flight envelope: in terms of attitude (the pitch and bank angles values are limited), load factor, at high speed and at high angle of attack. When the protections are not triggered, the longitudinal orders from the side-sticks command a load factor according to the aircraft's normal axis and the lateral orders command a rate of roll.
In alternate law, the longitudinal orders from the side-sticks command a load factor according to the aircraft's normal axis, like with normal law but with fewer protections. Furthermore according to the BEA report:

- in alternate 1, the lateral orders from the side-sticks still command a rate of roll;
- in alternate 2, the side-sticks command the ailerons and lift dumpers directly.

In direct law, the protections are lost and orders from the side-sticks control the position of the various control surfaces of the aircraft directly.
Another law, called the abnormal attitudes law, is triggered in certain cases where the aircraft's attitude is outside certain ranges, for example when the bank angle exceeds 125°. This is an alternate 2 law with maximum lateral authority and without automatic trimming.

Sequence of events[27]
According to the investigation report 'the aircraft departed from Rio de Janeiro-Galeão International Airport on 31 May 2009 at 19:29 local time (22:29 UTC), with a scheduled arrival at Paris-Charles de Gaulle Airport 10h34min later. The last verbal contact with the aircraft was at 01:35 UTC, when it reported that it had passed waypoint INTOL (1°21′39″S 32°49′53″W 1.36083°S 32.83139°W), located 565 km (351 mi) off Natal, on Brazil's north-eastern coast. The aircraft left Brazilian Atlantic radar surveillance at 01:49 UTC.
The Airbus 330 is designed to be flown by a crew of two pilots. But because the thirteen hours duty time (flight duration, plus pre-flight preparation) for the Rio - Paris route exceeds the maximum ten hours permitted by Air France's procedures, flight 447 was crewed by three pilots: a captain and two co-pilots. With three pilots on board, each of them can take a rest during the flight, and for this purpose the A330 has a rest cabin, situated just behind the cockpit.

In accordance with common practice the captain had sent one of the co-pilots for the first rest period with the intention of taking the second break himself.
At 01:55 UTC, he woke the second pilot and said: *'... he's going to take my place'*. After having attended the briefing between the two co-pilots, the captain left the cockpit to rest at 02:01:46 UTC.
At 02:06 UTC, the pilot warned the cabin crew that they were about to enter an area of turbulence. Two minutes later, the pilots turned the aircraft slightly to the left and decreased its speed from Mach 0.82 to Mach 0.8 (the recommended 'turbulence penetration speed').
At 02:10:05 UTC the autopilot disengaged and the airplane transitioned from normal law to alternate law. The engines' auto-thrust systems disengaged three seconds later. Without the auto-pilot, the aircraft started to roll to the right due to turbulence, and the pilot reacted by deflecting his side-stick to the left. One consequence of the change to alternate law was an increase in the aircraft's sensitivity to roll, and the pilot's input over-corrected for the initial upset. During the next thirty seconds, the aircraft rolled alternately left and right as the pilot adjusted to the altered handling characteristics of his aircraft. At the same time he made an abrupt nose-up input on the side-stick, an action that was unnecessary and excessive under the circumstances. The aircraft's stall warning sounded briefly twice due to the angle of attack tolerance being exceeded, and the aircraft's recorded airspeed dropped sharply from 274 knots to 52 knots. The aircraft's angle of attack increased, and the aircraft started to climb. By the time the pilot had control of the aircraft's roll, it was climbing at nearly 7,000 ft/min.
At 02:10:34, after displaying incorrectly for half a minute the left-side instruments recorded a sharp rise in airspeed to 215 knots, as did the Integrated Standby Instrument System (ISIS) another half a minute later (the right-side instruments are not recorded by the recorder). The icing event had lasted for just over a minute. The pilot continued making nose-up inputs. The trimmable horizontal stabilizer (THS) moved from three to thirteen degrees nose-up in about one minute, and remained in that latter position until the end of the flight.
At 02:11:10 UTC, the aircraft had climbed to its maximum altitude of around 38,000 feet. There its angle of attack was 16 degrees and the thrust levers were in the TO/GA (take off/go around) detent (fully forward).
At 02:11:15 UTC the pitch attitude was slightly over 16 degrees and falling, but the angle of attack rapidly increased towards 30 degrees.
A second consequence of the reconfiguration into alternate law was that 'stall protection' no longer operated. Whereas in normal law the airplane's flight management computers would have acted to prevent such a high angle of attack, in alternate law this did not happen. (Indeed the switch into alternate law occurred precisely because the computers, denied reliable speed data, were no longer able to provide such protection - nor many of the other functions expected of normal law). The wings lost lift and the aircraft stalled ultimately resulting in the crash of the aircraft.
At 02:11:40 UTC, the captain re-entered the cockpit. The angle of attack had by then reached 40 degrees and the aircraft had descended to 35,000 feet with the engines running at almost 100% N_1 (the rotational speed of the front intake fan, which delivers most of a turbofan engines' thrust). The stall warnings stopped, as all airspeed indications were now considered invalid by the aircraft's computer due to the high angle of attack. In other words, the aircraft was oriented nose-up but descending steeply, a typical stall situation.
Roughly 20 seconds later, at 02:12 UTC, the pilot decreased the aircraft's pitch slightly, air speed indications became valid and the stall warning sounded again and sounded intermittently for the remaining duration of the flight, but stopped when the pilot increased the aircraft's nose-up pitch. From there until the end of the flight, the angle of attack never dropped below 35 degrees.

From the time the aircraft stalled until it impacted with the ocean, the engines were primarily developing either N1 100% or TO/GA thrust, though they were briefly spooled down to about N1 50% on two occasions. The engines always responded to commands and were developing in excess of N1 100% when the flight ended.
The flight data recordings stopped at 02:14:28 UTC, 3 hours 45 minutes after take-off. At that point, the aircraft's ground speed was 107 knots, and it was descending at 10,912 feet per minute. Its pitch was 16.2 degrees (nose up), with a roll angle of 5.3 degrees left. During its descent, the aircraft had turned more than 180 degrees to the right to a compass heading of 270 degrees. The aircraft remained stalled during its entire 3 minute 30 second descent from 38,000 feet before it hit the ocean surface at a speed of 151 knots (280 km/h), comprising vertical and horizontal components of both 107 knots. The aircraft broke up on impact; everyone on board died.
It took until April 2, 2011 before the wreckage of the aircraft was localised. The wreckage was found about 6.5 NM on the radial 019 from the last known position, slightly to the left of the planned route. The wreckage rested on an abyssal plain at a depth of 3900 meters. This localisation of wreckage made it possible to recover both flight data recorders and important parts of the aircraft itself. The latter could be examined on specific signs of failure. The flight data recorders were recovered on May 1, 2011. The underwater search and recovery operation ended on June 16, 2011, the date the aircraft parts arrived at the port of Bayonne in France'.

Management of a sudden anomaly and implications on human performance
The BEA report[28] states that 'in some cases maintaining flight safety after the appearance of an anomaly (or even the acceptability of an anomaly) supposes appropriate crew intervention. First of all, it is expected that the crew ensures control of the aircraft and follows the flight path. The intention is then that the crew will detect the anomaly, that they will possibly 'make sense' of this detection, that they will modify their priorities on tasks in progress, and that they will take the corresponding action, (control inputs and/or acting on processing malfunctions, associated with procedures or check-lists), all of this in the expected timeframe (whose order of magnitude is indicated in the certification logic if it is critical).
On the A330, the Electronic Centralized Aircraft Monitoring system ECAM proposes actions to be carried out in the majority of failure or emergency cases. From the information available on the ECAM, the crew must analyze and confirm the type of failure before undertaking any failure processing action. In other cases the 'adequate reaction' expected of the crew supposes immediate memory items with the purpose to stabilize the situation, than recourse to action instructions available on the ECAM, and/or recourse to procedures explained in the Quick Reference Handbook and classified by category of diagnosed anomaly.
In all cases this includes a specific number of implications concerning human performance, which may be based on what can reasonably be expected of any human operator (for example noticing a clearly audible aural signal), or generic professional abilities normally present in the pilot community ('basic airmanship'), or even specific abilities which must be explicitly developed through a specific training course and / or practice.
In addition, these expected reactions result from various cognitive modes of activity. Human operators notice and act according to their mental representation of the situation, and not to the 'real' situation. The probability and speed of detection of anomaly signals is connected to their 'salience', that is to say to their ability to destabilize and modify the representation of the situation in progress, all the while being situated possibly outside the frame of this representation (that is to say unexpected, surprising, absurd, even 'unthinkable' in its context). Depending on the frequency of the operator's exposure to the anomaly during his training or in real operations, his response may be automatic, applying rules, or developed on the basis of in-depth knowledge'.

It is essential in these indirect controlled systems that the representation of the situation and condition of the system as presented to the operator (pilot) coincides with the actual and factual situation of the system. That was one of the problems in this case, because the pilots lacked access to that vitally important information. Automatic responses assume recognition of very specific stimuli, to which the reaction is associated without true interpretation. Applying rules assumes not only their knowledge, but also the recognition of their conditions of applicability, and therefore the correct identification plus a specific interpretation of the anomaly.
The construction of a response by calling on experience assumes incorporation of the anomaly in the mental representation of the situation, which can go via its destruction/reconstruction, very wasteful in resources and time-consuming. In this way the correct perception of the situation by a crew, which enables the reliability and speed of diagnosis and decision to be improved, is linked not only to the way in which the situation is presented to this crew (interfaces, parameters) but also to their training and experience.
Based on the preceding, for a good chance that these expectations of the crew may be met, according to the BEA report[29] it is therefore necessary:

- 'That the signs of the problem are sufficiently salient to bring the crew out of their preoccupations and priorities in the flight phase in progress, which may naturally be distant from strict monitoring of the parameter(s) involved in the anomaly;
- That these signs be credible and relevant;
- That the available indications relating to the anomaly are very swiftly identifiable so that the possible immediate actions to perform from memory to stabilize the situation are triggered or that the identification of the applicable procedure is done correctly. In particular, it is important that the interfaces that usually carry anomaly information display, or at least allow, this initial diagnostic, given the minimum competence expected of a crew. Failing this, it is necessary to offset the lack of information supplied by the system which would enable the diagnostic to be reached by specific training;
- That the memory items are known and sufficiently rehearsed to become automatic reflexes associated only with awareness of the anomaly, without the need to construct a more developed understanding of the problem;
- That there are no signals or information available that suggest different actions or that incite the crew to prior reconstruction of their understanding the situation'.

It is generally accepted in aviation that the order of actions is as follows:

1. Aviate: keep the aircraft flying.
2. Navigate: know where you are both horizontally and vertically.
3. Communicate: both internal on the flight deck and with the cabin crew as well as external to traffic control and/or other aircraft in the vicinity.
4. Manage: take care of the solution of the emergency.

This order is quite absolute as experts from the aviation industry have explained. In modern aircraft actions 1 and 2 are highly computerized. It is therefore first of all necessary to understand what the computerized system determines to be the nature of the problems.

Risk model in mental representation
According to the BEA report[30] in a situation analogous to that which preceded the accident (cruise flight in the area of the Inter-Tropical Zone Convergence (ITCZ), the aeroplane is in autopilot. Crews generally just undertake confident monitoring of the flight path and the automated systems due to their level of performance and reliability. Their preoccupations are above all centred on tactical and strategic aspects of navigation and fuel management.

The risk model in the mental representation of the situation by crew members contains:

- **As a top priority**, the risk associated with crossing the ITCZ and consequently with turbulence, and perhaps with icing. The ITCZ is a zone that may be difficult to cross, and the crossing strategy depends as much on knowledge of the aeroplane (management of meteorological radar and knowledge of limitations and performance for example) as on the changes in the ITCZ itself (vertical development and horizontal movement). This strategy implies flight management that may require decision making, such as avoidance or a change of flight level;
- **A second risk**, doubtless far behind the first in the scale of perceived priorities, associated with the risks of loss of high frequency (HF) radio contact with Air Traffic Control (ATC), of mid-air collision, of triggering an alert phase and of not being able to declare a need for a diversion and/or storm cell avoidance;
- A third risk present in the communications exchanged by the crew and linked to the management of a possible diversion and to the arrival conditions (for example, accessibility of alternate aerodromes for a diversion in the event of pressurisation or engine failure etc.);
- Lastly a **set of risks** grouping together all the possible problems and malfunctions on board, in the cockpit or cabin, and in the environment, the air mass or on the ground. This fourth group was not expressed verbally in the recorded communications, or any specific action. It is always present in the background of a pilot's cognitive activity, and is expressed by a visual/attention circuit which may not be recorded by current equipment.

The management of the first three areas of risk needs active handling of the action plan underway, that is to say by preoccupations and occupations: search for information (example adjusting the radar), thinking, calculations, evaluations, judgements, decisions, communications between crew members, possible actions on the flight path targets. The management of the fourth group of risks is performed by monitoring various marker parameters, signals and corresponding warnings. It remains passive until detection of an anomaly, which will trigger the appropriate active response by rapidly reorganising the action plan around new priorities.

Cause of the accident

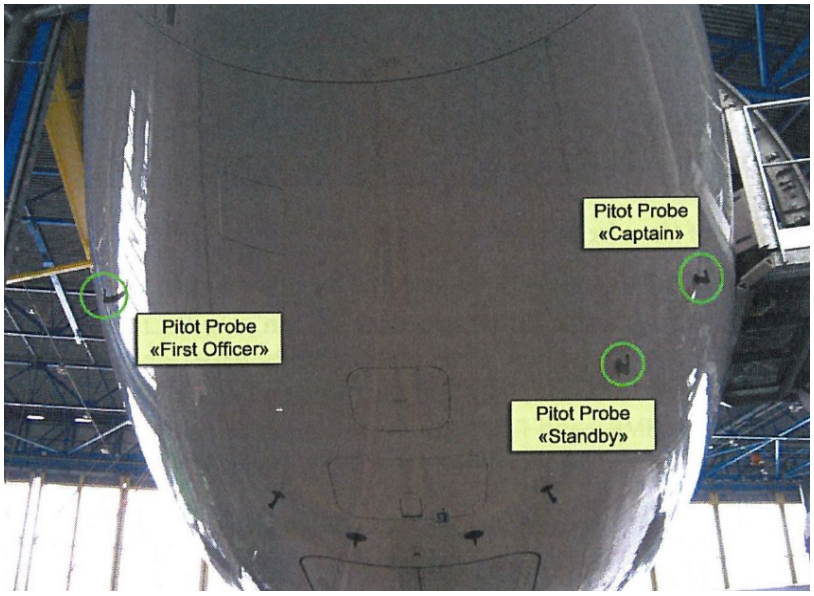

Figure 62. Pitot tubes on an Airbus A330 (BEA report)

The obstruction of the pitot tubes by ice crystals during cruise was a phenomenon that was known but misunderstood by the aviation community at the time of the accident. From an operational perspective the total loss of airspeed information that resulted from this was a failure that was classified in the safety model. After initial reactions that depend upon basic airmanship, it was expected that it would be rapidly diagnosed by pilots and managed where necessary by precautionary measures on the pitch attitude and the thrust, as indicated in the associated procedure.
The occurrence of the failure in the context of flight in cruise completely surprised the pilots of flight AF 447. The apparent difficulties with aeroplane handling at high altitude in turbulence led to excessive handling inputs in roll and a sharp nose-up input by the pilot flying PF. The destabilisation that resulted from the climbing flight path and the evolution in the pitch attitude and vertical speed was added to the erroneous airspeed indications and ECAM messages, which did not help with the diagnosis. The crew, progressively becoming de-structured, likely never understood that it was faced with a 'simple' loss of three sources of airspeed information.
In the minute that followed the autopilot disconnection, the failure of the attempts to understand the situation and the de-structuring of crew cooperation fed on each other until the total loss of cognitive control of the situation. The underlying behavioural hypotheses in classifying the loss of airspeed information as 'major' were not validated in the context of this accident. Confirmation of this classification thus supposes additional work on operational feedback that would enable improvements, where required, in crew training, the ergonomics of information supplied to them and the design of procedures.
The aeroplane went into a sustained stall, signalled by the stall warning and strong buffet. Despite these persistent symptoms the crew never understood that they were stalling and consequently never applied a recovery manoeuvre. According to the investigation report 'the combination of the ergonomics of the warning design, the conditions in which airline pilots are trained and exposed to stalls during their professional training and the process of recurrent training does not generate the expected behaviour in any acceptable reliable way'.
In its current form recognising the stall warning even associated with buffet supposes that the crew accords a minimum level of 'legitimacy' to it. This then supposes sufficient previous experience of stalls, a minimum of cognitive availability and understanding of the situation, knowledge of the aeroplane (and its protection modes) and its flight physics. An examination of the current training for airline pilots does not, in general, provide convincing indications of the building and maintenance of the associated skills.
According to the BEA-report[31] the accident resulted from the following succession of events:

- 'Temporary inconsistency between the airspeed measurements, likely following the obstruction of the pitot tubes by ice crystals that, in particular, caused the autopilot disconnection and the reconfiguration to alternate law;
- Inappropriate control inputs that destabilized the flight path;
- The lack of any link by the crew between the loss of indicated speeds called out and the appropriate procedure;
- The late identification by the pilot not flying (PNF) of the deviation from the flight path and the insufficient correction applied by the PF;
- The crew not identifying the approach to stall, their lack of immediate response and the exit from the flight envelope;
- The crew's failure to diagnose the stall situation and consequently a lack of inputs that would have made it possible to recover from it'.

These events can be explained[32] by a combination of the following factors:

- 'The feedback mechanisms on the part of all those involved that made it impossible:
  - To identify the repeated non-application of the loss of airspeed information procedure and to remedy this;
  - To ensure that the risk model for crews in cruise included icing of the pitot tubes and its consequences;
- The absence of any training at high altitude, in manual aeroplane handling and in the procedure for *'Vol avec IAS douteuse'*;
- Task-sharing that was weakened by:
  - Incomprehension of the situation when the autopilot disconnection occurred;
  - Poor management of the startle effect that generated a highly charged emotional factor for the two co-pilots;
- The lack of a clear display in the cockpit of the airspeed inconsistencies identified by the computers;
- The crew not taking into account the stall warning, which could have been due to:
  - A failure to identify the aural warning, due to low exposure time in training to stall phenomena, stall warnings and buffet;
  - The appearance at the beginning of the event of transient warnings that could be considered as spurious;
  - The absence of any visual information to confirm the approach-to-stall after the loss of the limit speeds;
  - The possible confusion with an over speed situation in which buffet is also considered as a symptom, Flight Director indications that may led the crew to believe that their actions were appropriate, even though they were not;
  - The difficulty in recognizing and understanding the implications of a reconfiguration in alternate law with no angle of attack protection'.

The double failure of the planned procedural responses shows the limits of the current safety model. When crew action is expected, it is always supposed that they will be capable of initial control of the flight path and of a rapid diagnosis that will allow them to identify the correct entry in the dictionary of procedures. A crew can be faced with an unexpected situation leading to a momentary but profound loss of comprehension. If, in this case, the supposed capacity for initial mastery and then diagnosis is lost, the safety model is then in 'common failure mode'. During this event, the initial inability to master the flight path also made it impossible to understand the situation and to access the planned solution. This reverses the principle of precaution whereby 'act first, understand later' is replaced by understand the situation and act upon comprehension of possible scenarios, applicable procedures and their consequences / possible outcomes, in other words an on the spot risk analysis. The applicable procedures do not by necessity have to be predetermined. They can be developed from tacit knowledge which requires (resilience) time.

5.3.6 Reflection on the Qantas and Air France cases

Complicated dynamic systems

Both cases show how complicated modern dynamic systems have become. Yet sometimes they require quick responses from the operating staff involved. However, even under these conditions the complexity of the system and the nature of its malfunctioning (multiple problems) make it necessary to avoid the necessity of an operators' response only at skill based level, because such an (intuitive) response runs every risk of being inadequate or worse increasing the problem (pilot induced oscillation is a classic example of this).

In order to do so, the operators:

- Must be thoroughly competent both for normal operation and every foreseeable abnormal operation;
- Must have sufficient input about the cause and possible consequences of the abnormality;
- Must have adequate standard operational abnormal procedures for dealing with abnormalities;
- Must have sufficient time to implement a plan-do-check-act loop regarding the execution of procedures:
    - sufficient time to check these abnormal procedures and select the correct one;
    - sufficient time to execute the selected abnormal procedure;
    - sufficient time to check the response of the system after execution of the abnormal procedure;
    - sufficient time to reassess the situation and if necessary adjust the selection of procedures;
- Must be trained to be alert for signs of new problems whilst busying themselves with the mitigation of earlier ones and if necessary adjust priorities between them.

These cases show that under time pressure there is a real danger of operators being forced from rule-based behaviour to skill-based behaviour where execution of the correct skills becomes fully dependent on the subconscious experience of the operator.
It is possible that the system is in a different state compared to where it appears to be to the operator (pilot). Also system states can change in quick succession.
The fundamental difference between the Air France and Qantas case is that in the former the crew were in the unknown unknown state and remained in that state until the moment of impact. In the latter the crew managed to move themselves mentally from the unknown unknown state to the known known state and thereby saved the aircraft and everybody on board.
In the Air France case part of the crew lacked essential basic flying skills such as how to react to a high altitude stall. Also there was not a clear division of tasks between the two pilots. The Qantas crew had all the necessary skills and the crew was managed in an effective way by good leadership from the captain of the flight.

Role of resilience time

Complex risk sensitive systems require risk assessment under abnormal conditions. In less complicated systems it is quite common to (re)act first and understand later. Railway accidents are classic examples of this: first reaction is shutting down the entire system, bringing it to a full stop. This usually stabilises the system locally in a safe state from where later on a controlled recovery is possible.
Such an emergency stop strategy might be feasible on a rail related system, although the Amsterdam metro cases (see §5.2.1 and §5.2.3) have shown that in a rail system shutting it down can have negative consequences elsewhere (translating risk to other parts of the transport system). In many other transport related systems such as road transport, commuter rail systems and aviation systems a total shutdown is simply not possible let alone acceptable to society (another example of a George dilemma). You cannot stop an aircraft in mid-air. Major road traffic jams create havoc for the economy. Shutting down airports or runways can create new safety critical problems such as congestion at other airports, similar to a partial shutdown of a rail network. Practice shows that when the railways in the west of the Netherlands (in particular around Amsterdam, Rotterdam or Utrecht) are down during rush hour, the inevitable result is chaos on the motorways and accidents because of this.

Complicated systems such as those defined by Perrow[33] as complex and tight coupled can become more unstable if the operator does not understand the reason for its abnormal behaviour. This is where the notion of resilience time becomes interesting. A system with sufficient resilience time is a system with buffer time to execute the Rasmussen loops at the correct level including interaction between levels. It even allows for reassessment of the situation after first execution of mitigating measures. It avoids the situation where the operator is forced in a position where he cannot undo a procedure. A mitigating procedure once selected must be executed in full until the end of the procedure.
Thus according to Hollnagel et al[34] important characteristics of the system under abnormal conditions are:

- The ability to address the **actual**: knowing what to *do*, that is, how to respond to regular and irregular disruptions and disturbances either by implementing a prepared set of responses or by adjusting normal functioning;
- The ability to address the **critical**: knowing what to look for, that is, how to *monitor* that which is or can become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, that is, its own performance;
- The ability to address the **potential**: knowing what to *expect*, that is, how to anticipate developments, threats, and opportunities further into the future, such as potential changes, disruptions, pressures, and their consequences;
- The ability to address the **factual**: knowing what *has happened*, that is, how to learn from experience, in particular how to learn the right lessons from the right experiences – successes as well as failures.

These notions will be further explained in the next chapter.

5.4 Conclusion

The railway cases show the important role of time as a hidden property of safety critical systems. The fact that resilience time can become negative makes it clear that such a state is very much unwanted. What is also important is the acceleration and deceleration of events around a chaotic, catastrophic situation. Mental processes of operators must be able to keep pace with this, just as the way their information streams flow. When that condition is no longer valid, the system is vulnerable and in fact possibly in deep trouble already some time before the actual mishap.
Is a system with a resilience time characteristic where that time parameter is at some point much larger than 0 always at low risk or in a state of controlled risk? Unfortunately not. It can create a mental trap where the operator lacks a sense of urgency. He starts analysing the system and weighing the options without coming to a decision regarding a survival strategy. The Air France case shows this to a certain extend. Initially despite the seriousness of the abnormality there was sufficient resilience time available. Because the true nature of the abnormality was not understood on the flight deck, the mitigating procedures were not selected until at such a time where the resilience time had become negative and the aircraft was inevitably on its way to disaster above the Atlantic Ocean.
The Qantas case however shows that a system with a resilience time characteristic much larger than zero can provide the operator with precious extra time to try an emergency procedure and if necessary, when that procedure does not seem to contain the emergency, the possibility to switch to a fall-back option or to develop a survival strategy in cases where the nature of the abnormality is very much unclear.

On the other hand a system where scenarios can occur with negative resilience time characteristics are not per definition always safety critical. Just as according to Perrow[35] tight coupled complex systems can be expected to fail in an unforeseen way due to systems properties unbeknown to the operator, these same unforeseen properties can sometimes safe a system under abnormal conditions. If that happens it is popularly explained as 'providence saved us' or something similar when referring to a superior power of nature in relation to unexpected system resilience present.
That answers research question 4: *What methodologies exist, which can be used to improve the situation?* The answer to that question can best summarised by Hollnagel et al: the ability to address the actual, factual, potential and critical under abnormal conditions. If you fail to do that, sooner or later you will be confronted by a normal accident as defined by Perrow.
Common techniques are quantitative risk assessments, scenario analysis and sensitivity analysis. All these techniques are based on the assumption that you have at least some idea about how the system is going to operate and the way it can fail. They fail to deal with the unknown unknowns, the unpredictable situations.
Research question 5 was: *If existing methodologies are not adequate in dealing with these issues, which improvements are possible?* It is preferable to design resilience into the system if the safety of the system depends on it. It is therefore necessary to design the system in such a way that fall-back options become possible, including temporary measures to arrest or slow down the deterioration of the system (increasing resilience time). Fall-back options are system state dependent. When a system state is misjudged a fall-back option when applied can increase the problem rather than diminish it, as was shown both at Harrisburg and Chernobyl. The next chapter will show how this can be achieved. It is therefore necessary not only to model the system states but also to transitions between these states.

Notes

[1] Ref. ILT (IVW) report RV-08U0288, 2008
[2] Ref. RIVM, 2003
[3] Tijdelijke commissie infrastructuren, 2004
[4] Ref. ILT (IVW) report RV-04U008, 2004
[5] Telerail was a Dutch Railways radio system to communicate between rail traffic controllers and train drivers; it has been replaced by GSM-R
[6] ATB: Dutch system of automatic train control
[7] ERTMS (European Rail Traffic Management System) has two basic components: ETCS, the European Train Control System, is an automatic train protection system (ATP) to replace the existing national ATP-systems; GSM-R, a radio system for providing voice and data communication between the track and the train, based on standard GSM using frequencies specifically reserved for rail application with certain specific and advanced functions. ERTMS aims at replacing the different national train control and command systems in Europe.
[8] Ref. Tweede Kamer Commissie voor Verkeer en Waterstaat, 2006
[9] Ref. ILT (IVW) report RV-08U0938, 2009
[10] Ref. SWOV, 2009
[11] Unfortunately this is no longer true. A passenger was killed in the Amsterdam train crash on April 21, 2012.
[12] See chapter 5.2.2
[13] Ref. Beukenkamp
[14] After this investigation, when the judge in court questioned him during his dismissal trail, the driver claimed that he was suffering from diabetes and felt not well at that moment. The judge replied by

stating that it is the responsibility of the driver to report that he is unfit for duty, which he failed to do. Therefore this is no excuse for his behaviour according to the judge.
[15] Ref. ILT (IVW) report RV09-0179, 2009
[16] Ref. RAIB report Broken rails at Urchfront and Kennington following passage of a freight train 5 January 2006.
[17] Ref. ILT (IVW) report RV-08U0831
[18] Ref. ILT report RV12-0346
[19] Ref. ILT report RV12-0346 p. 18
[20] Ref. Commissie Bijlmerramp, 1999
[21] Ref. Commissie Bijlmerramp, 1999
[22] Ref. Rasmussen (1983): Skills, rules and knowledge; signals, signs en symbols
[23] Ref. ATSB report AO-2010-089
[24] Ibidem p. 2
[25] Ibidem p. 37-38
[26] Ref. BEA Final report on the accident on 1st of June 2009 to the Airbus A330-203
[27] Ibidem p. 21-24
[28] Ibidem p. 101-103
[29] Ibidem
[30] Ibidem p. 167
[31] Ref. BEA report p. 200
[32] Ibidem
[33] Normal accidents
[34] Ref. Hollnagel et al, p. xxxvii
[35] Normal accidents

6. System dynamics: states and transitions

6.1 Introduction

The previous chapter identified hidden properties regarding risk sensitive systems. One of these properties is the time factor as indicated by the notion of resilience time. Our perspective of a risk sensitive system needs to be more dynamic and non-linear in time. Also the outcome of chapter 5 indicated a necessity to include fall-back strategies in the systems design, amongst others to buy time for an effective recovery strategy to be implemented. This in effect is one of the aspects of resilience engineering.
This chapter will show that next to the earlier described George dilemma when a system is fully operational, another dilemma with important safety implications can occur, this time at an early stage of the life cycle of a system: the Collingridge dilemma. When change is easy the need for it cannot be foreseen. When the need arises any change is so expensive, difficult and time-consuming that it is almost impossible to achieve. The implications of Collingridge and its interaction with the George dilemma are described in this chapter.

6.2 From a static to a dynamic perspective

The previous chapters have indicated that the traditional approach to emergencies and catastrophes has given us insight in catastrophic failure modes. Sometimes what they fail to provide is sufficient transparency regarding the required knowledge to prevent them. Despite Stirling, Slovic, Stoop, Rosmuller and van Poortvliet and their theoretical models failures of risk sensitive systems still occur and we keep on studying them often from a static linear single actor perspective.
Empirical evidence as shown in the cases as presented in this study indicates a requirement for a more dynamic approach to counter decision making dilemmas such as the George dilemma. Although the outcome of the case studies appear to suggest a tension between a probabilistic approach versus a deterministic one, in practice this tension is not so clearly noticeable. Also the George dilemma as such is not so much a cause as a response to an underlying not clearly defined problem. That problem is identifying the importance of the distinction between process and contents.
We have encountered the George dilemma which focuses on the contents and is first and foremost a control dilemma. It is not the only important dilemma though in these matters. The Collingridge dilemma (see §6.3) is related to the accompanying process and system lifecycle and is an engineering (design) dilemma. These two dilemmas are not only separated by the operational level at which they act but also by required skills to deal with them.

Another distinction is the difference between event and system, events having a linear time line and systems being characterised by state transitions with a non-linear time line, showing discrete sequences with accelerations and decelerations. Integrating state dynamics with resilience engineering offers a new perspective and opens the way to novel solutions for some of the dilemmas seen as inevitable and inescapable.

6.3 The Collingridge dilemma

One of the dominating problems in safety critical systems is that you can face a double bind dilemma. A double bind is an emotionally distressing dilemma in communication in which an individual (or group) receives two or more conflicting messages, and one message negates the other. This creates a situation in which a successful response to one message results in a failed response to the other (and vice versa), so that the person will automatically be wrong regardless of response. The double bind occurs when the person cannot confront the inherent dilemma, and therefore can neither resolve it nor opt out of the situation. David Collingridge first observed such a dilemma regarding safety critical systems in 1980[1]:

1. Early in the life span of a safety critical system it is difficult to identify safety hazards and their consequences; because of a lack of experience quantification of risks is not based on statistical proof.
2. Once the system is developed and fully operational including an expending use by society, eliminating or mitigating a hazard is often very difficult.

This is as Collingridge noted a paradox which lies at the core of many problems in dealing with a lot of new technologies. One recent example of a Collingridge dilemma is nanotechnology[2]. Nanotechnologies have been hyped as bringing about another industrial revolution. But they have also caused concern about their potential adverse effects on human health and the environment, misuse for military purposes, and excessive corporate control of intellectual property. Policymakers find themselves in the difficult position of promoting the development of nanotechnologies (short term), while at the same time securing public trust in their safe commercial application (long term).

Another example of a Collingridge dilemma is driverless cars[3]. They pose a dilemma when it comes to safety. These autonomous vehicles are programmed with a set of safety rules, and it is not hard to construct a scenario in which those rules come into conflict with each other. Suppose a driverless car must either hit a pedestrian or swerve in such a way that it crashes and harms its passengers. What should it be instructed to do?

Collingridge was somewhat pessimistic about our ability to work of the prediction side of the dilemma using a Bayesian approach, due to the high level of ignorance which in his view invalidated Bayesian risk assessments in infant systems. In 'This explains everything' technology critic Evgeny Morozov explains Collingridge's dilemma as follows: 'When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time consuming[4]'.

When a system is in its infant stage, there is ample time for change but because of unforeseen developments there is no urgency for change, thus creating the Collingridge dilemma. When a system has reached maturity and social acceptance, time for change is so short that the George dilemma becomes apparent. The Collingridge dilemma is a design dilemma, whereas the George dilemma (§2.2) is a predominantly organisational (managerial) dilemma. The time line of the 2004 Amsterdam train collision is an example of Collingridge in practice.

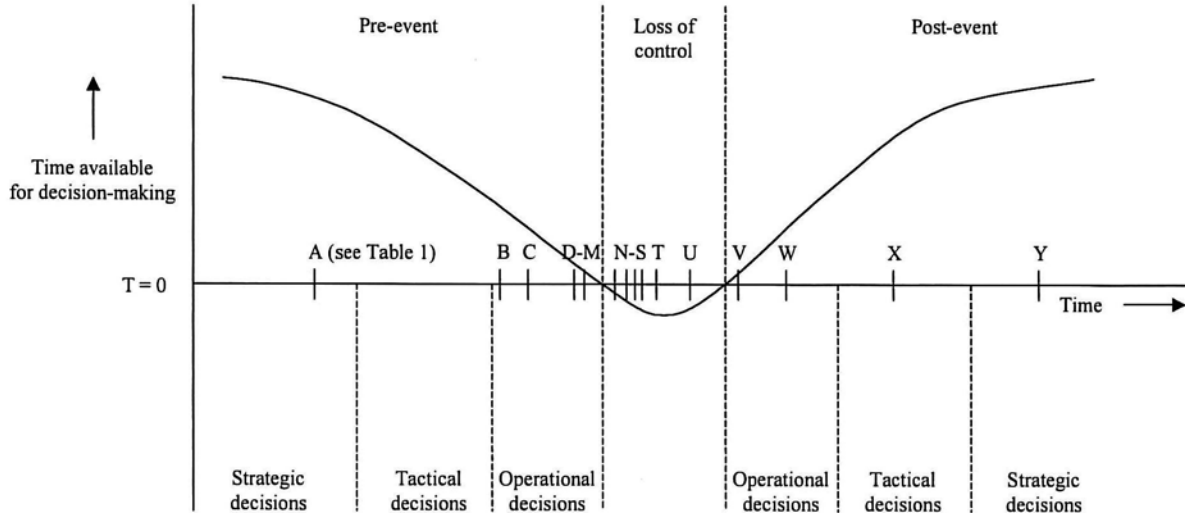

Figure 63. Time line of the train collision at Amsterdam Central Station, 2004.

The Collingridge dilemma can not only be identified at the beginning of the life cycle of a system. There are also examples of this dilemma at the perceived end of it. Some designs have been made obsolete before their time. They were forced into obsolescence by the introduction of new designs. Once almost gone their reintroduction when deemed necessary was very costly. The electric tram or streetcar is a typical example. Despite potential for innovation and fundamental design changes, in the 'fifties' of the 20th century the electric tram almost disappeared from the streets of many cities, being ousted by the mass introduction of the motor car and motor bus. Nowadays the tram is brought back at considerable cost because of the negative effect of the road traffic to the environment in the cities.

The Collingridge dilemma arises when there is a lack of identification of knowledge deficiencies and subsequently a lack of understanding the hidden threats of these deficiencies. This lack of understanding the threats can lead to a prisoner's dilemma, as indicated by Richard Tay. In his paper[5] he showed how using the classic prisoner's dilemma framework in game theory the emphasis on occupant protection may result in a pareto inferior outcome.

Pareto efficiency, or Pareto optimality, is a state of allocation of resources in which it is impossible to make any one individual better off without making at least one individual worse off. The term is named after Vilfredo Pareto (1848–1923), an Italian engineer and economist who used the concept in his studies of economic efficiency and income distribution. The concept has applications in academic fields such as economics, engineering, and the life sciences.

Pareto improvement is defined to be a change to a different allocation that makes at least one individual better off without making any other individual worse off, given a certain initial allocation of goods among a set of individuals. An allocation is defined as "Pareto efficient" or "Pareto optimal" when no further Pareto improvements can be made.

Pareto efficiency is a minimal notion of efficiency and does not necessarily result in a socially desirable distribution of resources: it makes no statement about equality, or the overall well-being of a society. The notion of Pareto efficiency can also be applied to the selection of alternatives in engineering and similar fields. Each option is first assessed under multiple criteria and then a subset of options is identified with the property that no other option can categorically outperform any of its members.

Shifting the relative emphasis from increasing occupant protection to non-aggressiveness of a vehicle, however, is likely to improve the environmental quality as well as reducing road accidents. Because of the prisoner's dilemma this shift will not take place despite the rational arguments in favour of it.
Also presumed positive aspects of an innovation can dominate the debate. Sometimes scientific research can take many years and is not always offering a single view on the consequences of such a new development. What we can observe when looking at a Collingridge dilemma is that two movements can occur simultaneously, as exemplified by the Cynefin model, figure 64.

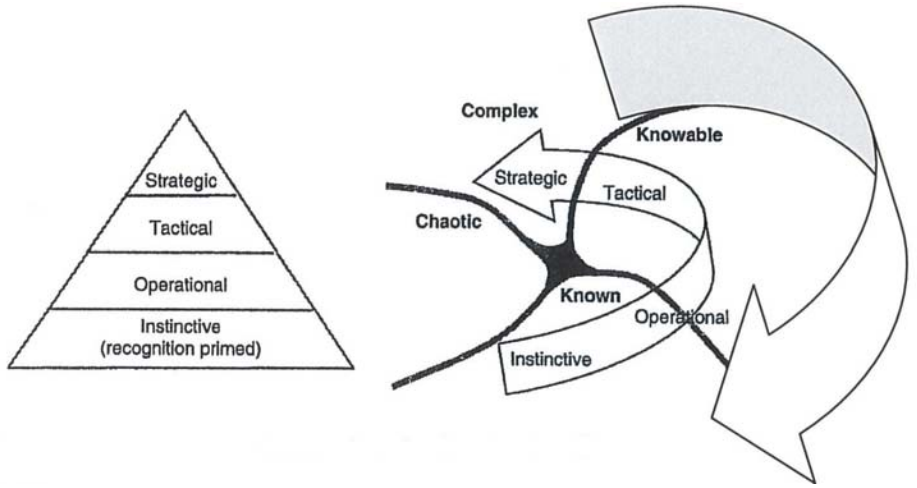

Figure 64. Collingridge dilemma in relation to Cynefin.

Development of a new design follows the outer (clockwise) movement, which is in effect the way the Collingridge dilemma itself develops. Over time through experience the designers learn more and more about the behaviour of the system they designed. Reaction from society follows the inner (anti-clockwise) movement, once a design becomes known to its potential users and the system becomes increasingly integrated in society. Both developments can enter the chaotic state, where the clash between them can result in a George dilemma that emerges at the end of the process that Collingridge describes. When the time dimension is not observed these developments fail to show themselves to the operator(s) or designers, resulting in a fall-back to a George dilemma.
Robert Meyer[6] gave another good example of a safety dilemma: 'If a disaster wipes out a town, we do not concede the risk and build elsewhere. *We rebuild in the same place*. Now, in principle this could work if the buildings we constructed in the same location were impervious to the kind of hazard that first destroyed them, but more often than not that is not the case. The reason, simply, is that doing so would require us to engage in a kind of long-term thinking that we have not had much need for over the millennia: that of seeing merit in investing resources in preventive actions whose benefits are unlikely to be realized in the short term.
And here is the final straw: because the limited investments we make in mitigation and prevention are not completely *in*effective, we are censored from viewing the limited damage imposed by mild—and more common—hazards that previously served as effective reminders of the riskiness of our environment. Add to the mix an expanding population exposed to peril and one has the perfect potential storm—a society that is unaware of the accelerating levels of risk that it has exposed itself to' according to Meyer.

The focus of science is primarily aimed at explaining and understanding the functioning of a system, instead of also paying attention to the possible future disfunctioning of it. The latter is often seen as the responsibility of the engineer in his role of designer of a technological system. Unfortunately as Petroski has shown[7] when engineering on the edge of what is possible, failure cannot be avoided and often serves to understand the functioning of a system and helps to improve it.

A key idea followed in the software and system safety community is that an identified hazard is best dealt with by changing the requirements of the system so that the hazard does not occur. This modus operandi creates a serious dilemma. The hazard identification that is needed in order to know what hazards to avoid, is best done after the code has been written, because only then are the potential effects of any particular stimulus, event, et cetera, deducible. However, if the response to the identified hazard is to change the requirements, then this requirements change will happen only after the code is written. Such changes are both expensive and dangerous. So a means to identify all hazards at the requirements analysis stage is needed.

If the engineer has enough leeway important failures will occur in the test phase of a system, leading to fundamental changes thus improving the safety and reliability of the system. If not a latent fault or weakness in the design can lay dormant for many years until it emerges with catastrophic consequences, see §5.2.1 the Amsterdam metro derailment of 2008. Such an experience changes the way we look at these systems at a time when change is slow and difficult to achieve.

The Millennium problem shows what can happen when a potentially unstable system continuous to be upgraded and adapted. Billions had to be spend globally to counteract potential threats of important system failures. Systems that should have been renewed years before, because when they were designed it was never envisaged that they would still be operational in the next century. Now 16 years later we still cannot determine what would have happened if we had failed to address this potential problem.

Putting Collingridge in a time perspective you can observe that when there is ample reaction time without any sense of urgency, the Collingridge dilemma emerges. When reaction time is running out decision making can be dominated by the George dilemma. This is caused by the fact that an event is described by a timeline, whereas a system is described by transition times. You need different knowledge and different skills to address these two components.

The principal question to be asked when dealing with Collingridge is: how much leeway is available to the engineer when change is required and how predictable is the influence of any envisaged change? The George dilemma on the other hand is caused by the uncertainty of the outcome of decisions at system level in which technological properties are only one of many aspects to be taken into account. In other words Collingridge is dealing with avoiding damage, whereas George is dominated by the fact that whatever the decision given a matter of emergency, damage is unavoidable.

It can be argued that the George dilemma is not only a possible outcome of a Collingridge dilemma but also one of the triggers of it. Developing a new technology is costly and time consuming. There is a continuous economical and/or societal pressure to get it to work and market it as soon as possible. If the developer takes time to test his system as much as possible he can run the risk of a competitor coming up with a similar innovation or it has been overtaken by new developments. If on the other hand the new technology is put on the market too soon teething troubles can give it such a bad image that it will lose the market.

One way of dealing with such dilemmas is implementing the Citadel principle. Using that principle the dominating question changes from what could happen if the systems gets implemented to what is it that should not happen when the system is implemented.

6.4 Resilience and resilience engineering

Dilemmas like the ones formulated by Collingridge and George as shown in the previous paragraph are not unique, they tend to occur often when the underlying concepts are not clearly defined. These dilemmas appear to be unavoidable and tend to result in no-win situations. The outcome of such dilemmas is a somewhat blurred image of the factual situation followed by compromises, whereby either discrepancies are not resolved but smoothed out at a level of detailed engineering and operational practice (Collingridge) or they result in decision making accepting that some form of damage appears to be unavoidable. Therefore understanding the concepts and architecture in earlier stages of design is just as important as making them applicable later on. One of the relevant concepts from an engineering point of view is the notion of resilience and its applicability.

The basic principles of resilience engineering are described in 'Resilience engineering in practice' by Hollnagel et al. They define the difference between 'classic' safety management and resilience engineering as[8] 'the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions'.

Resilience engineering requires that the system is anchored in distinctive conditions whereby each of these conditions contains safety critical characteristics, such as envelope protection (design envelope versus operating envelope). One of the aspects of a crisis is that there is no longer protection of the design and operational envelope resulting in an either unrecognised or unidentified and therefore uncontrolled escalation of the crisis. This is what Hollnagel calls 'emerging situations'.

It is necessary to acknowledge these emerging situations. An example of an emerging situation is the famous quotation of former US Defence Secretary Donald Rumsfeld[9]: 'there are known unknowns. We know there are things we don't know. There are also unknown unknowns. The ones we don't know we don't know.' This example shows the necessity to take care of transparency whereby the system stays away from the George dilemma (§2.2).

In resilience engineering failures are not synonymous with breakdowns or malfunctioning of the normal way in which a system is supposed to behave. Instead they represent the ability to adapt to the emerging real world complexity. Emergence is an important concept in resilience, meaning that simple entities because of their interaction and feedback, their cross-adaptation and cumulative change, can produce unexpected complexities when they work as a collective. Small changes in the initial state of a complex system can drastically alter the outcome.

According to Dekker et al[10] 'the systems perspective of living organisations whose stability is dynamically emergent rather than structurally inherent, suggests that safety is something a system does, not something a system has. Failures in the systems perspective represent breakdowns in adaptations directed at coping with complexity: it is related to limits of the current model of competence, and, in a learning organisation, reflects a discovery of those boundaries (which in dynamic operational environments are shifting most of the time). The aim of a resilient organisation is not stability but sustainability'.

The way we look at accidents has changed over the years. Accidents were initially looked at as the (inevitable) conclusion of events, where human errors were seen as causes or contributors. The operator failing to work according to the rules was not seldom criminalised. It took some time before questions were being raised why he wasn't obeying the rules, thus introducing human factors. Then came the notion of systems becoming so complex that they become unpredictable. Accidents can emerge from a confluence of conditions aimed at the pursuit of success, yet in reality bringing unexpected failure.

There are two schools regarding modelling of accidents. The linear school models accidents as the outcome of a series of events in a complex system. The risk needs containing and the usual way of doing that is by introducing barriers aimed at stopping negative developments such as potential accidents. The barriers separate the object-to-be-protected from the hazard by a series of defences. These models suggest a firmly rooted Newtonian vision of causes, especially the symmetry between cause and effect. Really bad causes must result in really bad outcomes.
To understand how something works these models mostly look at the disseminating parts. Macro properties of a system such as safety are a function of the lower order components or subsystems that are its building blocks. The assumption is that safety can be increased by improving the reliability of each and every component of the system. If the components do not fail, neither will the system as a whole. The much quoted Swiss cheese representation by Reason (figure 65) is an example of a latent failure model.

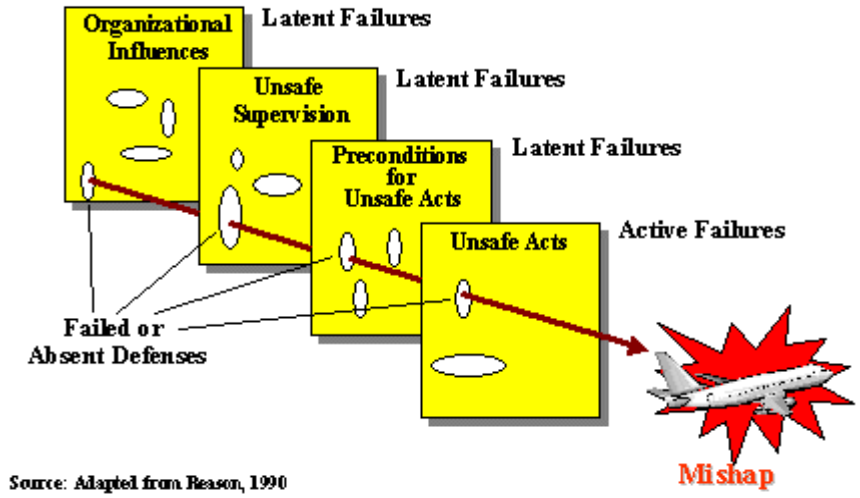

Figure 65. Example of the Reason model and Accident Causal Chain

Although such models help to explain why accidents have happened, they fail in one important way. These models can explain why an accident happened and help to visualise a sequence of events, but they cannot explain why a similar system (or the same system) functioning under near identical conditions didn't crash. If it can be represented in such a simple way, why did the accident occur in the first place?[11] It is not the models that fail, it is the knowledge derived from them that sometimes fails to create an escape from an accident situation. We interview those involved in the mishap. Did we bother to interview those who did not crash under similar circumstances?
The second school of thoughts regarding accident is the complexity systems school. They view systems and their behaviour as a whole as the unit of interest and analysis. They abandon Newtonian ideas about symmetry between cause and effect. Well know theories are:

- Normal accidents theory
- Control theory
- High reliability theory
- Resilience engineering

Interactive complexity is the notion of component interactions that are non-linear, unfamiliar or unplanned. They are either invisible at first or not immediately comprehensible for the operators[12]. The **Normal accidents** theory as proposed by Perrow[13] indicates that the more tightly coupled and complex a system is, the more likely it is to fail in an unpredicted way, thus creating a 'normal' accident. Given the characteristic of the system involved, multiple failures which interact with each other will occur, despite efforts to avoid them. Perrow said that operator error is a very common problem, many failures relate to organizations rather than technology, and big accidents almost always have very small beginnings. Such events appear trivial to begin with before unpredictably cascading through the system to create a large event with severe consequences.

One important danger of the ability of organisations to protect themselves from normal accidents is the tendency to create detailed plans for emergency situations, unexpected problems and developments. Sometimes they are called 'fantasy documents' that fail to cover most possible accidents , lack any historical record that may function as a reality check, and are soon obsolete because contact details change, organisation designs change et cetera. Even worse: fantasy documents can impede organisational learning as well as preparedness. They create a false sense of safety, according to Dekker et al[14].

Nevertheless false as these documents may or may not be, at least they make people think about the unthinkable. The problem lies in the unthinkable: something nobody guessed could happen in this way or to such an extent. Is there a defence against normal accidents? The suggestion is this theory is almost fatalistic.

An improvement on the previous theory is the Control theory. Accident models based on the control theory explicitly look at accidents as emerging from interactions among system components. These models usually don't look at what may or may not have gone wrong with the way the system was operated or organised. They look at the way systems are being controlled. According to Dekker et al[15] 'Accidents happen when components failures, external disruptions or interactions between layers and components are not adequately handled. When safety constraints that should have applied to the design and operation of the system have loosened or become badly monitored, managed, controlled'.

A further development came with the **high reliability** theory. This theory describes the efforts that have to be put in by everybody involved in an organisation to ensure consistently safe operations despite its inherent complexity and risks. According to Dekker et al[16] 'through leadership safety objectives, the maintenance of relatively closed systems, functional decentralisation, the creation of a safety culture, redundancy of equipment and personnel, and systematic learning, organisations could achieve the consistency and stability required to effect failure-free operations'.

Furthermore according to Dekker et al[17] 'the creation of safety involves a belief to continue operating safely. This belief is build up and shared among those who do the work every day. It is moderated or even held up in party by constant preparation for future surprise – preparation for situations that may challenge people's current assumptions about what makes their operation risky or safe. It is a belief punctuated by encounters with risk, but it can become sluggish by overconfidence in past results, blunted by organisational smothering of minority viewpoints, and squelched by acute performance demands or production concerns. But that also makes it a belief that is, in principle, open to organisational or even regulatory intervention so as to keep it curious, open-minded, complexly sensitised, inviting of doubt, and ambivalent toward the past'.

However, as safety improves when systems mature, the rate of improvement becomes asymptotic. It takes an increasing amount of effort to reach higher goals. The returns regarding improvements of safety become less and less optimistic, almost grinding to a stand-still. The probability of a high-risk accident seems to be almost reduced to nought.

This is where **resilience engineering** steps in. Resilience engineering looks at accidents not as a representation of breakdown or malfunctioning of normal systems functions. Rather it represents the inability to implement necessary adaptations to cope with the real world complexity. A system functions successfully when it has the ability of groups, individuals, and organisations to anticipate the way risks change before damage occurs in the real world. A resilient system is capable of adjusting its functioning prior to, during or following changes and disturbances, so that it can continue to perform as required after a disruption or a major malfunctioning such as an accident in part of the system, under continuous stresses.
According to Dekker et al[18] the four cornerstones of resilience engineering are:

- Knowing what to *do*, i.e. how to respond to regular and irregular disruptions and disturbances by adjusting normal functioning. This is the ability to address the *actual*.
- Knowing what to *look for*, i.e. how to monitor that which is or could become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, i.e. its own performance. This is the ability to address the *critical*.
- Knowing what to *expect*, i.e. how to anticipate developments and threats further into the future, such as potential disruptions, pressures, and their consequences. This is the address to address the *potential*.
- Knowing what *has happened*, i.e. how to learn from experience, in particular to learn the right lessons from the right experience. This is the ability to address the *factual*.

The ability to address the actual can be derived from the following distinction of threats[19]:

1. Regular threats that occur so often that it is both possible and cost-effective for the system to develop a standard response and to set resources aside for such situations.
2. Irregular threats or one-off events, for which it is virtually impossible to provide a standard response. The very number of such events also makes the cost of doing so prohibitive.
3. Unexampled events, which are so unexpected that they push the responders outside of their collective experience envelope. For such events it is utterly impracticable to consider a prepared response, although their possible existence at least should be recognised.

The ability to address the **actual** depends on whether threats or events can be imagined, on whether it is possible to prepare a response, and on whether it is cost-effective to do so. The marginal costs of the extra safety thus gained can be high and must be weighed against other safety priorities, which introduces the notion of the value of statistical life. Such readiness only works for regular threats. Does that mean we can disregard irregular threats? By no means can we do so, in many cases society wouldn't accept that. Apparently they must be dealt with in a different manner.
Generally it is only practicable for a system to be ready to respond to regular threats or sometimes only a subset of these. A possible solution is monitoring for what may become **critical**, and use that to change from a state of normal operation to a state of readiness when the conditions indicate that a crisis or failure is imminent. If a system can make itself ready (active) when something is going to deteriorate, rather than remain in a state of readiness (passive) more or less on a permanent basis, resources may be freed for more productive purposes. This change in state of the system does require reconfiguration time to change to a state of readiness. Also the identification of the impending event must be accurate to prevent that preparations are made in vain and resources are wasted or wrongly allocated.
In general it makes sense to look at the immediate future for what may go wrong. Less obvious is that there is an advantage to look further ahead as well, also when the system is in an apparently normal state. This is looking for the **potential**.

The difference between monitoring and looking ahead is not just that the time horizons are different (short versus long), it is also done in different ways. In looking for the potential the goal is to identify possible future events, conditions or state transitions both within and outside the system that are best to be avoided. While monitoring tries to observe regular threats, looking for the potential targets the most likely irregular threats.
Every modern safety-critical system must be capable of learning form experience. This requires knowing what has happened, the **factual**. Sometimes this is incorporated in law, such as the Dutch Railway Act[20]. Straight forward as it is, it requires careful planning and sufficient resources. It also depends on the agreed scope of learning: which events are taken into account, how are they analysed and understood and when and how often learning takes place. And above all: what is the focus of learning: individual or organisational?

6.5 Putting resilience engineering in perspective

Resilience engineering addresses all the conditions as described in §6.4 in a specific way. However, in every condition the time factor is important. You need time to address the actual, just as time is needed to ascertain the factual. Above all you need time to monitor for the critical. The time factor is obvious when looking for the potential. Even learning requires time. What do you do with the current system during the learning phase? Is there enough time to await the outcome of the studies? Therefore resilience time is an important notion in the process of resilience engineering.
The Cynefin model as presented by French (figure 66) combines the Reason model with the behavioural model by Rasmussen:

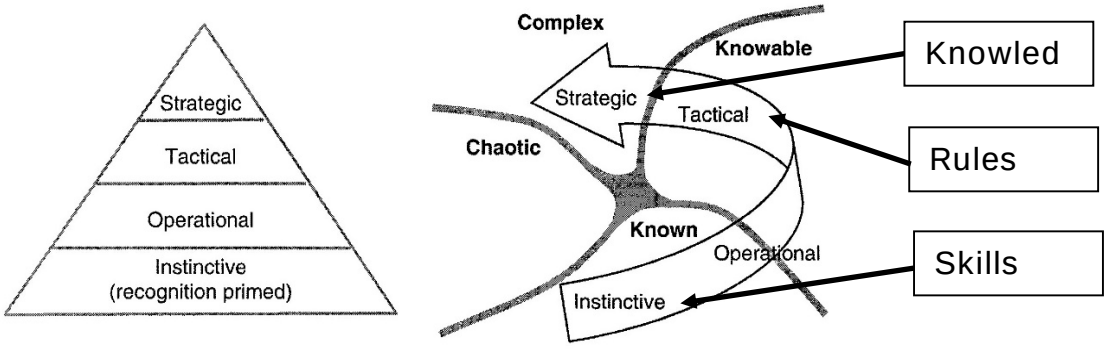

Figure 66. Reason model combined with the Cynefin model

The Known (operational level) area based on instinctive decision making predominantly relies on the skills of the operator. In few cases is any management involved here. The knowable area at tactical level relies on the set rules and the knowledge of them and correct application of these rules by the operators and managers. The complex area becomes a strategic matter where much depends on the knowledge of the operators and (senior) managers. There are indications that show the boundary from Complex to Chaotic appearing to be weak.
Returning from chaotic to complex can be difficult though. In practice there are several cases where this appears to be a tough barrier, such as the international financial crisis that emerged from 2008. All the financial expertise could not prevent a collapse of financial markets and bankruptcy of some large banks. The EU is still struggling to recover from the effects of this crisis, as a recent stress test of European banks indicates.

On the other hand the Qantas flight 32 example shows that it is possible to return from chaotic to complex if the knowledge is there and above all if there is time for the crew to rethink the whole situation (critical, actual and factual) and relearn the system as it is operating at the time. They didn't rely on skills which would have been an instinctive reaction that in a way would have been logical.
Something similar can be seen at the lower side of the Cynefin model. The Air France flight 447 shows that it is easy to get from known to chaos, almost unnoticed. Getting back might seem not to be difficult, yet there looms a trap. Split second instinctive decision making avoids a thorough analysis of the situation. It is based on first impressions. Recovery is conditional depending on the ability to avoid the danger of giving in to (false) instinctive reaction, thus increasing the chaos.
Such an instinctive reaction has cost the lives of most passengers in the Kaprun tunnel fire[21]. Only the professional fireman who was a passenger on board managed to control his emotions and relied on routine drill skills. He recognised the true danger (the threatening flash-over) and fled downwards from the train initially towards the fire, followed by a few fellow passengers. In the Air France case the crew had no answer to the chaotic situation and fell back on instinctive decision making, resulting in a situation where they got stuck in chaos because they applied the wrong skills based on what they thought was happening and not on what the factual and actual situation was.
The Amsterdam 2004 train crash (see §5.2.2) is another example of the strong barrier preventing a system from escaping from chaos. The system as a whole was already in chaos some minutes before the accident occurred. Yet the chief players (train dispatcher, train driver) continued to rely on their skills unaware of the increasingly unstable condition of the local rail system, resulting in the system getting stuck in chaos, thus making the subsequent train collision inevitable. In fact in the Amsterdam case the skills prevailed over the rules requiring a specific minimum separation in time between two trains. This same phenomenon can be seen in the Amsterdam 2012 train crash. Again skills prevailed over rules in a chaotic situation. The resulting train crash cost the life of one passenger and injured over 200 people on board the two trains.
Cognitive resistance against change and the reconfiguring of mental frameworks can be explained as a phenomenon that external signals are recognised but only after a long time result in adaptation of existing mental frameworks[22]. Cognitive resistance is seen by him as the phenomenon that external signals are recognised, yet they or not used at all or only after a long time to adapt existing mental frameworks.
Analysis of these accidents requires the acknowledgement that you need to look not just at the operational level but at the other levels (tactical and strategic) as well. Also in order to describe the actual and factual situation you need a systems approach and understand the dynamics of the system. If there are conditions for which there are no fall-back strategies, what about precaution? How many fall-back strategies are available?

- Designed and build into the system?
- Trained?
- Supervision?
- Trend analysis (management)?

And above all: what happens if the fall-back strategy creates another dilemma, such as the need to reduce train traffic around Amsterdam Central in April 2012 because of infrastructure maintenance versus the economic driven wish to run as many trains as possible? One of the characteristics of a safety critical system is that the boundaries as shown by French between normal operation and chaos are weak. What policy decision making instruments are at hand to safeguard the system from crossing boundaries and drifting into chaos and subsequent failure?

Is (part of) the system recognised as safety critical and if so, why is it so? If not, what makes the owners of the system so sure about that? All these questions need to be asked as early as possible and that leads to the DCP diagram, figure 67.

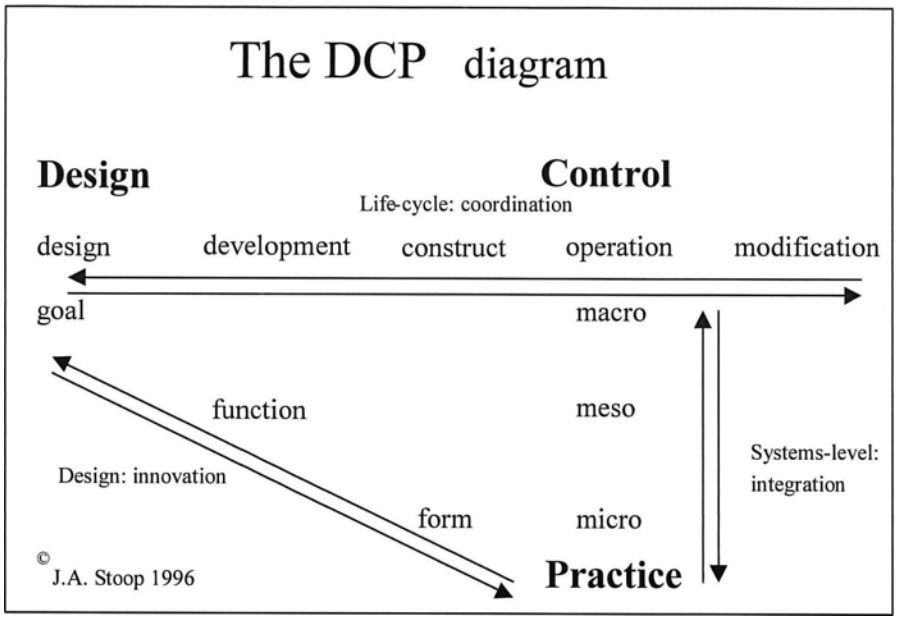

Figure 67. DCP diagram by Stoop

Resilience must be determined in the design stage of a system. Resilience engineering develops the concept to the construct and the form that emerges from of it. Additional resilience engineering is required when the system is approaching the boundaries of its original design envelop. Minor changes can have major consequences! Above all practice shows as can be learned from this research that it is important to incorporate the aspect of the time dependency (the hidden dynamic properties of the system) at each stage of the design process.
It is important to take the aspect of human behaviour into the design of the system. The cases described in this thesis show that in a crisis situation the only way back from the knowledge level in Rasmussen's model to the skills level is through the chaos situation (figure 68). This requires some form of mental resilience.

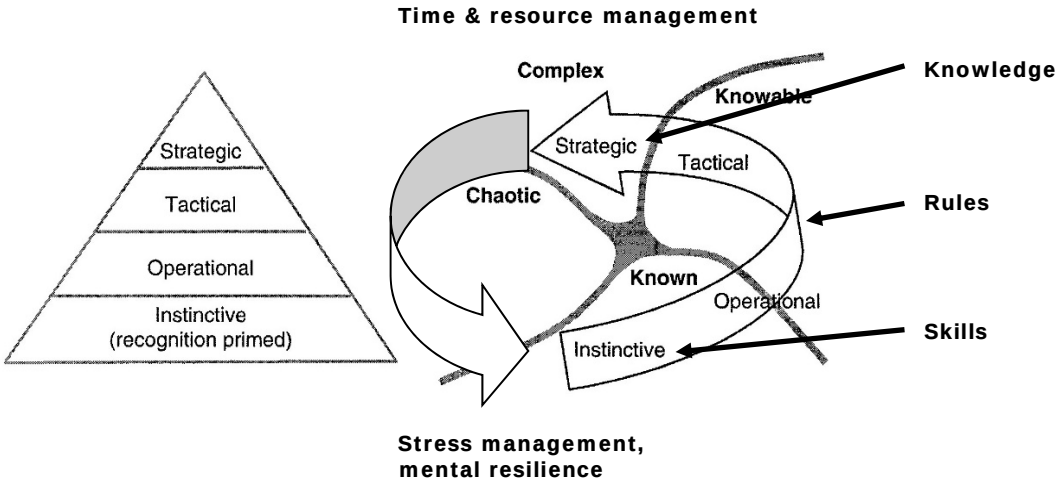

Figure 68. Rasmussen's model combined with the Cynefin model modified by Beukenkamp

The question is, what is needed to control the chaos: more rules and procedures? Or perhaps a different approach?
According to Beukenkamp[23] there are five stages in human behaviour during catastrophes:

1. The people involved are not aware that a catastrophe is developing.
2. In this stage the frequency bias occurs: there is widespread disbelieve, 'this can't happen to me'. The catastrophe is mentally denied.
3. The catastrophe is recognised but its full scale is not understood. This creates what is creates what is called 'negative hysteria'. People become either apathetic or extreme rational. At this stage actions are predominantly instinctive based on known skills.
4. The people involved have become aware of the full scale of the catastrophe, the factual situation. In this stage the first reactions are visible, either rationally or irrationally. The first actions are followed by others who had remained passive until then (following behaviour).
5. The following behaviour leads to exceptions (again some rational, other irrational). These exceptions are followed by others.

Reverting to the acceleration in time as shown earlier in figure 30 (§5.2.2), it can be seen that this can be combined in two ways:

Event phase diagram (combination with Rasmussen)

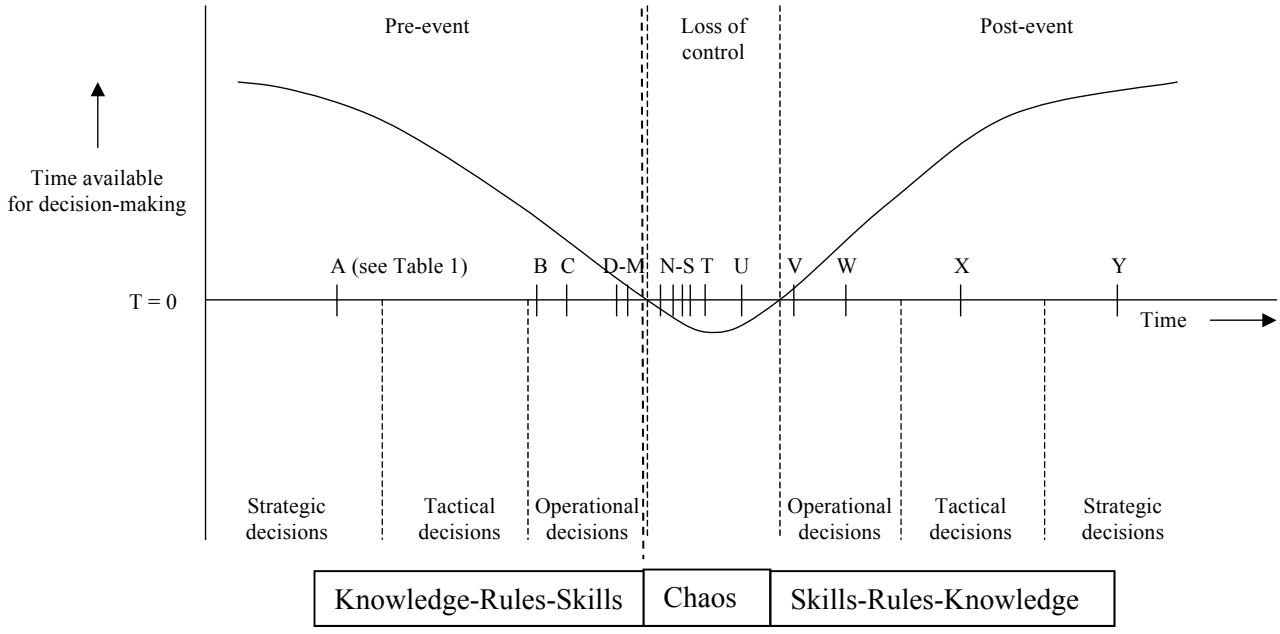

Figure 69. Beukenkamp critical time model combined with the Rasmussen and Cynefin

System phase diagram:

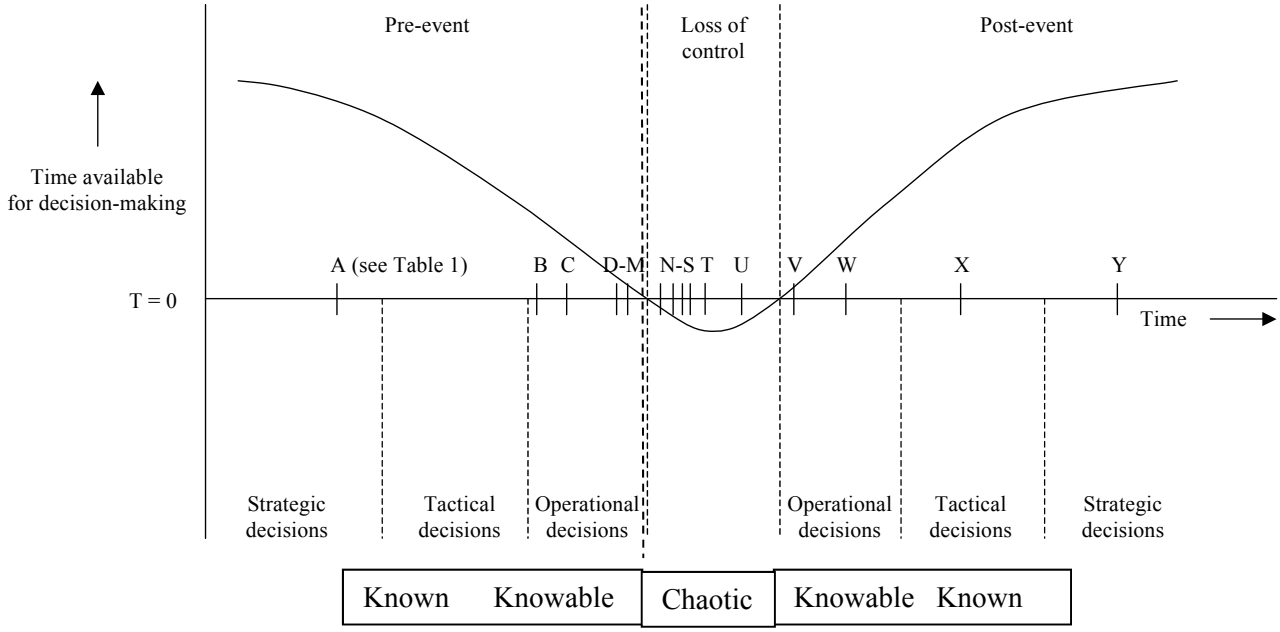

Figure 70. Beukenkamp critical time model combined with French

There is an important distinction between figure 69 and 70. Figure 69 focuses on events, whereas figure 70 looks at the system itself and its transitions. Events have a time line which is dominated by a sequence of events, whereas transitions have transition times which are discrete events by nature.
It is important to test the behaviour of vital systems such as digital networks, power supplies, data storages and financial systems under stress. This is often done using discrete-event simulation. A discrete-event simulation models the operation of a system as a discrete sequence of events in time. Each event occurs at a particular instant in time and marks a state transition in the system. Between consecutive events, no change in the system is assumed to occur; thus the simulation can directly jump in time from one transition to the next.
This contrasts with continuous simulation in which the simulation continuously tracks the system dynamics over time. Instead of being event-based, this is called an activity-based simulation; time is broken up into small time slices and the system state is updated according to the set of activities happening in the time slice. Because discrete-event simulations do not have to simulate every time slice, they can typically run much faster than the corresponding continuous simulation.
A more recent method is the three-phased approach to discrete event simulation. In this approach, the first phase is to jump to the next chronological event. The second phase is to execute all events that unconditionally occur at that time (these are called B-events). The third phase is to execute all events that conditionally occur at that time (these are called C-events). The three phase approach is a refinement of the event-based approach in which simultaneous events are ordered so as to make the most efficient use of computer resources. The three-phase approach is used by a number of commercial simulation software packages, but from the user's point of view, the specifics of the underlying simulation method are generally hidden.

It is important for a timeline of events to understand the underlying knowledge (competence) component of the operator(s). Which skills are required, which knowledge of the rules is required including how they apply and which factual knowledge of the behaviour of the system is available? Deficiencies in the general knowledge/competence component form the basis for the George dilemma.
For state transitions insight in the nature of knowledge deficiencies and their importance (specially re the uncertainties, the unknowns) are relevant. If they are not clear at an early stage of the development, they can result in the Collingridge dilemma and others, see §6.3. One of the purposes of accident investigation is to identify these knowledge deficiencies. In turn they can serve to trigger new fields of science.
Practice has shown many times that it is almost impossible in simulations to willingly create the chaos, the stress that occurs in real catastrophic situations, and the sense that you are going to die. Phase 4 and 5 of human behaviour as described by Beukenkamp[24] are determined by the element of chance. In these phases group dynamics can be seen above all based on emotion. What is done by the first person to react triggers similar behaviour by others.
Training should be aimed at emotional qualities, next to cognitive qualities. The reason for this is that in the chaos phase there is very little time for thinking. Emotional behaviour slows down the thinking process and turns it into haphazard actions. Yet according to Beukenkamp[25] the physical reaction in the human body (the stress factors such as the adrenaline boost) makes it possible to do some quick thinking if only you are capable of structuring that thinking.
This notion is underlined by the research done by Gorter et al (Project Samurai Pilot)[26]. Their recent research shows an intra-subjective (bottom up) approach. According to them it is important to introduce 'techniques that allow pilots to reduce the emotional charge, which can be experienced during novel life threatening situations, in order to maintain full control over their rational thinking'[27].
The relation between stress and performance is known as Yerkes-Dodson law, illustrated by figure 71. Furthermore Gorter et al state: 'while pilots receive ample training in simulators for emergency situations and failures, they do not receive training in which they can effectively self-regulate their physiological responses in said situations'[28].

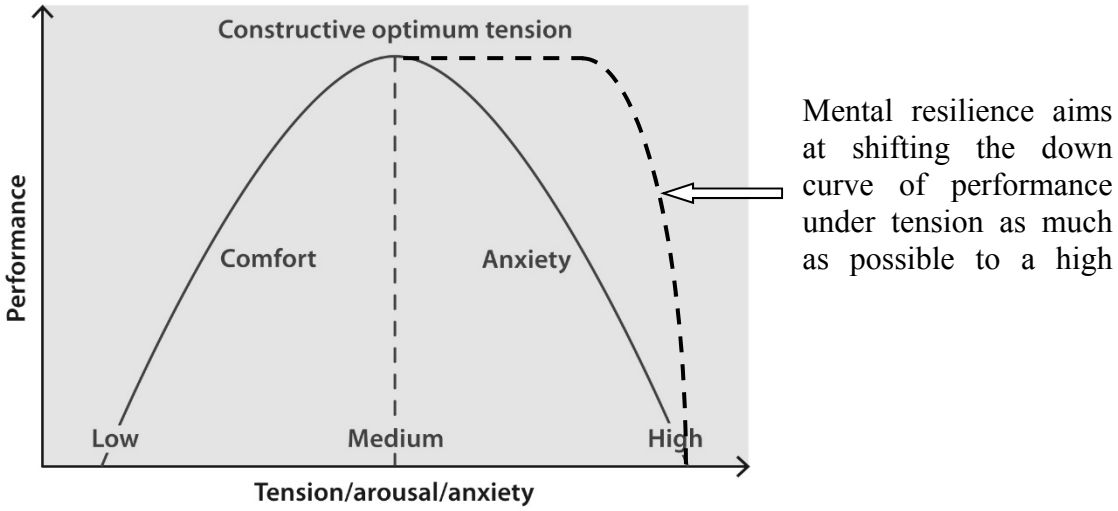

Figure 71. Performance curve as a function of arousal (stress) (Yerkes-Dodson law, 2011)

In 2010 the Dutch Railway Inspectorate supervised the commissioning of the new tram tunnel for tram route 19 in Den Haag (Sytwende tunnel). One of the required tests was an emergency drill in combination with the police and the fire brigade. The test was setup by the designers of the tunnel in cooperation with the local fire brigade. At the last moment the inspectorate intervened and changed the test scenario considerably. The organisers of the test were instructed not to inform the participants of the test.
The 'passengers' in the tram were taken by surprise about what happened and started to panic. Their main drive was to get out of the smoke and the tunnel as quickly as possible. They ignored verbal instructions by the intercom system and forced their way out through an electromagnetically locked door. This door formed the barrier between the tram tunnel and the road tunnel next to it and should not be opened by the tunnel operators until the road tunnel was clear of traffic. As suspected by the inspectorate the magnets holding the escape door shut could not withstand the force of a number of people with high adrenaline levels. From that moment on chaos reigned supreme at almost every level of the system. The sober conclusion by the commanding officer of the fire brigade was that apparently a complete review of emergency plans was necessary.
In his recent study Mohrmann addresses the top-down intersubjective recovery potential in such situations[29]. Furthermore Mohrmann indicates the problem of automation of control systems[30]: 'automation brings with it a paradox: it provides crews with necessary assistance in managing the complexity of fourth generation airliner operations, but at the same time dissociates the crew from those operations. The problem that arises from this paradox is that crews are placed 'out of the loop'. It becomes increasingly difficult for them to be fully aware of the aircraft's state and situation, which in turn inhibits their ability to effectively manage the aircraft and its systems when asserting manual control in the event that automation falls short of self-recovery'.
The major derailments of freight trains near Borne (November 2013) and Vleuten (March 2009) in the Netherlands show this to be a problem not confined to the airline industry. In both cases the automatic traction control system of the loco was more than capable of compensating for the extra drag caused by the partly derailed freight train. The train drivers were not aware that something was seriously wrong with their train until they were stopped by the train controllers. By then major damage had been inflicted to the infrastructure and the train itself.
It was control of emotions that prevented a serious rail incident developing into a catastrophe[31]. March 29, 2007 a delayed Dutch Railways intercity from Leiden to Utrecht passed a signal at danger near Harmelen junction, west of Utrecht. At that point quadruple tracks merged into double track. A freight train was running on the track next to the intercity and was on its way from Rotterdam to Utrecht. The signals for the freight train were showing a green aspect ('proceed at maximum allowed speed') because it had been given priority over the delayed intercity at the junction of the two tracks by the automatic route setting system.
When the freight train approached the junction the driver became aware of the intercity overtaking him on the other track. It suddenly dawned on him that the intercity next to his train was going too fast to stop in time. Although his signals were showing a green aspect which allowed him to proceed at maximum allowed speed, he made an emergency braking application. Moments later his signal changed from green to red as a result of the intercity passing a signal at danger and coming to an emergency stop in his path. The freight train stopped in time for the signal that now showed an unexpected red aspect.
This instinctive action avoided a collision between two trains that could have resulted in a major catastrophe[32]. By controlling his emotions the driver recognised the (hidden) chaotic state of the system. Through chaos the driver changed to the knowledge level and acted accordingly based on his skills.

These examples show the importance of the autonomy of the operator. It indicates a new fulfilment of the notion of situational awareness. Instead of accepting the deliberation as it presents itself to the operator, based upon the George dilemma a new set of deliberations is created eliminating that dilemma. The scope of the problem is determining the deliberations, whereby the focus on the process is replaced by the focus on the outcome based on professional judgment.
One of the problems with the George dilemma and other safety related dilemmas is that they force themselves upon the operator(s) and the responsible manager(s). They result from a process approach where the focus is on the process itself instead of the result where the context is dominating the problem. This can lead to an attitude whereby liability will be avoided at all cost (trying hard to satisfy everyone and every dilemma), thus reducing accountability.
However, if the focus is on contents of the problem a different outcome can result. This requires some basic skills from the operator/manager:

- Cognitive: being able to mentally approach a problem through a processes of perception, memory, judgment, and reasoning, as contrasted with emotional and volitional processes;
- Competent: being able to combine knowledge, attitude and skills at a sufficient level to do the job;
- Composure: emotional resilience, being able to remain calm and ready for action;
- Conscientious: focus on the problem, being meticulous. This results in a cognitive resistance against distracting factors such as the George dilemma.

The shift from a process approach to a contents approach is depending on:

- Degrees of freedom (available resources);
- Available time (resilience time!);
- The ability to combine system modes with mental states of the operator.

6.6 Conclusion

Research question 5: *'If existing methodologies are not adequate in dealing with issues regarding risk sensitive systems, which improvements are possible?'* can be answered as follows. First of all next to an objective risk analysis it is sometimes necessary to translate the subjective societal perception of risk by means of a threat analysis. Second it is necessary to accept that it is impossible to protect the entire society and all its risk sensitive systems at all cost. Some form of damage must be accepted as long as the vital parts of a system keep on functioning. In other words it is necessary to focus resources where they matter instead of spreading them thin.
It is also necessary to make the already known principles of resilience engineering more dynamic to contain the chaos in accidental situations. The transition from a state of high reliability to a state of chaos can be sudden and at times encountering little resistance. The citadel principle creates temporary stability in such a chaotic situation, thus buying time to restore order to chaos and reconfigure the system, which is the first step away from the state of chaos (the state of the unknowns) back into the known state. However, this only works if resilience engineering is coupled to the notion of time criticality. The notion of time criticality is of cognitive importance, because it buys time for the operator to reconfigure his mind set and adapt to the new unexpected situation.

Notes

[1] Ref. Collingridge, 1980
[2] Ref. Jaspers, 2010
[3] Ref. MIT, 2015
[4] Ref. Morozov, 2013
[5] Ref. Tay, 2002
[6] Ref. Meyer, 2010
[7] Ref. Petroski, 1992
[8] Ref. Hollnagel et al p. xxxvi
[9] 'There are known knowns' is a phrase from a response United States Secretary of Defense Donald Rumsfeld gave to a question at a U.S. Department of Defense (DoD) news briefing on February 12, 2002 about the lack of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups.
[10] Ref. Dekker et al p. 5
[11] Ref. Stoop, JAAM & Dekker: Accident modelling: no more cheese please.
[12] Ref. Perrow, 1984
[13] Ibidem
[14] Ref. Dekker et al p. 32
[15] Ibidem
[16] Ref. Dekker et al p. 38
[17] Ref. Dekker et al p. 39
[18] Ref. Dekker et al p. 54
[19] Ref. Westrum, 2006
[20] Spoorwegwet artikel 33 lid 2: 'De attesthouder past een adequaat veiligheidszorgsysteem toe, met behulp waarvan wordt gewaarborgd dat de spoorwegonderneming: d) procedures vaststelt en hanteert voor het nemen van corrigerende maatregelen bij afwijkingen en incidenten, alsmede voor het voortdurend verbeteren van het veiligheidsniveau met het oog op zich wijzigende omstandigheden *en op grond van opgedane ervaringen'*.
[21] The Kaprun disaster was a fire that occurred in an ascending train in the tunnel of the Gletscherbahn Kaprun 2 funicular in Kaprun, Austria, on November 11, 2000. 155 people lost their lives. Only 12 managed to escape from the fire and survived.
[22] Ref. De Boer, 2014
[23] Ref. Beukenkamp et al, 2003
[24] Ref. Beukenkamp et al, 2003
[25] Ibidem
[26] Ref. Gorter et al, 2014
[27] Ibidem, p. 7
[28] Ibidem p. 13
[29] Ref. Mohrmann, 2013
[30] Ibidem, p. 9
[31] Ref. IVW report, 2007
[32] January 8, 1962 not far from this location the most serious train collision in Dutch history occurred when at Harmelen junction an express train overran signals in dense fog and crashed almost head on into a local train. 91 passengers and two train crew were killed and 52 people were injured.

7. Conclusion: resilience time and the citadel principle

7.1 Introduction

The previous chapters have shown that there are a number of risk management techniques on hand which if used in the proper context and in proper relationship to each other are adequate to design, develop, build and maintain risk sensitive systems. Several of these technique show a somewhat static approach, others are more dynamic in nature. Although time is not ignored in some techniques, its true dynamism is not always understood. This chapter will show the findings of this research and its conclusions.

This most important finding is that the behaviour of a risk sensitive system is dynamic in time. This dynamism creates unforeseen uncertainties and unexpected failures. A system can be on its way to catastrophic failure at a point where it appears to be functioning at or above normal service level. Decision making in these systems is a continuous interaction between various levels of management and operation, each requiring time to act and interact. This research shows that time is an important hidden characteristic of risk sensitive systems, more in particular the notion of resilience time.

7.2 Findings and conclusions

Although aspects of safety and security are important in the process of decision making regarding risk sensitive systems, they are not always dominating the discussions about the design, construction and operation of these systems. They are susceptible to two major dilemmas, i.e. the George dilemma (regarding the conflict between political acceptability, economic viability and analytical correctness) and the SEE framework where safety (and security) have to compete with economic aspects and the environment regarding attention and most of all limited financial resources.

What hampers safety and security in these matters is that it is impossible to calculate and measure them directly, unlike (economical) costs and the environmental impact of a design. Safety and security can only be measured using an indirect approach based on statistical experience, in other words, it is a retrospective approach unlike the other two aspects which can be determined by a prospective approach. This statistical retrospective approach requires a proper systems strategy when dealing with uncertainty, because it is uncertainty that sooner or later dominates the performance of the system.

One option to control uncertainty is switching from collecting more data points (incidents/accidents) to an investigation in depth of each data point in order to better understand their dominating but sometimes hidden complexities. Thorough accident investigation and subsequent analysis are important to support this. Feedback from reality, serendipity et cetera are leading notions in such a diagnostic process. The explanatory power of system behaviour can also be deducted from case based analysis. Where to intervene based on what explanatory power is an issue that can be dealt with using the Citadel Principle.
There are three ways of dealing with uncertainty, depending on the nature of the uncertainty.

1. Scenarios can be of help when the effects are quite well understood but not the likelihood of occurrence.
2. When the likelihood of an occurrence is sufficiently known but the effects are not well understood, a sensitivity analysis is an accepted method of examining such a system.
3. Problems start when nothing is certain about a system, which is one characteristic of security related matters or emerging innovative technologies.

Another problem arises when a once stable and resilient system through changes in use and/or updates moves to a situation where the operating envelop is no longer within the boundaries of the original design envelop. The result can be described as drifting into failure, often unnoticed until it is too late to prevent accidents.
A novel approach as shown in this research, called the Citadel approach, can bring back stability in a system under such circumstances. It can buy time to reconfigure a system when it is showing abnormal behaviour. It can prevent catastrophic failure by implementing containment measures. It avoids the need for ad-hoc (panic) intervention at management level, where the operational expertise should be put to work to combat the emergency.
Emotional training in crises or catastrophes offers a way out of the George dilemma. In such a situation it is important to focus on the situation itself, not on the influences outside the system itself that dominate the George dilemma. Instead of accepting the unknown unknowns and act in a haphazard way the people involved restore rationality in their behaviour and focus on the known knowns.
Emotional training is helped by a resilient system, because such a system is designed to survive initial impact independent of the operator and the operators know that. There is time to become aware of the factual situation, to get out of the negative hysteria. Subsequently there is time to select the most effective skills to control it.
Systems with residual strength can be described as follows:

- Robust: it is virtually impossible to create chaos;
- Redundant: it is possible to avoid chaos;
- Reliable: the probability of chaos is acceptable and predictable;
- Resilient: it is possible to survive chaos with relative little damage.

Precaution is first getting a proper overview, the big picture, followed by getting insight into the various aspects of the (potential) problem. However, an often seen reaction is to accept accidents as something inevitable because in some cases systems are so complex that they are intractable.
In a way risk sensitive systems based on a probabilistic design appear to be hampered by a fatalistic way of thinking. It is suggested that we have to accept accidents as something inevitable even with catastrophic outcomes as long as the likelihood of such an occurrence is acceptably low. 100% safety does not exist. Safety is in practice an accepted level of unsafety. This may be true yet this thesis shows that given major failure there is no reason why there shouldn’t be major recovery avoiding substantial damage.

The consequences of emotional reaction in a chaotic situation were apparent around Den Haag and Rotterdam when on September 19, 2014 in the middle of evening rush hour (around 18.00 hrs) it was decided by the railway infrastructure manager and rail traffic control to shut down three important railway stations for emergency inspection and repair of points and crossings. The consequences were that within minutes train traffic in the west of the Netherlands came to a standstill thus causing serious delays to many passengers.
Subsequent investigation by the Railway Inspectorate into this major disruption revealed that the cause of the problem was emotional reaction at operational level not checked by adequate management at tactical and strategic level. Even more remarkable was the conclusion of the Railway Inspectorate that initially all the problems in the infrastructure were known and controlled at an acceptable level. It was a feeling of uncertainty in a situation with a known increased level of risk that triggered disproportionate actions by staff at operational level. These actions helped to create the chaos and inflate it to a level where they were no longer capable of controlling it.
A similar phenomenon occurred in 2010 following the eruption of the Eyjafjallajökull volcano on Iceland. Beginning of April 2010 this volcano erupted and created large ash plumes high in the atmosphere. Because of the prevailing jet stream this ash plume dispersed over much of north-western Europe. April 15, 2010 the UK Civil Aviation Authority decided to close the airspace over the UK, followed by other CAA's in Europe.
This had severe consequences for air traffic in much of Western Europe and transatlantic air travel. Most of it came to a halt between April 19 and April 23. Subsequently it became known that the risk from such an eruption was well know and understood being focussed on the performance of jet engines. Major airline companies such as Lufthansa and KLM carried out test flights during that shut down period. They returned with the conclusion that the risk to flight was minimal. Yet the major CAA's refused to review their policy of total risk avoidance.
As Giovanni Bisignani, IATA's CEO stated '*Airspace was being closed based on theoretical models not on facts. Test flights by our members showed that the models were wrong. Our top priority is safety. Without compromising on safety, Europe needed to find a way to make decisions based on facts and risk assessment, not on theories*'[1].
According to Rasmussen in a looming accident the level of human behaviour changes from skill based via rule based to knowledge based level. The Rasmussen model combined with the Cynefin model shows that the way back is almost inevitable through the chaos phase. It is therefore important to design and maintain the system and its operators in such a way that chaos can be controlled.
Chaos and the resulting stress can be difficult to simulate. Rules and procedures require some level of rational behaviour, a behaviour that is usually present during training (simulation) but appears to be sometimes lacking during the chaos following a real crisis. Therefore could it be better to shift from cognitive training to emotional training to restore rational behaviour when the danger of negative hysteria looms? Instead of acting on the unknown unknowns the operators involved can act on the known unknowns and even known knowns.
The Air France (§5.3.5) and Qantas (§5.3.4) cases are examples of this. In the Air France case the crew failed to understand that they were operating in a situation with many unknown unknowns. They lacked factual understanding of the actual situation due to a deficiency in their training. In the Qantas case the crew was well aware that they were dealing with many unknown unknowns. They managed to restore order in the chaos by working back from the known knowns, exploring their available options one by one. In general such a mental transition requires that the operators are trained in stress management techniques, see figure 69 and figure 71.

7.3 Recommendations

In order to make a risk sensitive system less susceptible to unanticipated catastrophic failure, the following points are recommended:

1. Each system already at the design stage should be analysed regarding its risk sensitivity, more specifically aspects such as resilience time, acceptable and non-acceptable failure scenarios, fall-back options et cetera.
2. It is important to design risk sensitive system in such a way that they are either robust, redundant, reliable, resilient or a combination of these properties.
3. Risk sensitive systems need stop lines regardless what scenario applies, defining the safety and security citadel, from which a controlled recovery of the system is possible.
4. Resilience time should become an integral part of the design, construct and practice environment of risk sensitive systems.
5. Emotional training is just as important as cognitive training to survive a chaotic situation: emotional resilience.

The first 2008 Amsterdam metro derailment (§5.2.1) shows that decision time can be a hidden factor undermining the design of a system. The Amsterdam train collision case (§5.2.2) introduces the notion of resilience time. The second 2008 Amsterdam metro derailment (§5.2.3) shows that accidents can be far more complex than thought of first. A system can appear to be behaving in a normal way whilst already being in a substantial damaged state. The Amstelveen tram/bus accident (§5.2.4) learns that it is important to check the operating envelop of a system against those of other systems that interact with it.
The case of the sliding trains at Leiden (§5.2.5) indicates that malfunctioning of systems not always results in effective remedial actions, again because time criticality resulting from design problems in rolling stock was not fully understood at operational level. It took several accidents to raise the awareness at management level that action was required.
The Qantas case (§5.3.4) is an example where the crew showed emotional resilience, thus avoiding haphazard instinctive behaviour. The Air France case (§5.3.5) is an example of acting on unknown unknowns, resulting in the instinctive impulsive selection of the wrong skills. The Den Haag railway disruption and Icelandic Volcano air traffic disruption show the importance of emotional training.
An important lesson to be learned is the way safety management systems address the aspect of the unknown unknowns. Their primary focus is on the known uncertainties. However, in what way do they stimulate investigation into the unknown uncertainties? Do they stimulate learning from hidden dangers? Or are they part of a system where the culture is to avoid knowing what we don't want to know let alone learn from it?
This thesis shows that a strategic reconnaissance is necessary when dealing with hidden dangers through unknown uncertainties and learning from their resulting catastrophes. It is important to view the system throughout its entire life cycle and not just focus on the safety management system in the operational phase under normal (anticipated) operational conditions.

7.4 Further research

This empiric research has shown the importance of resilience engineering as a tool of controlling the behaviour of risk sensitive systems. Resilience time and discriminating multiple system states have been identified as a hidden dynamic property. Further research is required into the behaviour of resilience time and the way it can be translated into mathematical models.
Furthermore it is important to study the transition from factor and event to vector and system. Is it possible to create mathematical models regarding resilience just as has been done regarding reliability?
On the other hand it is also important to translate resilience as an organisational tool into a more practical engineering tool aimed at both the physical and organisational design of the system into an integrated approach.

Notes

[1] Ref. Bye, 2011

8. Epilogue

This research started in 2004 following the aftermath of the 9/11 events. At the time the author worked for the Transport Research Department of the present Ministry of Infrastructure and the Environment. His profession was to research the societal consequences of the transportation of hazardous materials by road, rail and air and how to contain the risks involved. Next to that he became involved in security matters regarding national infrastructures, mainly because security was his old job in the Dutch Foreign Office where he worked until three weeks after 9/11. In 2007 he joined the Railway Inspectorate of the same ministry as senior inspector, doing incident and accident investigation.
Learning from feedback from operational practice in the railway field the pressures on restarting the transport system became apparent, the stresses emerging with all involved to do something. As this thesis shows in such circumstances it is important to control emotional reactions. It takes time to restore rational to chaos and consider the options. On the other hand this thesis also shows that the emotional factor and its stresses to create a more realistic emergency training and testing situation. A training scenario can be improved by introducing a gaming situation.
Furthermore this thesis shows the importance of empirical accident investigation. Much can be learned not only from going out to the wreckage site, looking for evidence, studying the analysis and interviewing those involved. Lessons can be learned as well from building a picture not only of what they did but also the circumstances in which they had to function, the emotions that were involved and why such accidents did not happen to others under similar conditions.
In many cases the outcome of such an investigation is that the accident should not have happened or the consequences should not have been so severe. That the signs of disaster waiting to happen were there for all to be seen. Is it therefore not so much a matter of why did it happen but more why could it not have been prevented? Why did these professional people at every level failed to see the signs that there was something wrong with the system? Why did they react in a way that exacerbated the problems instead of diminishing them?
Sometimes the official reports do not give answers to these questions or if they do so, the answers appear to be somewhat superficial, thus ignoring important learning opportunities, because at present engineering models are mostly based upon rationality. They seem to underestimate the influence of emotions on the part of the operator.

The Air France case indicates a possible knowledge deficiency regarding crew behaviour under stressful conditions that could have a similar impact regarding the way we look at such systems as the De Havilland Comet cases had (1952-1954) regarding the problem of metal fatigue and the Tenerife disaster (1977) had on crew resource management.
This awareness of a knowledge deficiency in the system that leads to unexplained failure changed the course of this research when it became apparent how often this could be observed in the aftermath of a serious accident. This thesis aims at shedding light how to deal with chaotic situations by looking at problems from a system perspective. In that way a condition can be created whereby chaos can be survived. This creates a solution, a way out to the George dilemma.
As Lemony Snicket put it[1] '*Assumptions are dangerous things to make, and like all dangerous things to make -- bombs, for instance, or strawberry shortcake -- if you make even the tiniest mistake you can find yourself in terrible trouble. Making assumptions simply means believing things are a certain way with little or no evidence that shows you are correct'*. It is this serendipity, the feedback from reality that shows a way out of the George dilemma.
This escape can only be achieved if the system is resilient. A resilient system requires the necessity to create stop lines from where recovery is possible rather than accepting total collapse if the likelihood is acceptably low enough, as is done in the probabilistic school of thinking, leaving room for fatalistic thoughts.

Notes

[1] Ref. Lemony Snicket, The Austere Academy

Samenvatting

Heden ten dage hebben wij een uitgebreide set aan wet- en regelgeving om veiligheid thuis en op het werk te regelen. We kennen veiligheidszorgsystemen om veiligheid op systeemniveau te verankeren. Voorts beschikken we over geavanceerde computermodellen om systemen te testen terwijl ze nog op de ontwerptafel liggen. Ondanks dit alles gebeuren er nog steeds ongevallen, ongewilde en ook opzettelijk veroorzaakte. Kennelijk is veiligheid als zodanig niet de belangrijkste kwestie in onze moderne westerse samenleving, maar het borgen van de veiligheid, dat is waar het om gaat. Vandaar de titel van dit proefschrift: 'Veiligheid veiligstellen' of in het Engels: 'Securing safety'.
Onze moderne samenleving is in toenemende mate complex en kwetsbaar. Daar staat tegenover dat onze kennis van de daarmee samenhangende risico's in de loop der jaren is toegenomen. Het is mogelijk door gebruik te maken van digitale risicoanalysemethoden om constructies te ontwerpen en te bouwen die nog maar twee of drie decennia eerder voor onmogelijk werden gehouden. Welke ontwerphulpmiddelen we gebruiken, hangt af van de kennis die we hebben van de desbetreffende systemen.
Eén ding is duidelijk: het is niet de bedoeling dat er ongevallen gebeuren. Toch zijn die niet altijd te vermijden, zoals dit proefschrift laat zien. Ongevallen kunnen het gevolg zijn van onopzettelijke inschattingsfouten door onvoldoende kennis en of inzicht in het feitelijk functioneren van het systeem, in het Engels aangeduid met het begrip 'safety'.
Ook kunnen zij het gevolg zijn van opzettelijk destructief handelen, zoals terrorisme, in het Engels aangeduid met 'security'. Deze begrippen moeten goed onderscheiden worden van het begrip risico, de blootstelling aan een gevaar of ongewenste gebeurtenis. Op deze begrippen komt dit proefschrift diverse malen terug. Vroeg of laat kan een systeem aan een of meer dreigingen worden blootgesteld. Schade is onvermijdelijk, maar is het ook onvermijdelijk dat de uitkomst fataal is?
Wat weten we eigenlijk van de gevolgen als dingen mis kunnen gaan en hoe betrouwbaar is onze kennis over de kans dat zo'n gebeurtenis zich voordoet? In de meeste gevallen is onze kennis goed vastgelegd en gedefinieerd, zowel met betrekking tot wat we weten als wat we niet weten. Het is de kennis wat we niet weten wat we niet weten (de onbekende risico's, het onbekende soms onvoorspelbare gedrag van een systeem dat volgt uit verborgen eigenschappen) dat een uitdaging vormt voor een adequate beheersing van risico's. Hoe bereid je je voor op het risico dat je niet kent?

De probleemstelling voor dit onderzoek is als volgt:

Het lijkt erop dat bestaand beleid op het gebied van risicomanagement tekort schiet om de rol van veiligheid op strategisch en tactisch niveau te borgen ten aanzien van grote infrastructuren, met als mogelijk gevolg een verhoogd risiconiveau zonder dat de degenen die hierover moeten beslissen zich dat bewust zijn.

Dat resulteert in het volgende doel van het onderzoek.
Ontwikkel een benaderingswijze die op systeemniveau zowel efficiënt als effectief is wanneer we moeten omgaan met het aspect van kleine kans/groot effect in relatie tot transportsystemen.

Hoewel risicobeheersing op strategisch (macro-) niveau goed begrepen wordt, lijken problemen op tactisch (meso-) en operationeel (micro-)niveau veel minder goed te worden begrepen. Dit wordt mede veroorzaakt door een gebrek aan kennis met betrekking tot het belang van de tijdfactor in kritieke situaties en de dilemma's die onder tijdsdruk opgelost moeten worden.
Er wordt daarbij soms de indruk gewekt dat sommige dilemma's onvermijdelijk en vrijwel onoplosbaar zijn. Dit proefschrift toont aan het mogelijk is uit zo'n ogenschijnlijk kansloze toestand te komen. Ook wordt hier aangetoond hoe belangrijk de verborgen invloed van de tijdfactor is in systemen met een hoog risicogehalte.
Dit onderzoek is niet zozeer gebaseerd op een theoretische benadering, gevolgd door praktijkproeven. Eerder het omgekeerde heeft plaatsgevonden: empirische studies (bestaande casuïstiek) hebben geleid tot onderzoek gericht op verborgen eigenschappen en het vinden van verklarende variabelen. De meeste casuïstiek komt uit de wereld van het Nederlandse vervoer. Hoewel dit ogenschijnlijk beperkt lijkt laat dit onderzoek zien dat de daaruit te leren lessen qua toepassingsgebied een bredere potentie hebben.
Hoewel 'resilience engineering' op zich niet nieuw is, is de manier waarop dat in dit onderzoek wordt toegepast wel tamelijk nieuw, omdat het resilience engineering omvormt van een tot op zekere hoogte statisch hulpmiddel met zijn zwaartepunt in de ontwerpfase, naar een dynamisch hulpmiddel op operationeel niveau in het dagelijks gebruik. Deze nieuwe benadering heet het Citadelprincipe. De belangrijkste verschuiving in denken is wegstappen van de vraag wat er zou kunnen gebeuren naar het begrijpen wat we per se niet willen dat er gebeurt ongeacht de oorzaak ervan. Op die manier wordt het omgaan met de onbekende onbekenden toch enigszins beheersbaar.
'To engineer is human' schreef Petroski in 1992. Slechts door het bestuderen van falen van een systeem leren we de goede lessen eruit. De uitdaging is niet alleen naar het verleden te kijken en een herhaling te voorkomen van wat er toen misgegaan is, maar ook n aar de toekomst te kijken en datgene te voorkomen wat zich nog niet eerder heeft afgespeeld. Vaak zien we een natuurlijke reactie waarbij de beoordeling door experts vervangen wordt door nieuwe regels en procedures. Nog meer regels, nog meer procedures die het toch al complexe handboek voor de operator er niet eenvoudiger op maken en de kans doen toenemen dat hij nalaat ze correct toe te passen. Deze studie laat hier trieste voorbeelden van zien.
Dit onderzoek richt zich op toestand overgangen, het dynamische gedeelte van systeemgedrag, waar veel studies zich vooral richten op de toestanden zelf, een meer statische benadering derhalve. Zoals hier te zien valt, is het tijdens een ongeval of ramp bijna onvermijdelijk dat het systeem zich op enig moment in een toestand van chaos lijkt te verkeren. Hoe het systeem uit die chaotische toestand weet te ontsnappen, hangt in belangrijke mate af van een ingebouwde veerkracht en flexibiliteit plus (heel belangrijk) de vaardigheden van de menselijke operator.

Vaak wordt de mens gezien als een last, een onzekere risico verhogende factor. Dit onderzoek toont aan dat de mens juist de ultieme veiligheidsfactor kan zijn, speciaal in totaal onvoorziene omstandigheden. Per slot van rekening is op dit moment alleen de menselijke geest in staat om snel te leren en nieuwe strategieën te bedenken, gebaseerd op beperkte beschikbare informatie. Een dergelijke mentale veerkracht vereist niet allen cognitieve maar ook emotionele training van de operators.
Dit onderzoek laat een aantal belangrijke observaties zien. Ondanks vele onderzoeken en studies gaan er nog steeds dingen fundamenteel mis. We lijken te stagneren in onze bestaande analyses. Dit blijkt uit de statische, lineaire wijze van benadering, gericht op een individuele actor. Het blijkt nodig te zijn om de benadering naar een meer dynamisch niveau te brengen, zoals valt af te leiden uit Collingridge, George, French en anderen.
Bestaande theoretische modellen lijken in deze tekort te schieten, in die zin dat zij niet in voldoende mate het gedrag van risicogevoelige system lijken te verklaren. Dat laatste valt of te leiden uit de casuïstiek en empirische waarnemingen bij grote ongevallen.
Wat ontbreekt is een gedegen begrip van het belang van de factor tijd en het gedrag ervan in een risicogevoelig systeem. Hoewel tijd doorgaans als lineair gezien wordt, is dat niet altijd het geval. Tijd kan versnellingen en vertragingen vertonen, wat direct of indirect van invloed is op het systeemgedrag.
Een ander niet altijd goed gepositioneerd onderscheid is die tussen proces en inhoud. Als die niet convergeren, kan dat resulteren in diverse dilemma's zoals Collingridge en George. Ook is het in dit kader belangrijk om een gedegen onderscheid te maken tussen een gebeurtenis en het systeem. Beide vereisen een specifieke manier van modelleren, ingegeven door het verschil in tijdlijn. Gebeurtenissen verlopen volgens een tamelijk lineaire tijdas, terwijl een systeem gekarakteriseerd wordt door toestandsveranderingen. Deze zijn discreet van karakter met niet-lineaire intervallen.
Ten einde een risicogevoelig systeem minder ontvankelijk te maken voor onverwacht catastrofaal falen, worden de volgende aanbevelingen gedaan die voortvloeien uit dit onderzoek.

1. Elk systeem moet al meteen in het begin van de ontwerpfase geanalyseerd worden ten aanzien van potentiele risicogevoeligheid, meer in het bijzonder aspecten zoals resilience time, acceptabele en niet-acceptabele faalscenario's, terugvalopties en dergelijke.
2. Het is belangrijk om risicogevoelige systemen zo te ontwerpen, dat ze ofwel robuust of redundant, betrouwbaar, veerkrachtig of een combinatie hiervan zijn.
3. Risicogevoelige systemen hebben stoplijnen nodig, die onafhankelijk zijn van het scenario dat van toepassing is. Die stoplijnen bepalen de veiligheidscitadel van waaruit een beheerst systeemherstel mogelijk is.
4. 'Resilience time' moet een integraal onderdeel worden van het ontwerp, de bouw en de gebruiksomgeving van risicogevoelige systemen.
5. Emotionele training is net zo belangrijk als cognitieve training om een hectische situatie te overleven: emotionele veerkracht.

Dit empirische, casuïstisch gedreven, onderzoek heeft het belang aangetoond van resilience engineering als een hulpmiddel om het gedrag van risicogevoelige systemen te beheersen. Resilience time is daarbij geïdentificeerd als een verborgen dynamische eigenschap. Het Citadelprincipe is een bruikbaar hulpmiddel gebleken om op een efficiënte en effectieve wijze om te gaan met onbekende risico's.
Overigens zijn alle casuïstieken gebaseerd op officiële onderzoeksrapporten, die geacht worden de toets der maatschappelijke acceptatie te hebben doorstaan. In veel gevallen zijn er naderhand wetenschappelijke publicaties verschenen, die deze rapporten aanvullen en daarmee in een wetenschappelijk zuiverder context plaatsen.

Qua wijze van valideren zijn er meerdere perspectieven mogelijk: het wetenschappelijke perspectief (is het waar?) versus de engineering en het ongeval onderzoek (is het geloofwaardig en toepasbaar?).
In dit proefschrift wordt er van uitgegaan dat de feiten zoals afgeleid uit de ongeval onderzoeksrapporten op zich juist zijn. Die worden dan ook op zich niet in twijfel getrokken. Wat hier gedaan wordt is deze feiten in een ander perspectief plaatsen, door het koppelen van de gebeurtenissen aan het systeem. Dat levert, zo is uit dit onderzoek gebleken, nieuwe inzichten op, die aspecten kunnen verklaren die tot dan onderbelicht waren.
Er is verder onderzoek nodig naar het gedrag van resilience time en de manier waarop die gemodelleerd kan worden. Voorts is het van belang om de transformatie van factor en gebeurtenis naar vector en systeem nader te bestuderen. Is het mogelijk om resilience (veerkracht) net zo te modelleren als betrouwbaarheid? Aan de andere kant is het ook van belang om resilience te vertalen van een organisatorisch hulpmiddel naar een meer praktisch hulpmiddel gericht op het fysieke en organisatorische ontwerp van het systeem.

Summary

Nowadays we have all sorts of legislation to safeguard safety at home and at work. Safety management systems are supposed to safeguard safety issues at system level. We have advanced computer models to test system designs when still on the drawing board. Safety as a whole is very much safety conscious. Yet despite all our efforts accidents still happen, unwanted or wanted. Apparently safety as such is not an issue in our modern western society, securing safety is the challenge, hence the title of this thesis.
Modern society is increasingly complex and vulnerable. On the other hand our knowledge of risks has increased over the years. Using modern digital risk analysis tools it is possible to design and build structures that would have been impossible only two or three decades ago. Risk management as such is nothing new. The various tools we use depend on the level of knowledge we have about the systems.
One thing is clear: accidents should not happen, yet it is difficult to avoid them as this thesis will show. They can be the consequence of unintentional misapprehensions through lack of knowledge and/or understanding of the factual functioning of the system (safety). Or they can be the consequence of intentional acts of destruction such as terrorism (security). A third often used notion is risk: the exposure of a danger or unwanted event. Sooner or later a system can be exposed to one or more threats. These distinction between these notions (safety, security and risk) must be clear. This thesis will use them in several analyses. Damage is unavoidable but should it be fatal?
What do we know about the effects when things can go wrong and how reliable is our knowledge about the likelihood of occurrence of such a condition/situation? In most cases the extend of our knowledge is well defined, both about what we know and what we don't know. It is the knowledge about what we don't know we don't know (the unknown risks, the unknown unexpected behaviour of a system following from its hidden properties) that poses a challenge to adequate risk management. How to prepare yourself for the risk you don't know?

The problem statement for this research is as follows:

It appears that present risk management policies fail to safeguard the role of safety and security at strategic and tactical level when dealing with major infrastructures and therefore might result in an increased risk level without policy decision makers and managers being aware of this.

Based upon this problem statement, the following research aim is defined:

To develop an approach, which is at systems level both efficient and effective when dealing with large effect low probability risks relating to transport systems.

Although risk management is well understood at strategic (macro) level, problems at tactical (meso) and operational (micro) level appear to be far less understood. This is caused by the lack of understanding the importance of the time factor in critical situations and the dilemmas that have to be tackled under time pressure. Indeed the impression exists that some dilemmas are inevitable and (almost) unsolvable. This thesis will show that it is possible to escape from such a no-win situation. This thesis also shows the hidden influence of time criticality in high risk systems.
This research is not based on a theoretical approach, followed by practical tests. Rather the reverse has happened: empirical studies have resulted in research aimed at hidden properties and discovering explaining variables. Most of the cases are from Dutch transport practice. Despite this apparent limitation the lessons learned from them through this research show a potential for a more general applicability.
Although resilience engineering as such is not new, the way it is being used in this thesis is quite novel, because it transforms resilience engineering from a somewhat static tool at strategic level with its centre of gravity in the design phase into a dynamic tool at operational level in the daily use situation. This new approach is the citadel principle. The most important shift in thinking is diverting from what could happen to the system to understanding what it is we don't want to happen to the system, never mind the cause. That way dealing with unknown unknowns to a certain extend becomes controllable.
'To engineer is human' wrote Petroski in 1992. It is only through failure that we learn the right lessons. The challenge is not only looking at the past and preventing reoccurrence of what has happened, but also looking forward and preventing occurrence of what hasn't happen yet. A natural reaction often seen is to replace expert judgement by new rules and procedures, more rules and procedures, adding to the already complex manual of the operator and increasing the probability that he fails to observe them. This thesis shows unfortunate examples of this.
This research focuses on the state transitions, the dynamic part of system behaviour, where many studies tend to focus on the states of a system, a more static approach. As this study shows during an accident or catastrophe it is almost inevitable that at some stage the system is in chaos. How the system escapes from the chaotic state is to a large extend depending on a combination of build in resilience and flexibility plus (very important) the skills of the human operator.
Often the human factor is seen as a liability, whereas this research shows that it can be the ultimate safeguard, especially in totally unforeseen circumstances. After all at present it is only the human mind that is capable of learning quickly and develop new strategies, based on limited available information. Such a mental resilience requires both cognitive and emotional training of operators.
This research shows a number of important observations. Despite many studies and models, we are not getting to grips with accidents. We are stagnating in our policies. Tools used are static, linear, based on a single actor approach et cetera. It is necessary to move to a different, more dynamic level, as suggested by George, Collingridge, French and others. These observations can be deduced from analysing existing case studies and empirical evidence from accident investigation as done by the author himself.

What is missing is a good understanding of the importance of the time factor and the behaviour of time in a risk sensitive system. Although time is perceived as linear, in some cases time can accelerate and decelerate. Direct or indirect these accelerations and decelerations influence the way a risk sensitive system behaves.
Another aspect not always well positioned is the distinction between process and contents. If at some point they diverge instead of converging, various dilemmas such as George and Collingridge can be the outcome of it. Another distinction is the one between event and system. They require specific modelling, because they have different time lines. Events follow a somewhat linear time line, whereas systems are characterised by state transitions, discrete events with non-linear intervals.
In order to make a risk sensitive system less susceptible to unexpected catastrophic failure, the following points are recommended.

1. Each system already at the design stage should be analysed regarding its risk sensitivity, more specifically aspects such as resilience time, acceptable and non-acceptable failure scenarios, fall-back options et cetera.
2. It is important to design risk sensitive system in such a way that they are either robust, redundant, reliable, resilient or a combination of these properties.
3. Risk sensitive systems need stop lines regardless what scenario applies, defining the safety and security citadel, from which a controlled recovery of the system is possible.
4. Resilience time should become an integral part of the design, construct and practice environment of risk sensitive systems.
5. Emotional training is just as important as cognitive training to survive a hectic situation: emotional resilience.

This empiric research driven by cases from the transport world has shown the importance of resilience engineering as a tool of controlling the behaviour of risk sensitive systems. Resilience time has been identified as a hidden dynamic property. The Citadel principle has been shown to be a useful tool when dealing in an efficient and effective way with unknown risks.
Every case study used in this thesis is based on official accident investigation reports, which are deemed valid and accepted by society. In many cases these reports have been followed by scientific publications aimed at elaborating on the initial findings and improving the scientific context. There are various perspectives to validate these investigation reports: a scientific perspective (is it true?) versus an engineering and accident investigation perspective (is it credible and useful?).
This thesis does not question the facts and findings as they can be deducted from the investigation reports. Instead these findings are put in a different perspective by connecting events to the system involved. That results as can be learned from this study in new insights capable of explaining aspects hitherto hardly noticed.
Further research is required into the behaviour of resilience time and the way it can be translated into mathematical models. Furthermore it is important to study the transition from factor and event to vector and system. Is it possible to create mathematical models regarding resilience just as has been done regarding reliability? On the other hand it is also important to translate resilience as an organisational tool into a more practical engineering tool aimed at both the physical and organisational design of the system.

References

Ale, B, 2005. Tolerable or acceptable: a comparison of risk regulation in the United Kingdom and in the Netherlands. Risk Analysis, vol. 25, no. 2

Ale, B, 2006. Een kwestie van cultuur. Externe veiligheid 1

Algemeen Dagblad, 2006. Maeslantkering hapert teveel. 11-02-2006

Algemeen Dagblad, 2006. Dijkverzwaring als rugdekking. 21-02-2006

Alphen, W.J.T. van et al, 2008. Leren van ongevallen. SDU

Apostolakis, G.E. and D. Lemon, 2005. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis vol. 25, no. 2

Australian Transport Safety Bureau, 2013. In-flight uncontained engine failure Airbus A380-842, VH-OQA. Final report AO-2010-089, June 2013

Atta, D. van, 1998. Terrorism and the media. Harvard International Review, vol. 20, nr. 4

AVV, 2004. Consequentieonderzoek Externe Veiligheid. Report

AVV, 2006. Veiligheidseffecten van infrastructuurprojecten. Aanvulling op de Leidraad OEI

Beck, U, 1992. Risk society. London, Sage

Beukenkamp, W.R. and J.A. Stoop, 2002. Al doende leert men: HSL-Zuid Integrale Veiligheid. TU-Delft

Beukenkamp, W.R. and M. van Raamsdonk, 2003. Menselijk gedrag bij calamiteiten. Brand en brandweer, September nr. 8, 2003

Beukenkamp, W.R., 2004. Infra at point blank. AVV, Conference paper Volpe Conference on transport security

Beukenkamp, W.R., M.H. Flinterman and A. Sarnari, 2005. Throwing objects from a bridge or overpass – experiences in the Netherlands and Italy

Beukenkamp, W.R. and J.A. Stoop, 2005. Security and critical infrastructures: the citadel principle. ESReDA #29 conference paper

Beukenkamp, W.R. and S. IJsselstijn, 2006. Reliability of safety-critical systems: unravelling criticality. ESReDA #30 conference paper

Beukenkamp, W.R., S. IJsselstijn, M. Kuiken and J.A. Stoop, 2006. Scenario's: a multi-actor decision-making support tool. PSAM-8 conference paper

Beukenkamp, W.R. and R. Methorst, 2006. Ageing in transportation systems. ESReDA #31 conference paper

Bezuyen, M.J., M.J. van Duin and U. Rosenthal, 1995. Watersnood 1995. Bestuurskunde 1995, pp. 353-360

Boer, R. J. De, 2015. Seneca's error: An affective model of cognitive resistance. PhD thesis, TU Delft, 2014

Brand, P. van den, 2006. A2 afgedekt bij stadscentrum Leidsche Rijn. Alert 4

Bruin, J.A. de, E.F. ten Heuvelhof and R.J. in 't Veld, 1998. Proces management. Academic Services

Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, 2012. Final report on the accident on 1st of June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris

Centraal Bureau voor de Statistiek (Statistics Netherlands CBS). Website: http://statline.cbs.nl/StatWeb/

Clarke, R.A, 2004. Against all enemies. Free Press

Coleman, L, 2006. Frequency of Man-made disasters in the 20th century. Journal of Contingencies and crisis management vol. 14 no. 1

Collingridge, D, 1980. The Social Control of Technology. New York: St. Martin's Press

Commissie Bijlmerramp, 1999. Een beladen vlucht

Commissie preventie rampen (CPR), 1997 (1987). Methods for determining and processing probabilities (Red Book). CPR 12E, SDU

Commissie preventie rampen (CPR), 1997 (1985). Methods for the calculation of physical effects (Yellow Book). CPR 14E, SDU

Commissie preventie rampen (CPR), 1999 (1988). Guidelines for quantitative risk assessment (Purple Book). CPR 18E, SDU

Committee of science and technology in countering terrorism, 2002. Making the nation safer: the role of science and technology in countering terrorism. National Academic Press

Connekt, 2001. Connekt congres 'Ruimte voor Inhoud'. Connekt Kenniscentrum voor Verkeer en Vervoer, Amsterdam

Coombs, L.F.E., 1978. The Harrow railway disaster. David & Charles, 1978

Crelinsten, R.D., 1997. Television and Terrorism. Implications for Crisis Management and Policy-Making. Terrorism and Political Violence, vol.9, nr. 4

Dekker, S, E. Hollnagel, D. Woods and R. Cook, 2008. Resilience engineering: new directions for measuring and maintaining safety in complex systems. Final report. Lund University School of Aviation, November, 2008

Duin, M.J. van, 1992. Van rampen leren. Thesis Leiden, 1992

Ee, M van and R. van Ee, 1997. Ongevallen op Nederlands Spoor. De Alk, 1997

ESReDA working group report, 2005. Shaping public safety investigations of accidents in Europe. DNV

Falkenrath, R.A., Newman, R.D. and B. Thayer, 2001. America's Achilles' Heel. MIT Press

French, S, 2013. Cynefin, statistics and decision analysis. Journal of the Operational Research Society (2013) 64, 547-561

George, A, 1980. Presidential Decisions Making in Foreign Policy. Westview Press

Gorter, D.P. and C.D. Jaeger, 2014. Project Samurai Pilot. Thesis, TU Delft and University of Leiden

Government of the Republic of Estonia, 1997. Final report on the MV Estonia disaster of 28 September 1994

Hadden et al, 1964. Accident research: methods and approaches. Harper & Row

Hall, S, 1999. Hidden dangers; railway safety in the privatisation era. Ian Allan

Hall, S, 2003. Beyond hidden dangers; Ian Allan

Hendrickx, L.C.W.P., 1991. How versus how often. Van Denderen

Heymann, Ph.B., 1998. Terrorism and America: a common sense strategy for a democratic society. MIT Press

Hollnagel, E, 2012. FRAM; the functional resonance analysis method. Ashgate Publishing Ltd

Hollnagel, E, J. Pariès, D.Wood and J. Wreathall, 2011. Resilience engineering in practice; a guidebook. Ashgate Publishing Ltd

Hollnagel, E, 2008. The changing nature of risks. Ergonomics Australia Journal 22, 1-2 (2008) 33-46

Hood, C., H. Rothstein and R. Baldwin, 2004. The government of risk. Oxford University Press

Hupkes, dr. G., 1977. Gasgeven of afremmen – Toekomstscenario's voor ons vervoerssysteem. Kluwer, Deventer/Antwerpen, 1977

IJsselstijn, S., W.R. Beukenkamp, M. Kuiken, J.A. Stoop, (2006). Scenarios: a multi-actor decision-making support tool. PSAM8 conference paper, New Orleans

Inspectie Leefomgeving en Transport (Dutch Railway Inspectorate ILT), 2014. Rapport RV14-0103 Infraproblemen rond Den Haag en Rotterdam

Inspectie Leefomgeving en Transport (Dutch Railway Inspectorate ILT), 2013. Rapport RV12-0346 Treinbotsingen te Leiden Centraal

Inspectie Leefomgeving en Transport (Dutch Railway Inspectorate ILT), 2013. Rapport RV12-0369 Treinbotsing te Amsterdam Westerpark

Inspectie Leefomgeving en Transport (Dutch Railway Inspectorate ILT), 2013. Veiligheidsbalans 2012

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2011. Veiligheidsbalans 2011

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2010. Veiligheidsbalans 2010

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2009. Rapport RV09-0179 inzake de ontsporing van een goederentrein bij Harmelen Aansluiting, 2009

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2009. Rapport RV-08U0938 inzake de ontsporing van een Amsterdamse metro bij Weesperplein

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2009. Rapport RV08-U0831 inzake de botsing tussen een tram en een bus in Amstelveen

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2008. Rapport RV08-U0288 inzake de ontsporing van een metrotrein bij Amsterdam Centraal Station

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2008. Veiligheidsbalans 2008

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2007. Veiligheidsbalans 2007

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2007. Rapport RV07-U0238 Bijna botsing te Harmelen aansluiting

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2005. Rapport RV-05U0026 inzake de aanrijding tussen een reizigerstrein en een vrachtwagen op een overweg in de gemeente Wijhe

Inspectie Verkeer en Waterstaat (Dutch Railway Inspectorate IVW), 2004. Rapport RV04-U0008 inzake de treinbotsing op Amsterdam-Centraal

Jastrzebski, R, 2006. Rijk en gemeenten beraden zich op knelpunten Betuweroute en HSL. Alert 4

Jastrzebski, R, 2006. Veiligheid zwaar criterium bij stadsvernieuwing Dordrecht. Alert 4

Jones, F, 1986. Air crash. W.H. Allen & Co, 1986

Jongerius, R.T., 1993. Spoorwegongevallen in Nederland. Schuyt & Co

Jorissen, R.E. and P.J.M. Stallen, 1998. Quantified societal risk and policy making. Kluwer, 1998

Laquer, W, 1999. The new Terrorism. Fanaticism and the Arms of Mass Destruction. Oxford University Press

Lawton, R and N. Ward, 2005. A systems analysis of the Ladbroke Grove rail crash. Accident Analysis and Prevention no. 37

Leeuwendaal, 2001. De bochtige weg naar beheerst risico. Naar een evenwichtige besluitvorming bij grote infrastructurele projecten. Leeuwendaal Advies

Locaalspoor- en Tramwegwet, 1900

Methorst, R., 2003. Vulnerable road users – Report on the knowledge base for an effective policy to promote the safe mobility of vulnerable road users. AVV Transport Research Centre, Rotterdam

Methorst, R., 2005. Voetenwerk. AVV Transport Research Centre, Rotterdam

Methorst, R., 2006. Pedestrians' Quality Needs – A Conceptual Model. COST 358, AVV Transport Research Centre, Rotterdam

Meyer, R.J., 2010. Safety in Ignorance? Dilemmas of Disaster Prep. Wharton Magazine

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2005. Rapport analyse bescherming vitale infrastructuur. MinBZK

Ministerie van Verkeer en waterstaat, 2002. Verder met veiligheid: een gemeenschappelijke visie op veiligheid. MinV&W

Ministerie van Verkeer en waterstaat, 2005. Nota Mobiliteit

Ministerie van Verkeer en waterstaat, 2006. Nota Vervoer gevaarlijke stoffen

MIT, October 22, 2015. Why Self-Driving Cars Must Be Programmed to Kill. Emerging technology from the airXiv

Mohrmann, J.F.W., 2013. Investigating flight crew recovery capabilities from system failures in highly automated fourth generation aircraft. Thesis, TU-Delft

Mooij, R. de and P. Tang, 2003. Four futures of Europe. Centraal Planbureau, Den Haag, 2003

Morozov, E., 2013. This explains everything. Harper Perennial

Murray, Andrew, 2002. Off the rails: the crisis on Britain's railways. Verso

Nacos, B.L., 2000. Accomplice or Witness? The media's role in Terrorism. Current History, vol. 99, nr. 178

National commission on terrorist attacks upon the United States, 2003. The 9/11 commission report. Norton & Company Ltd.

OECD, 2001. Ageing and transport – mobility needs and safety issues. OECD, Paris, 2001

Parkes, Dr. O, 1973 (1957). British Battleships: A history of Design, Construction and Armament. Seeley Service & Co, London

Perrow, Ch., 1999 (1984). Normal accidents: living with high risk technologies. Princeton University Press

Petroski, H, 1992. To engineer is human: the role of failure in successful design. Vintage books

Poortvliet, A. van, 1999. Risks, disasters and management. Thesis, Eburon

Preuß, E, 1998. Kursbuch des Schreckens. Transpress

Projectteam Tunnelveiligheid (2003). Beleidsnota Tunnelveiligheid. Deel A: Proceseisen

Raad voor de Transport Veiligheid, 2005. Door rood op Amsterdam CS. RvTV

Rail Accident Investigation Branche report 27/2006. Broken rails at Urchfront and Kennington following passage of a freight train January 5, 2006

Rasmussen, J, 1983. Skills, Rules, And Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on systems, Man, and Cybernetics, Vol. SMC-13, No. 3, May/June 1983, p. 257-266.

RIVM, 2003. Nuchter omgaan met risico's. RIVM 251701047

Rolt, L.T.C., 1998. Red for danger. Sutton Publishing

Rosental, U, 2000. Veiligheidsniveaus: over menselijke fouten, het systeem en nieuwe zondebokken. NVVK Jan de Kroes lezing

Rosmuller, N, 2001. Safety analysis of transport corridors. Thesis, Trail

Rooij, R. and M. Tacken, 2001. Beperkte mobiliteitsbehoefte? TU Delft - Faculteit Bouwkunde, Delft 2001.
Sapolski, H, 1990. The politics of risks. Deadalus, 119/4: 83-96

Semmens, P, 1994. Railway Disasters of the world. Patrick Stephens Ltd.

Slovic, P., 1987. Perception of risk. Science, vol. 236, 17 April 1987

Slovic, P, 1999. Trust, emotion, sex, politics and science: surveying the risk-assessment battlefield. Risk Analysis, vol. 19, no. 4

Slovic, P, M. Finucane, E. Peters and D. MacGregor, 2004. Risk as analysis and risk as feeling: some thoughts about affect, reason, risk and rationality. Risk Analysis, vol. 24, no. 2

Socialdata, 2005. Monitoring verplaatsingsgedrag mensen met een beperkte mobiliteit 2004 – Eindrapportage. Heerlen

Spoorwegwet, 2005

Spoorwegwet, 1875

Stirling, A (1999). On science and precaution in the management of technological risk. European Commission Joint Research Centre, Institute of Prospective Technological Studies, Sevilla

Stirling, A and S. Mayer, 2000. Precautionary approaches to the appraisal of risk. International Journal of occupation, Environment and Health no. 6

Stoop, J.A.A.M. , 1990. Safety and the design process. Thesis, TU-Delft

Stoop, J.A.A.M., 1999. Niet anders dan door schokken. NVVK lecture

Stoop, J.A.A.M., 2001. Veiligheid, van operationele kostenpost naar strategische beleidsissue. In: ‘Zeven jaar transportbeleid en logistieke organisatie. Lessen voor de toekomst.’ TU-Delft

Stoop, J.A.A.M. and W.R. Beukenkamp, 2002. Monitoring safety in design and construct: the HSL-South case study. ITA World Tunnelling Congres 2002, Conference paper

Stoop, J.A.A.M., M. Kuiken and T. Postma, 2003. Liable or reliable: applying scenario concepts in infrastructure design. Proceedings of the 10th TIEMS conference

Stoop, J.A.A.M., J.H. Baggen, J.L. de Kroes, J.M. Vleugel and J.L.M. Vrancken, 2007. HSL-beveiligingssysteem ERTMS. Een onafhankelijk onderzoek naar nut en noodzaak van de aanpassing van het HSL-beveiligingssysteem ERTMS in opdracht van het Onderzoeks- en Verificatiebureau van de Tweede Kamer der Staten-Generaal. TU-Delft

Stoop, J.A.A.M. and S. Dekker, 2010. Accident modelling: no more cheese please. Proceedings of the 10th International PSAM Conference, Seattle, Washington, USA, 2010

Suddle, S, 2004. Physical safety in the multiple use of space. Thesis, TU-Delft

Tay, R., 2002. The Prisoner's Dilemma and Vehicle Safety. Journal of Transport Economics and Policy, vol. 36, part 3.

Tijdelijke Commissie Infrastructurele projecten (Commissie Duyvestein), 2004. Onderzoek naar infrastructuurprojecten, appendix 10. SDU

Toft, B. and Reynolds, S., 1994. Learning from disasters. Butterworth-Heineman Ltd.

Tweede Kamer, 1989. Omgaan met risico's (Premises for risk management). TK vergaderjaar 1888-1989, 21137, no. 5

Tweede Kamercommissie voor Verkeer en Waterstaat, 2006. Op de rails. TK 29 984, nr. 22

Vaugh, A., 2000. Tracks to disaster. Ian Allan Publishing

Vollenhove, P. van, 2006. RisicoVol. Inaugural speech, Enschede

Wegenverkeerswet, 1990

Wolmar, C., 2002. Down the tube. Aurum Press Ltd.

Wolmar, C., 2005. On the wrong line. Aurum Press Ltd.

About the author

Willem R. (Wim) Beukenkamp (born in Rotterdam in 1956) studied mining engineering at Delft University (1974-1976) and civil engineering at Haarlem Polytechnic (1976-1980), where he obtained a Bachelor in structural engineering. From 1985-1987 he studied Software Engineering, getting his Bachelor in ICT. In 1997, Wim returned to Delft, to study systems engineering and policy analysis. He graduated as a Master in transport safety in 2001 on the subject of a methodical approach to the safety and security issues relating to the protection of Dutch embassies against terrorism.

From 2004 until present, Wim has been working on a PhD project, looking at the role of safety in the decision-making processes regarding transportation systems. This project was done at Delft University of Technology in cooperation with the Ministry of Transport and Watermanagement). Papers have been presented at several national and international conferences, including conferences organized by the European Safety, Reliability & Data Association (ESReDA), where in 2005 he presented and successfully defended the citadel approach, as well as a presentation in 2006 about safety critical systems and another in 2006 about the problem of ageing in transportation systems. He was also keynote speaker on the subject of the 'Citadel Approach' at a joint symposium organized by the Universities of Twente, Eindhoven and Delft in 2006. In 2009 he presented a paper for ESReDA about lessons learned from accident investigation, reflecting his new job at the railway inspectorate.
After graduating from Haarlem Polytechnic, Wim joint the Royal Dutch Steelworks (Koninklijke Nederlandse Hoogovens en Staalfabrieken, now Tatasteel IJmuiden) as a junior engineer. In 1985 he became project engineer in the then newly formed Industrial Computer Department of the same company. In 1991 he moved to the Ministry of Foreign Affairs, where he became security and safety coordinator and later senior safety engineer.
After graduating from Delft University in 2001 he took on a job as senior researcher and consultant in the then AVV Transport Research Centre of the Ministry of Transport and Water management (present Centre for Transport and Navigation). His research at AVV included risk assessment of vital infrastructures, external safety and the transportation of hazardous goods, safety of light rail systems (where he played a vital role in establishing a national standard for the design of light rail systems in urban environments), railway safety and incident management on motorways.

In December 2007, Wim joined the Dutch Railway Inspectorate (part of ILT) as senior inspector, specializing in the maintenance of railway infrastructure and the design, operation and maintenance of tram and metro systems. He was chief accident investigator in a number of serious rail accidents. The majority of the ILT reports referred to in this thesis were written by him. In 2011 he became team coordinator rolling stock.
In private life Wim is active as national instructor and examiner in the field of First Aid. In the latter capacity he published a book about how people approach and behave in accidents and the way they act as First Aiders, which is used in the training of First Aid instructors nationwide. Wim is also involved in safeguarding the national heritage, in particular rail transport heritage. Wim is Board member of several first aid and heritage societies. In 2006 Queen Beatrix of the Netherlands honoured Wim by appointing him as Member of the Order of Orange-Nassau for his outstanding work in the field of First Aid and the protection of the (inter)national heritage.

Recent publications by Wim Beukenkamp:

Title	**Co-author**	**Year**
ILT report RV12-0346 Treinbotsingen te Leiden Centraal		2013
Vakman is meesterschap; OR ILT	OR commissie O&O	2013
ILT report RV12-0386 Bijna-botsing van een reizigerstrein met een goederentrein te Utrecht Centraal		2013
ILT report RV12-0337 Botsing van twee goederentreinen op de Maasvlakte		2013
ILT report RV11-0080 Bijna-aanrijding tussen een trein en een taxibusje te Bilthoven		2012
ILT report RV10-0717 Bijna-botsing te Kapelle-Biezelinge		2012
ILT report RV10-0561 Spoorstaafbreuk Uithuizen c.a.		2011
Article: Een oorverdovende stilte (in: HulpVaardig, november 2009)		2009
Article: De werking van het immuunsysteem (in HulpVaardig 7-3, augustus 2009)		2009
Conference paper: A diabolic dilemma: towards fully automated train control or a human centred design? (IFAC 2009)	John Stoop, Jos Vrancken, Jaap vleugel	2009
ILT report: RV08-0831 Botsing tram met bus		2009
Conference paper: Lessons learned from accident investigation: derailment of an Amsterdam metro (ESReDA)		2009
Article: De vergeten objecten (in: Op Oude Rails, februari 2009)		2009
ILT report: Veiligheid wissels hoofdspoorweginfrastructuur: onderzoek LOD 3		2009
Article: Shock: belangrijk onderwerp in de EHBO, maar wat is het eigenlijk? (in: HulpVaardig 7-1, februari 2009)		2009
Article: BHV: let op de RI&E (in: HulpVaardig 6-3, september 2008)		2008
ILT report: Veiligheid wissels hoofdspoorweginfrastructuur		2008
Article: Het gevaar van inerte gassen (in HulpVaardig 6-1, januari 2008)		2008
Article: Onweer en Eerste Hulp (in HulpVaardig 5-3, september 2007)		2007
Article: A phenix arises (in: The Journal (UK), oktober 2007)		2007
Article: De waarde van replica's (in Op oude rails, juni 2006)		2006

Conference paper: Ageing and transportation systems (ESReDA)	Rob Methorst	2006
Conference paper: Safety critical infrastructures (ESReDA)	John Stoop	2006
Book: Bij nader inzien; het belang van waarnemen in de Eerste Hulp		2006
Conference paper: Scenario's: a multi-actor decision-making support tool (PSAM-8)	Sandra IJsselstijn, Maria Kuiken, John Stoop	2006
Conference paper: Security and critical infrastructures: the citadel principle (ESReDA)		2005
AVV report: Veiligheid tram en wegkruisingen		2005
AVV report: Audit airside Schiphol Airport		2005
AVV report: RWS Vitaal		2005
Conference paper: Infra at point blank (Volpe, USA)		2004
AVV report: Externe Veiligheid en Spoedwetprojecten		2004
Article: Menselijk gedrag bij calamiteiten (in Brand en Brandweer, 2003)	Monique van Raamsdonk	2003
Report: Al doende leert men: HSL-Zuid en integrale veiligheid	John Stoop	2002
Report: Infra op scherp: security infrastructuren	Henk Roodbol, José Hernandez	2001
Master thesis: Algiers: ambassade onder vuur		2001
Article: Kwaliteitsborging in het EHBO-onderwijs (in Reddingwezen, 2001)		2001

TRAIL Thesis Series

The following list contains the most recent dissertations in the TRAIL Thesis Series. For a complete overview of more than 150 titles see the TRAIL website: www.rsTRAIL.nl.

The TRAIL Thesis Series is a series of the Netherlands TRAIL Research School on transport, infrastructure and logistics.

Beukenkamp, *Securing Safety: Resilience time as a hidden critical factor,* T2016/18, October 2016, TRAIL Thesis Series, the Netherlands

Mingardo, G., *Articles on Parking Policy,* T2016/17, October 2016, TRAIL Thesis Series, the Netherlands

Duives, D.C., *Analysis and Modelling of Pedestrian Movement Dynamics at Large-scale Events*, T2016/16, October 2016, TRAIL Thesis Series, the Netherlands

Wan Ahmad, W.N.K., *Contextual Factors of Sustainable Supply Chain Management Practices in the Oil and Gas Industry,* T2016/15, September 2016, TRAIL Thesis Series, the Netherlands

Liu, X., *Prediction of Belt Conveyor Idler Performance,* T2016/14, September 2016, TRAIL Thesis Series, the Netherlands

Gaast, J.P. van der, *Stochastic Models for Order Picking Systems,* T2016/13, September 2016, TRAIL Thesis Series, the Netherlands

Wagenaar, J.C., *Practice Oriented Algorithmic Disruption Management in Passenger Railways,* T2016/12, September 2016, TRAIL Thesis Series, the Netherlands

Psarra, I., *A Bounded Rationality Model of Short and Long-Term Dynamics of Activity-Travel Behavior,* T2016/11, June 2016, TRAIL Thesis Series, the Netherlands

Ma, Y., *The Use of Advanced Transportation Monitoring Data for Official Statistics,* T2016/10, June 2016, TRAIL Thesis Series, the Netherlands

Li, L., *Coordinated Model Predictive Control of Synchromodal Freight Transport Systems*, T2016/9, June 2016, TRAIL Thesis Series, the Netherlands

Vonk Noordegraaf, D.M., *Road Pricing Policy Implementation,* T2016/8, June 2016, TRAIL Thesis Series, the Netherlands

Liu, S., *Modeling, Robust and Distributed Model Predictive Control for Freeway Networks,* T2016/7, May 2016, TRAIL Thesis Series, the Netherlands

Calvert, S.C., *Stochastic Macroscopic Analysis and Modelling for Traffic Management,* T2016/6, May 2016, TRAIL Thesis Series, the Netherlands

Sparing, D., *Reliable Timetable Design for Railways and Connecting Public Transport Services,* T2016/5, May 2016, TRAIL Thesis Series, the Netherlands

Rasouli, S, *Uncertainty in Modeling Activity-Travel Demand in Complex Urban Systems*, T2016/4, March 2016, TRAIL Thesis Series, the Netherlands

Vries, J. de, *Behavioral Operations in Logistics,* T2016/3, February 2016, TRAIL Thesis Series, the Netherlands

Goñi-Ros, B., *Traffic Flow at Sags: Theory, Modeling and Control*, T2016/2, March 2016, TRAIL Thesis Series, the Netherlands

Khademi, E., *Effects of Pricing Strategies on Dynamic Repertoires of Activity-Travel Behaviour,* T2016/1, February 2016, TRAIL Thesis Series, the Netherlands

Cong, Z., *Efficient Optimization Methods for Freeway Management and Control,* T2015/17, November 2015, TRAIL Thesis Series, the Netherlands

Kersbergen, B., *Modeling and Control of Switching Max-Plus-Linear Systems: Rescheduling of railway traffic and changing gaits in legged locomotion,* T2015/16, October 2015, TRAIL Thesis Series, the Netherlands

Brands, T., *Multi-Objective Optimisation of Multimodal Passenger Transportation Networks,* T2015/15, October 2015, TRAIL Thesis Series, the Netherlands

Ardiç, Ö., *Road Pricing Policy Process: The interplay between policy actors, the media and public,* T2015/14, September 2015, TRAIL Thesis Series, the Netherlands

Xin, J., *Control and Coordination for Automated Container Terminals,* T2015/13, September 2015, TRAIL Thesis Series, the Netherlands

Anand, N., *An Agent Based Modelling Approach for Multi-Stakeholder Analysis of City Logistics Solutions,* T2015/12, September 2015, TRAIL Thesis Series, the Netherlands

Hurk, E. van der, *Passengers, Information, and Disruptions,* T2015/11, June 2015, TRAIL Thesis Series, the Netherlands

Davydenko, I., *Logistics Chains in Freight Transport Modelling,* T2015/10, May 2015, TRAIL Thesis Series, the Netherlands

Schakel, W., *Development, Simulation and Evaluation of In-car Advice on Headway, Speed and Lane,* T2015/9, May 2015, TRAIL Thesis Series, the Netherlands

Dorsser, J.C.M. van, *Very Long Term Development of the Dutch Inland Waterway Transport System: Policy analysis, transport projections, shipping scenarios, and a new perspective on economic growth and future discounting,* T2015/8, May 2015, TRAIL Thesis Series, the Netherlands

Hajiahmadi, M., *Optimal and Robust Switching Control Strategies: Theory, and applications in traffic management,* T2015/7, April 2015, TRAIL Thesis Series, the Netherlands