Safety Science 50 (2012) 1422–1430

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Are safety investigations pro-active?

John Stoop [a,b,*], Sidney Dekker [b]

[a] Delft University of Technology, Faculty Aerospace Engineering, Delft, The Netherlands
[b] Lund University, School of Aviation, Ljungbyhed, Sweden

ARTICLE INFO

Article history:
Available online 22 April 2011

Keywords:
Accident investigation
Human factor
Methodology
Safety management system

ABSTRACT

This paper elaborates on the debate whether safety investigations are obsolete and should be replaced by more modern safety assessment approaches. Despite their past performance, in particular in aviation, accident investigations are criticized for their reactive nature and the lack of learning potential they provide. Although safety management systems are considered a modern method with a more prospective potential, they too are hard to judge by their quantitative performance. Instead of measuring both concepts along the lines of their output, this contribution explores the origin, context and notions behind both approaches. Both approaches prove to be adaptive to new developments and have the ability to shift their focus towards learning and cognition. In assessing their potential, accident investigations prove to cover a specific domain of application in the risk domain of low probability and major consequences, fulfilling a mission as public safety assessor. In order to make optimal use of their analytic and diagnostic potential, investigations should mobilize more complex and sophisticated scientific theories and notions, in particular of a non-linear nature. Consequently, they are neither reactive, nor proactive, but provide a specific approach to safety issues.

1. Introduction

Over the past two decades, the concept of 'investigation' has seen a broadening of its applications beyond the scope of crime scenes and transportation accident investigations. New organizational models and legal institutions have been created to further disseminate the concept of independent investigations worldwide, while new missions have been added to existing investigation agencies. Simultaneously, the concept of single event investigation is criticized for its lack of statistical relevance and low cost-effectiveness. Moreover, safety boards should not provide a learning potential due to their reactive nature or lack of an adequate learning methodology (Ale, 2003; De Bruijn, 2007). Even in aviation, safety investigations are criticized, despite their long lasting performance and proven value. Investigations should have become obsolete and should be replaced by more 'modern' concepts.

In contrast, 'modern' concepts, such as safety management systems, audits and quality assurance claim to be proactive. The dichotomy created by such a 'pro-active versus reactive' contradiction, cannot be valued because there are no criteria for how to measure the success of an investigation apart from the follow-up rate of its recommendations. Moreover, safety management systems too do not have a proven track record based on criteria which facilitate a comparison with other safety enhancement approaches (Hale, 2006, Swuste, 2009, Johnson, 2007).

In order to facilitate a comparison between both safety enhancement approaches, characteristics of both these approaches should be established and the context should be assessed in which these instruments could develop.

1.1. How did safety investigations emerge?

Safety investigations have a history of decades in aviation. In analyzing the historical development of safety investigations in aviation, three phases can be identified:

First, a technological phase in which the notion of technical failure was dominant. After the Second World War, as a flywheel for progress in aviation, the level of technical harmonization was selected focusing on navigation, communication and reliability (Freer, 1986, 1994). Many resources had to be invested in improving the technical reliability of the aircraft, because new technologies were in their infancy, causing teething troubles in various areas. New technologies involved the introduction of pressurized cabins, jet engine technology, radar and all-metal airframes. In order to keep public trust in the aviation industry, a common and public process of timely learning without allocating blame was deemed necessary. This system has been successful for 60 years, solving many knowledge deficiencies in aviation. This development was supported by a first series of accident modeling, starting as early as 1928. The US Army model derived from

* Corresponding author at: Delft University of Technology, The Netherlands. Tel.: +31 183637484; fax: +31 183630216.
E-mail address: stoop@kindunos.nl (J. Stoop).

0925-7535/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2011.03.004

Thorndyke in 1951 can be considered the first epidemiological/stochastic model, reinforced by Haddon, Suchman and Klein's classic book on accident causation in transport in 1964.

Some examples of aviation show case investigations after the Second World War are:

- the De Havilland Comet initiated research into metal fatigue and crack propagation
- the Tenerife disaster initiating human failure research and crew resource management
- de crashes at Mt Erebus and Tenerife lead to victim identification
- several accidents in the USA lead to family assistance and trauma care for survivors
- the Boeing 747 crash in the Bijlmermeer caused the development of an external safety policy and integral airport safety management system.

A second phase in accident investigation started at the beginning of the nineties when independence from state interference was deemed necessary. This development focused also on multimodal safety boards in order to learn from each other. The initiative for this development is taken in the USA, where in 1967 the National Transportation Safety Board becomes the first independent multi-modal investigation agency in the world (Benner 2009). Based on a visionary approach, the concept of multi-modal and systemic learning was developed, supported by arguments of economy of scale, critical mass in investigative resources and organizational efficiency. These more pragmatic arguments have played a role in particular in smaller countries like the Netherlands. In addition to technological issues, operational issues emerged in investigation practices, dealing with human error and organizational failure (ETSC, 2001).

A third phase in accident investigation has emerged over the past decade due to a breakthrough of independent investigations in the public eye which occurred after a series of major events outside the transportation sector, such as with disco fire in Göteborg in Sweden, the explosion of a firework storage in Enschede and disco fire in Volendam in the Netherlands (Kahan, 1998; Stoop, 2004, 2009).

Transportation Safety Boards now face new missions, dealing with public trust, serving as a public safety assessor, support to victims and relatives in taking care of family assistance and focusing on rescue and emergency services in the aftermath of major accidents (Roed-Larsen et al., 2005). Consequently, governance and policy making issues emerged on the agenda of investigation agencies by stating: Independent Accident Investigation; a citizen's Right and Society's Duty (Van Vollenhoven, 2006). This phase characterizes the transition from accident investigation into safety investigation: a shift from event analysis towards systems analysis.

1.2. How did safety management systems emerge?

The first attempts in industrial society to explore human behavior go back to the 19th century. The can be attributed to La Mettrie. With his 'L'Homme machine' he introduced the metaphor of man as an unpredictable machine. According to the mechanistic concepts of his time, the human body was described as complex clockwork which could perform certain tasks based on predescribed movements. Later medical and behavioral scientific research, focused on how this 'machine' behaved under physical and mental loads.

1.2.1. Accident modeling, a first generation

The first generation of accident causation models as derived by Heinrich, referred to accident analysis by metaphors, such as the Iceberg Principle and Domino Theory. Bird and Loftus applied a linear causality, while Kjellen introduced the deviation concept. The MORT approach explicitly put the responsibility for risk control at the corporate level. Multi-causality was introduced by Reason, defining accident as an interaction between latent and active failures, and in order to avoid such interaction, a pro-active involvement of top management. Based on attribution theory, Hale and Glendon were concerned about how people process information in determining the causality of events. They focused on the non-observable elements of the system: perceptions and decisions. After Wildavsky developed the concept of risk as a social construct, Reason developed his model on organizational accident causation. A next step was taken by Hollnagel who identified the system as the full context in which errors and accidents occur. A gradual development of accident modeling shows three generations of human error modeling, from a sequential accident model, via human information processing accident models towards systemic accident models (Katsakiori et al., 2008). The evolution expands the scope of the investigation from sequencing events towards a representation of the whole system (Roelen et al., in press). In practice however, such accident modeling based on the Reason model proved difficult to apply, resulting in an increasing amount of varieties and simplifications (Sklet, 2004).

Most of the models restrict themselves to the work level and technological systems. Sklet concludes that this means that investigators focusing the government and the regulators in their accident investigation to a great need to base their analysis on experience and practical judgment, more than on the results from formal analytical methods. Much of the accident data are conceptually inadequate and flawed because of the inadequacies of underlying accident models in existing programs (Benner, 1985). Due to these pragmatic objections, during the conduct of an investigation, the limitations and mutual dependence between causation model and investigation methods should be explicitly taken into account. (Kletz, 1991; Sklet, 2004; Katsakiori et al., 2008).

Finally, such modeling and accident phenomenon perceptions do not comply with the needs of investigators: a translation of human error models to practical investigation tools is still in its early phase of development (Benner, 1996; Strauch, 2002; Dekker, 2006). Investigation methods should support the visualization of the accident sequence, providing a structured collection, organization, and integration of collected evidence, identification of information gaps in order to facilitate communication among investigators (Sklet, 2004; Benner and Rimson, 2009; Braut and Nja, 2010).

1.2.2. Towards a second generation

Creating a second generation of safety management systems, Rasmussen takes this modeling issue one step further (Rasmussen, 1997). He discriminates stable conditions of the past against a present dynamic society, characterized by a very fast change of technology, the steadily increasing scale of industrial installations, the rapid development of information and communication technology and the aggressive and competitive environment which influence the incentives of decision makers on short term financial and survival criteria. In answering the basic question: do we actually have adequate models of accident causation in the present dynamic society, he states that modeling is done by generalizing across systems and their particular hazard sources.

His risk management concept is a control structure, embedded in an adaptive socio-technical system. Since decisions made in a complex and dynamic environment are not only rational and cannot be separated from the social context and value system, a convergence occurs of the *economist* concept of decision making, the *social* concept management and the *psychological* concept of cognitive control. Modeling task sequences and errors is considered not

effective for understanding behavior. One has to dig deeper to understand the basic behavior shaping mechanisms. Rather than striving to control behavior by fighting deviations, the focus should be on making the boundaries explicit and known and by giving opportunities to develop coping skills at boundaries.

Task analysis focused on action sequences and occasional deviation in terms of human errors, should be *replaced* by a model of behavior shaping mechanisms in terms of work system constraints, boundaries of acceptable performance and subjective criteria guiding adaptation to change. System models should be built not by a bottom-up aggregation of models derived from research in the individual disciplines, but top-down, by a systems oriented approach based on control theoretic concepts. A convergence of research paradigms of human sciences *should be guided by cognitive science concepts* (Italics added).

According to Rasmussen, the fast pace of technology has lead to the introduction of the 'general due clause' and has enhanced the regulator ability to protect workers. Each employer 'shall furnish to each of his employees a place of employment which is free from recognized hazards that may cause death or serious harm'. By stating safety performance objectives, safety becomes just another criterion of a multi-criteria decision making and becomes an integrated part of normal operational decision making. In this way, the safety organization is merged with the line organization. This requires an explicit formulation of value criteria and effective means of communication of values down through society and organizations. The impact of decisions on the objectives and values of all relevant stakeholders are to be adequately and formally considered by 'ethical accounting' (Rasmussen, 1997).

Design and operation should be based on reliable predictive models of accident processes and probability of occurrences. A full scale accident then involves simultaneous violations of all the designed defenses. The assumption is that the probability of failure of the defenses individually can and will be verified empirically during operations even if the probability of a stochastic coincidence has to be extremely low. Monitoring the performance of the staff during work is *derived from the system design assumptions, not from empirical evidence from past evidence.*

Rasmussen identifies a limited series of hazards: loss of control of large accumulations of energy, from ignition of accumulations of inflammable material and loss of containment of hazardous material. When the anatomy is well bounded by the functional structure of a stable system, then the protection against major accidents can be based on *termination of the flow of events after release of the hazard*. When particular circumstances are at stake, the basis for protection should be on *elimination of the causes of release* of the hazard.

Preconditions and assumptions should be explicitly stated in a Probabilistic Risk Assessment. In this view, Rasmussen states, fortunately it is not necessary for this purpose to predict performance of operators and management. When a plant is put in operation, data on human performance in operation, maintenance and management can be collected during operations and used for a 'live' risk analysis. Thus, predictive risk analysis for operational management should be much simpler than the analysis for a priory acceptance of the design. Such performance data can be collected through other sources than accident investigations; incident analysis and expert opinion extraction may compensate for the lack of abundant accident data.

This second generation of safety management systems comprises of several functional elements: training and communication should provide awareness, adequate feedback and monitoring should facilitate assessment of the safety performance and the company's ability to learn and improve its management system (Rasmussen and Svedung, 2000). In his overview of the merits of safety management systems, Swuste concludes that scientific proof for the importance of all these elements is sparse. There is only limited empirical evidence that links management and horizontal characteristics to safety performance. Major disasters investigations indicate inadequacies in these systems, deficiencies in hazard recognition, an inability to focus on accident scenarios in decision making and complacency after a long accident free period (Swuste, 2009). Vaughan's analysis on organizational failures reveal that it is not only difficult for organizations to learn, but that they also are resistant to lessons from the past (Vaughan, 1999). Research indicates that the learning capacity of safety management systems in process industry and nuclear power plants is further hampered by the fact that there is a gap between the designer's assumptions on the system's functioning and experienced feedback on hazards and risks from operational systems. Workers are not in the loop and cannot respond rapidly and adequately when required (Swuste, 2009).

1.2.3. Towards a third generation

At present, the contours of a third generation of safety management concept are dawning: the resilience concept (Hollnagel et al., 2008a,b).

This concept defines failure as a normal phenomenon, being the flipside of success, since they are both the outcome of normal performance variability. Hollnagel defines a resilient system by its ability effectively to adjust its functioning prior to or following changes and disturbances so that it can continue its functioning after a disruption or a major mishap, and in the presence of continuous stress. Therefore, four essential abilities are identified: to cope with the *actual*, to flexibly monitor the critical, to anticipate the *potential* in dealing with disruptions and their consequences and to learn from the *factual.* An increased availability and reliability of functioning on all levels will not only improve safety, but also enhance control (Hollnagel et al., 2008a).

This concept differs fundamentally from the second generation of safety management systems. The allocation of scarce safety resources is not exclusive designated to a specific entity in the organization – such as a safety management system at the corporate level or rescue and emergency resources in public safety – but is made flexible and creates discretionary competences at the operator level to adapt their responses in different system states. Resilience facilitates a merger of staff and line responsibilities for safety, reducing redundancy in a modern concept of 'mean and lean' and 'cheaper, faster and better' resource management. Originating from the military, this resilience concept facilitates evolutionary change and provides improved business continuity in crisis situations. The concept however requires a series of new system characteristics in order to provide the necessary transparency on the actual and factual functioning of the systems. Accident investigations may serve as a problem provider for systems development by providing a timely transparency in the factual functioning of a system. Empirical information and operational experiences simultaneously provide feedback for a systems redesign and engineering of safety enhancement strategies (Stoop and Dekker, 2008).

Some doubt the concept (Roelen et al., in press). Such more advanced models should not connect to the current practice of safety data collection and analysis. It should be questionable whether safety managers can be made aware of new insights and modeling approaches: 'The air transport industry is quite conservative, regulatory changes are very slow and Reason's Swiss Cheese concept is still relatively new to most people within the industry without going a step further. It makes more sense to develop an event chain model that fits current practice rather than to develop models with a completely different concept, *however correct these concept might be*' (Roelen et al., in press, Italics added). In accident modeling, the linear sequence of events is a main disadvantage in preventing relative simple major accidents. Such modeling

however seems to suffice. The recently developed resilience engineering of dynamic modeling is questioned on its merits. Only time will tell whether the drift into failure will remain another nice metaphor or whether it can be turned into a practical tool offering new insights into risk prevention as Hale concluded in his valedictory lecture (Hale, 2006).

Developing new risk management models at the level of the aviation industry are derived from the assumption that aviation could benefit from the nuclear power industry and the process industry, which have demonstrated the benefits of a unified – probabilistic-model. The question however is whether this assumption complies with the specific characteristics of the aviation industry with its technology, multi-actor involvement and continuous, open access network configuration.

1.2.4. Safety investigations as public safety assessor

When many actors take part in the same complex and dynamic environment, they all must achieve consensus in order to share their learning (ETSC, 2001). Such self-organising and learning behavior of each of the participants should guarantee a continued safe performance of the system.

Rosenthal wonders 'If we are not capable to come to an agreement on the causes of disasters, should we restrict ourselves to dealing with the consequences or the resilience capability after a disaster? If we cannot analyse the complex reality and cannot achieve consensus, are we deemed to restrict ourselves to a battlefield of subjective opinions' (Rosenthal, 1999)? By doing so, the debate on safety needs arbitration between contradictions. Do safety investigations provide a solution in their role as a public safety assessor?

Some dispute the usefulness of such a role for accident investigations. This is not only an academic but also a practical debate, which originates from the beginning of the process industry. In these days, safety experts in the rapidly developing process industry wondered whether the sector was suitable for a safety approach which was also applied in more conventional sectors.

According to Frank Lees it was necessary to distinguish between occupational accidents on one hand – which were quire common, but not representative for the modern process industry – and on the other hand a class of accidents which were critical for the business continuity of the company and its primary processes (Lees, 1960). Because this second class was unacceptable and very uncommon, it should have little learning potential. Accident investigations therefore should be replaced by either modeling and incident analysis or other performance indicators which were more common. In this view, the top management of a company should have the responsibility for quantifying the risk and for developing a separate safety management system.

Lees formulated his doctrine under the conditions which were valid at that time:

- He dealt with fixed site, stand-alone equipment
- production processes are almost completely automated
- there is one central management taking all safety critical decisions
- decision making is restricted to the private company
- the state of technology is assumed constant
- only rational, mathematical decision making models have scientific validity.

This Lees doctrine applies a design concept in which humans are fallible factors and eliminated by design from the system by automation. Their remaining role is restricted to complying with rules which have been imposed by management. There is no room for the operator in taking critical decisions. Learning in practice is replaced by modeling and by a centralized assessment of all interests by a single party; the corporate management. This Lees doctrine has become the role model for safety management systems as postulated by Rasmussen. The assumptions of Rasmussen in his modeling however raise questions about the generalizability of the concept: is it valid to bridge the differences across the industrial domains by creating this general model with a limited category of hazards without a relation to the technological state of the art and a reflection on the role of the human operator?

2. Concepts and context

2.1. Differences across industrial domains: the aviation case

Transport systems apply completely different design principles than the process industry or nuclear power supply. First, at the control level the system is designed as a support for the operator; it is a human centered design with delegated responsibilities. Second, there is a strict separation between the planning and control level with respect to capacity management and traffic control. It is a distributed responsibility. Finally, there are differences in concepts of the human operator with respect to his interfacing with technology.

2.1.1. First; the delegated responsibility

To prevent accidents and incidents between vehicles, they are separated in time, in distance and by visual detection. This creates a triple redundancy. Time tables, signaling systems and in-vehicle equipment should assure this separation and should support the observations and decisions of the drivers. These three principles are under pressure. High speeds make a direct outside observation impossible. To maximize the availability of capacity and interconnectivity of the network, a maximum traffic density is desirable.

ICT applications offer huge opportunities for a rapid reconfiguration in capacity management and traffic process control. Dynamic control opens up the opportunity for maximizing punctuality and minimizing tracking times. Consequently, separation in distance is all that is left. This put high demands on technology and requires good faith of the operator in the supporting technology. Some think they can buy 'off the shelf 'components. Recent research work proves that such standard technology does not exist. We should rather think in terms of system architecture, system integration and continuous adaptation and upgrading of control technologies (ERTMS, 2007).

2.1.2. Second: the distributed responsibility

In addition to this delegated responsibility there is another safety principle at a higher systems level, a distributed responsibility.

We speak separately of traffic management in addition to traffic control. This separation is introduced in order to prevent a conflict of interest in a situation where one individual or authority should be responsible for balancing safety versus economy.

By the increase of ICT opportunities for dynamic adaptation, this principle also has come under pressure. Some believe in full automation by eliminating the operator and traffic controller, replacing them by computers. Some dream about unmanned aerial vehicles, or fully automated surge barriers, in which a black box defines what experience and expertise should be canned into computer algorithms, complying with predefined rules and procedures. Some think that the best guarantee for developing a clean and safe technology comprises of strict regulations (RIVM, 2003). Such a view captures any technological development at a rule based level of decision making. This should leave the knowledge based level of decision making solely to the responsibility of managers and governance. Safety has been considered a matter too important to be left to engineers (Edwards, 1972).

2.1.3. Third; human centered design or full automation?

This reductionist view on full automation does not only remove all redundancy from the system, but also denies the operator a possibility to learn from experiences. Traditionally, there is an expert role for the captain of a vessel and pilot of an aircraft. Their collective knowledge represents a capital for the sector which far exceeds the invested capital of each of the companies. By this feedback from practical experience, transport systems could develop into Non Plus Ultra systems: systems which could not be outrivaled because practical experiences were rapidly incorporated in adapted operations. The erosion of both delegated and distributed responsibilities leads to so-called sacrificial decision making. According to the Lees doctrine, risk decision making is reduced to a single actor issue; one party makes the critical decisions for other parties too.

If such safety critical decisions are not explicitly countered in the conceptual design phase or assessed at an institutional level, catastrophic consequences may occur in practice. The burden of conflict solving is transferred to front line operators (Steenhuisen and Van Eeten, 2008). Restricting one self to a proactive Environmental Impact Assessment and a Cost-Benefit Analysis during design and development of infrastructures is not enough. Doing so, safety is sacrificed against environment and economy. There is a clear need for a proactive Safety Impact Assessment before such concepts are applied in practice (TCI, 2004).

However, is the dilemma between investigation and management sufficiently explained by this operational dilemma between safety and economy or should we conduct a more thorough analysis into underlying scientific models and concepts, in particular concerning the role of human failure?

2.2. A scientific focus on the human factor?

In the 1950s academic experimental psychology distanced itself from applied and clinical psychology in pursuit of a scientific status reflecting that of physical ad biological sciences. Its methodology was modeled after 'hard' physical sciences based on reductionist laboratory methodology, leaving out 'cognitive' and a contextually based 'socio-technical' approach.

Consequently, a close link with engineering was required, identifying 'human engineering' by keeping abreast of specific sets of engineering techniques (Michon, 1971). Until the introduction of advanced computing capacity, experimental psychology was faced with the complexity of modern man–machine interfacing issues in dynamic systems, and a lack of powerful mathematical data processing techniques.

2.2.1. Towards various rationalities

Such a research methodology is bound to adopt oversimplification of the situation and to concentrate on single variable laboratory tasks. In conducting experiments, major classes of possible explanations are to be excluded. The priority in assessing experimental results was in the significance of their effects, rather than predicting the performance of individual operators. Context-free psychological laws were sought for, rather than a context which was considered to introduce both constraints and uncertainty. At a philosophical level however, the paradigms of social sciences are very different from applied sciences and engineering design. Engineering design and applied sciences are concerned with prediction in a specific context, not so much with explanation and the magnitude of effects is as important as their significance.

During a safety investigation, the distinction between these two rationalities may reveal itself as a false dilemma between finding the Truth about the true explanation of the event versus the Trust that can be put on the predictability and confidence we may have in understanding the actual sequence of events. Safety investigations may serve to solve this dilemma by establishing a timely transparency in the factual functioning of the system under scrutiny, merging the rationalities of engineering design, behavioral and social sciences.

In order to deal with prediction in human behavior, the notion of a mental model was first accepted in engineering design with respect to cope with the control, context and structure of complex systems. Such models however, were based on a reductionist scientific view, dealing with rational and analytic, linear decision making models, not yet taking into account the contextual, dynamic nature of decision making practices in a multi-actor environment. After a first generation of deterministic and static models, the need to model real life complexity introduced stochastic models, in which second order effects and systems dynamics could be modeled also.

Throughout this development, several schools of thinking in psychology dealt with human error. On one hand, there is a behavioral school, focusing on perception aspects, dealing with fatigue, medication, vision, hearing, while on the other, a cognitive school, focuses on information collection, storage, processing and decision making (Moray, 2007). From an investigator's perspective however, both schools have their value. There is no need to take sides in this struggle for recognition of cognitive psychology as a leading scientific discipline. Baron states that from an investigators point of view, both cognitive and behavioral approaches are equally important and should be viewed as complementary rather than disparate: 'To say that the behavioral approach is 'largely irrelevant' and should be 'submitted' for the more vogue cognitive approach is an egregiously shortsighted view on the part of researchers and investigators' (Baron, 2007).

However, there is a second distinction in human error research. In the allocation of responsibilities in risk perception and risk acceptance, a dual process in reasoning is distinguished with respect to the rationality of decision making (Slovic et al., 2004). On one hand there is a cognitive rationality (decision making based on rational arguments and validated knowledge) while on the other hand an emotional rationality exists (decision making based on ethical considerations, based on individual and social norms and values). These processes are equivalent because they each represent a distinct decision making process of the human mind. They complement each other rather than being contradictory and unfortunately, are not equally distributed across all stakeholders (Van Ravenzwaaij, 1994). Risk bearers think along lines of mental pictures, consequences and scenarios, while policy makers think along lines of frequencies, performance indicators and rational utility functions. There is a distinction between 'how' versus 'how often' (Hendrickx, 1991).

The goal of safety investigations into human decision making therefore is to establish and analyse the 'local' rationality of operators along the lines of how the event revealed it selves to the operator. This identifies a third rationality in the accident reconstruction process in addition to a technological and socio-psychological rationality (Dekker, 2002).

2.3. Involving higher systems levels

Is it justified to address professionals to comply with rules, standards and commitment to a company safety culture under pressure of disciplinary actions, resignation or social exclusion as whistle blowers? Can we learn from these experiences if we focus on skill and rule based behavior and exclude the knowledge based level and motivation. Human error should not be considered the cause of a mishap, but as a symptom of deeper trouble in the organization (Dekker, 2006).

Can we shift control towards the management level by prescribing a Safety Management System (Hale, 2006)? Probably not: there

are questions about their theoretical basis, there is little scientific research into their actual performance and there have been expressed doubts about a good understanding in practice. Some want additional governmental pressure for more local rules in self regulation, prescriptive rules for training, culture and safety climate as well. But more essentially: Safety Management Systems address private companies at a rule based level. A better strategy is addressing management at knowledge based levels by developing the concept of learning organizations. Should then also Board Room decision come under scrutiny, in order to bring transparency in their decision making processes (Johnson, 2007)?

Is there a role for public government in settling such safety critical decisions on a higher level that a private company (Van Vollenhoven, 2006)? With the change in governance from prescriptive regulation towards goal setting objectives a new phenomenon has emerged in which enforcement and inspection is separated into a process assessment and a substantive judgement.

3. New challenges and contexts

Are Rasmussen's assumptions still valid if the concept is expanded from the process industry and nuclear power supply to aviation and from the corporate level into higher systems levels? Do these assumptions create new dilemmas?

3.1. Dealing with different systems states

Decision making is not only about perspectives, it is also a question how people come to their decisions. In a neo-classical economical approach, a rational assessment of arguments is given by logic decision making rules, which are valid irrespective of the individual and the environment in which they operate. Such an assessment has neither a relation with the psychology of the decision maker, nor with the decision making process. There is only one valid outcome possible.

In contrast with this substantive rationality, the institutional economical school in thinking adds the environment to this rationality by taking into account the process and context of the decision making. This procedural rationality is intendedly rational, but limitly so. It is dependent on deliberations and depends on the process. It is determined by search mechanisms and storage of patterns, transaction costs, norms and habits. This rationality focuses on a satisfying and optimizing instead of a maximizing strategy. Investigations into such decision making processes emphasize a detailed empirical exploration of complex decision making algorithms. This school of economic thinking has relations with 'naturalistic' decision making theories and experiential learning theory.

There seems to be a gliding scale from a formal rational utility assessment towards a bounded rationality due to risk exposure. A position on such a scale seems to be dependent on the information processing capacity, the available processing time, the level of anxiety in risk perception and the criticality of the task performance.

1. A type of formal rationality, deploying risk decision making as a rational utility function with respect to information acquisition, assessment and actions. This type focuses on a maximizing strategy.
2. Bounded rationality, where time and processing capacity constraints exist caused by stress or overload. This type applies information filtering by relevance, trustworthiness and may lead to perception narrowing, and selecting a single task dominance.
3. High mental load, with high anxiety levels and mental overload and life threats perceptions. Such decision making refers to survival behavior, instinct and experience and is seemingly irrational and random.

During accidents and incident handling, the third type is likely to occur due to the high level of anxiety, perceived danger instinct and experience driven behavior.

The focus of an investigation is on exploring the bounded rationality, with respect to the beliefs, desires, intentions as expressed by the actions and behavior of the operator. The input for this exploration and reconstruction is descriptive information on the situation as it develops throughout the sequence of events; the accident scenario. In addition, the instructions which were available to the operator are explored, while the individual goals of the operator should be revealed by interviews and behavior reconstructions. Finally, the feedback of the environment and dynamic interrelations with the system should be explored. Issue at stake are whether there were delayed responses in time, lagging behind system state transitions, information saturation and resonance, and non-linearity due to dynamic responses and intermediate adaptations. In short: during the investigation, the actual system state should be identified as normal, deviant or in crisis in order to identify the decision making processes which dominate the various systems states and to identify the change variables which facilitate a recovery to the normal system operating state or a permanent adaptation to the new requirements and operating context.

3.2. Sacrificial decision making

Some state that making so-called 'sacrificing' decisions is inevitable: sometimes, something should be sacrificed, in submitting the interest of one party to the interests of other parties. To the decision makers in charge, it is not only a decision about their own career perspective or a formal cost-benefit consequence analysis. It may have an impact on vital interests of other stakeholders as well. Protecting whistle blowers who object these decisions or issuing a Code of Conduct for professional behavior is necessary, but not sufficient. We should respect the professional dignity of our crews and respect our passengers (Ten Hove, 2005). Like a most experienced accident investigator stated: treat the victims of an air crash as if you were among the victims yourself.

3.2.1. Safety as a corporate value

Such 'sacrificing' decision making however should not imply a moral judgment on these decision makers themselves. It indicates the necessity to explore the non-linearity of complex risk decision making. Such non-linearity deals with notions of 'affect' and 'context' which have to be taken into account in a dynamic decision making environment.

If we take into account contextual influences and the ability of human operators to adapt to changes in the working environment, we are left with the question: how can we assess their changes in behavior and activities?

Coping behavior of operators may be assessed:

- either as 'deviant' from prescribed behavior with a potential drift into failure as a negative and unacceptable consequence, or
- as a flexible adaptation in practice, deemed inevitable and acceptable, eventually re-assessed as a tolerable, rationalized normalization of deviance, leading to new working standards, which are even perceived as 'safe'.

Either we see the human operator as fallible, capable of 'error' and 'mistakes' in selecting unsafe workarounds and shortcuts, or we see operators as individuals at the sharp end, creating safety by constant adaptation to change and anticipating possible new risks. Their mindfulness is based on self-organizing behavior, to keep within safe performance boundaries. Their experiential

learning capacity minimizes drift into failure while working with small margins close to the boundaries of the operating envelope. Such an operator concept emphasizes their strategic behavior and feedback learning capacity from practical experiences.

3.2.2. Safety as a social value

Several parliamentary inquiries in the Netherlands into major infrastructure projects have revealed both a loss of process control and an uncontrolled loss of quality of the final result (ERTMS, 2007).

The progress in such a project can be characterized as a negotiation arena in which the process drives out the contents. This separation between process and contents creates a deficiency which should be taken care of at a national governmental level. In its survey on developments in public safety, the Dutch Advisory Council for Governmental Policy discriminates between safety as a private value versus safety as a public value. In complex situations, safety as a public value is dismissed or ignored too easily (WRR, 2008). Specific care should be taken into account on how safety is addressed or sacrificed in an increasing aggressive and competitive environment. Such assessment proves to vary considerably across the various industrial domains.

The Trias Politica provides an institutional separation between legislative, judiciary and executive powers. The autonomous ability to come to a substantive and expert judgement on complex issues has no relation with these three powers. This diagnostic ability could be identified as the Fifth Power of Montesquieu, in addition to the Fourth Power, bureaucracy. Governmental agencies are still searching for how to deal with this Fifth Power. These new responsibilities in the transition from old 'inspectorate' to a new 'safety authority' are not yet fully developed (Mertens, 2006).

There is no problem owner who ends the distribution of all safety aspects across the various ministries. It might well be that an institutional arrangement such as a Ministry of Safety is an answer. If some think that a Ministry of Safety is not worthwhile, then why is there a reason of existence for a Ministry for the other two aspects of economics and the environment? At this governmental level too, sacrificial decisions have been made to the disadvantage of safety versus economy and environment.

There is an uphill discussion on safety responsibilities from operator, manager, entrepreneur towards governance, shifting from private towards public safety. This discussion is frequently contaminated with the blame issue. According to James Reason we could ask ourselves the question: has the Pendulum swung too far? Are we about to blame society (Young et al., 2005)? Rather than repeating the Blame Game at all these levels, it is far more interesting to respond to Sidney Dekker's question: why did their decisions make sense to them at the time (Kletz, 1991; Strauch, 2002; Dekker, 2006)?

3.3. Truth versus trust

This topic has presented the debate with a dilemma in discussing two visions on operator decision making. A most interesting issue in this dilemma is how to deal with newly adapted standards. How do we assess the new standard, given the changes in the environment and external influences? Does the absence of accidents make this standard a 'good' practice?

In the one vision, we may consider deviation a 'failure' from safety management systems because of the non-compliant behavior of the operator, while in the other vision safety management systems may provide a warning system associated with impending risks due to the organizational change.

In the one vision, we may consider the 'drift into failure' a proof of insufficient and unreliable data collection, while in the other vision, weak signals may have been cloaked in organizational noise or lost due to neglect by group think, tunnel vision or contextual entrapment.

In one vision, the focus in the investigation is on the 'cause', blaming a poor performing operator, assessing the other operators as 'good' performers' under the new standard by a lack of negative feedback on consequences. In the other vision, the focus is on the 'reasonability' of the new standard, in a new contextual and cooperative situation, putting the burden of proof of 'failure' on the investigation agency, based on their single case investigation. In the other vision, the burden of maintaining the credibility and legitimacy of a strict enforcement is on the inspectorate and safety authorities, due to their harsh judgement on the non-validity of the new standard (De Bruijn, 2007).

In considering both visions, a new safety assessment dilemma is created, in either finding the Truth in causation or establishing Trust in the validity of the new standard and the reasonability of the sacrificial decisions that have been made.

There is a new role for safety investigation agencies in avoiding such a 'normative' dilemma as public safety assessors, in providing timely transparency in the factual functioning of the system itself, taking into account causality as well as contextual influences and comparability of situations.

In both notions however, safety is a difficult performance parameter to measure accurately due to its stochastic nature. In both notions, safety is an emergent property, which is difficult to express in quantifiable parameters, such as the frequency and severity of accidents, incidents and occupational diseases. In both notions, other performance indicators however are 'hard' parameters, which can be expressed in monetary values such as economical costs and benefits, or environmental parameters such as emission, carcinogenic or mutagenic effects.

4. Are safety investigations proactive?

In selecting risk decision making tools, we should take into account the goal and validity of the available tools rather than stigmatizing tools as 'obsolete' or 'modern'.

Conventional rational risk assessments are part of a wider spectrum of the way in which societal risk acceptance can be expressed. Group risk decision making is the linear part of the spectrum in which acceptance decreases proportionally with the number of victims. This part has a better fit for mathematical modeling than the parts in which affection or governance and crisis management are dominant. Selecting a number of victims as a transition point between the various segments is not so much a rational choice. It is open to debate and proves to be open to adaptation, depending on whether major events occur with a certain frequency. Also the allocation of instruments to the segments is more or less arbitrary because here too a strict distinction is not possible. Safety Management Systems and accident investigations are umbrella notions which can be applied in various forms to various types of problems.

Does this non-linearity of the value of human life have a practical meaning in the debate on risk perception and acceptance for the availability of risk control instruments?

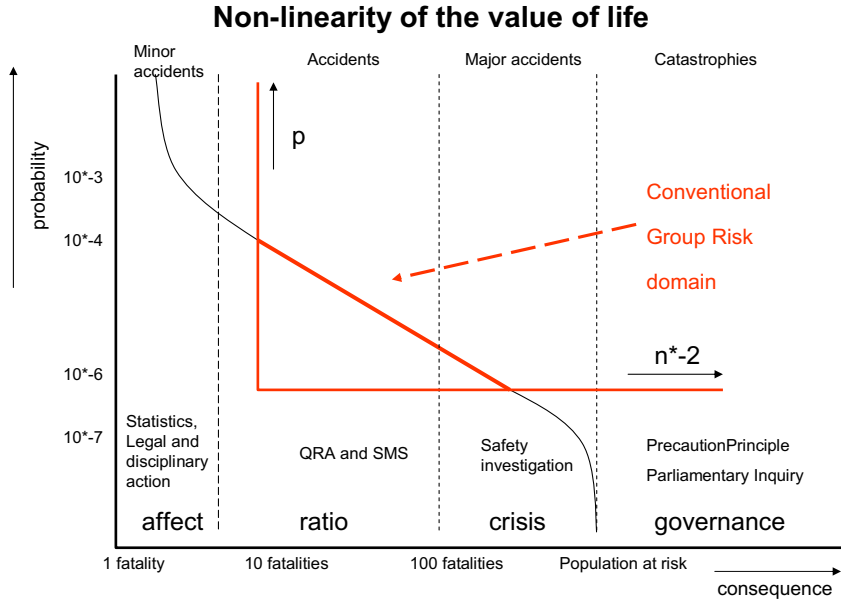
4.1. Non-linearity of the value of life

In defining various regions of non-linearity, discrimination is made in four segments in safety awareness and assessment, each with their specific and preferential instruments.

In the first segment the individual risk is a matter of personal involvement and perception. Identifiable loss and suffering are pivotal in communications with the environment. In this segment there is space for a personification of the events, an epic

concentration and projection of collective suffering onto a single individual. By introducing an icon value, large groups of victims may get a face back. In this way, Anne Frank personified the suffering of the Jewish population under the occupation and saving a single soldier – Saving Private Ryan-modeled the terror of warfare losses (Slovic et al., 2004).

Vision Zero concept for road safety. In the ETSC Annual Lecture in 2005, Tingvall notices a limited support for such a humanistic model. Some EU countries take up the concept, others have problems with communicating the concept. Others even question whether there is a sound ethical platform in this Vision Zero concept and refer to its social democratic context (Allsop, 2005).



In the second segment a rational assessment of frequent accidents with foreseeable consequences are central. This is the domain of Quantitative Risk Analysis and Safety Management Systems, in which data reliability and methodic validity are undisputed (RIVM, 2003).

The third segment is the domain of the low probability of a major event in which a timely transparency and recovery of public trust into the sector are essential.

The fourth segment is the domain of the societal unacceptable accident, irrespective of the sector involved in which the catastrophe occurred. After the occurrence of such an event, major changes and measures are taken – such as the closing of the Zeeland Estuary after the 1953 Storm surge – or a Parliamentary Inquiry is conducted into the lessons to be learned from the event. Since such events are unacceptable, Precautionary measures must be taken to prevent recurrence.

4.2. New developments: risk perception and social values

The second generation of safety management systems has seen problems in its implementation. Swuste refers to a fondness of rules, procedures, protocols and manuals: 'An ISO-madness puts a heavy burden on companies which seems rather addictive, creating demotivation among rule followers, while craftsmanship is undermined by detailed rules. Such an administrative concept can easily be interpreted as alibis for management for avoiding responsibilities for accidents' (Swuste, 2009).

The focus in safety management systems on accountability and rules is referred to in literature as the Anglo-Saxon model, in contrast with the Rhineland model which puts more emphasis onto stakeholder value and less to shareholder value. In addition, the Scandinavian humanistic concept of Vision Zero emphasizes the defense of the weak and deprived in society. Objections to this concept is that a Vision Zero concept should ignore the fact that safety is not a dependent property, but is part of a continuous trade-off, conflicting with other company's goals. The Swedish parliament has adopted a

This raises the issue of how to implement the concept of Rasmussen's 'ethical accounting'. Does it refer to the individual responsibility, creating whistle blowers within organizations or does it relate to higher systems levels, such as a national Vision Zero concept or the existence of independent safety investigation agencies as a Fifth Power of Montesquieu?

5. Conclusions

In answering the question – Are safety investigations pro-active? – the answer is a combined yes and no. Yes, because of the indispensable feedback that is required from empirical data and operator experiences in order to develop new knowledge and insights in the performance of complex systems. Such knowledge will be incorporated in the next generation of design and operations. A no is a formal correct answer, because this approach is complementary to other approaches in enhancing safety of complex systems. Among such approaches are safety management systems as discussed in this paper. They are complementary to each other and both submitted to change.

Modern safety investigations are characterized by:

- Evidence based information. Based on factual information and forensic sciences, such investigations provide transparency on the factual functioning of complex and dynamic systems, eliminating hypothetical and judgmental issues from a public and professional discourse.
- Knowledge based information. Safety investigations identify knowledge deficiencies in explaining events, consequently providing problem definitions for knowledge development in order to improve the comprehension of the systems' functioning.
- A systemic approach. In order to establish the causal complexity, meaning and interpretation of findings and the validity of recommendations, a systemic approach is required to structure the search during the investigation.

– Communication and dissemination. Investigations provide a case-based learning potential, which exceeds learning at a company level or even the sectoral level. Investigations facilitate a role as independent safety assessor in a public and professional debate irrespective of the sectoral or substantive value of the findings.

Safety investigations have developed, submitted to changes in society and scientific notions. In this respect they do not differ from 'modern' safety management systems and other methods. They originate from a specific domain – transport – and fulfill a specific 'niche' in the risk tool box, complementary with other instruments. Both instruments are neither obsolete, nor modern, but each require a careful positioning in the risk decision making spectrum, taking into account the non-linearity in risk decision making and risk assessment, the state of the art in technology, the specific characteristics of industrial sectors and an open, multi-actor decision making environment.

Acknowledgement

The authors thank W.R. Beukenkamp for his permission to publish the diagram on the non-linearity of value of life in risk decision making.

References

Ale, B., 2003. Ons overkomt dat niet. Inaugural lecture Delft University of Technology, 17 September 2003.
Allsop, R., 2005. Co-referring the 7th ETSC annual lecture. In: Europe and its road safety vision-how far to zero? The 7th European Transport Safety lecture. Prof. Claes Tingvall with comments of Prof Richard Allsop and Klaus Machata, Brussels.
Baron, E., 2007. Cognitive or behavioral Approach? April–June 2007, ISASI Forum, pp. 5–9.
Benner, L., 1985. Rating accident models and investigation methodologies. Journal of safety research 16, 105–126.
Benner, L., 1996. Accident Investigations: A Case for New Perceptions and Methodologies. National Transportation Safety Board, Washington, USA. The Investigation Process Research Resource Site.
Benner, L., 2009. Five Accident perceptions: their implications for accident investigators. Journal of System Safety, September–October 2009, pp. 17–23.
Benner, L., Rimson, I.J., 2009. Sifting lessons from the ashes: avoiding lost learning opportunities. In: 40th Annual Seminar "Accident prevention beyond Investigations". International Society of Air Safety Investigators.
Braut, A., Nja, O., 2010. Learning from accidents (incidents) – theoretical perspectives on investigation reports as educational tools. In: Guedes Soares, Matorell, (Eds.), Reliability, Risk and safety: Theory and Applications Bris, Taylor and Francis Group, London.
De Bruijn, H., 2007. Een gemakkelijke waarheid. Waarom we niet leren van onderzoekcommissies. NSOB, 2007.
Dekker, S., 2002. Reconstructing human contributions to accidents: the new view on error and performance. Journal of Safety Research 33, 371–385.
Dekker, S., 2006. The Field Guide to Understanding Human Error. Ashgate Publishing.
Edwards, E., 1972. Man and Machine: Systems for Safety. Loughborough: University of Technology, United Kingdom.
ERTMS, 2007. Een onafhankelijk onderzoek naar nut en noodzaak van de aanpassing van het HSL-beveiligingssysteem ERTMS. In: Stoop, J.A., Baggen, J.H., Vleugel, J.M., de Kroes en, J.L., Vrancken, J.L.M. (Eds.), Opdracht van het Onderzoeks – En Verificatiebureau van de Tweede Kamer der Staten Generaal Technische Universiteit Delft.
ETSC, 2001. Transport Accident and Incident Investigations in the European Union. European Transport Safety Council. Brussels.
ETSC, 2005. Europe and its road safety vision-how far to zero? In: The 7th European Transport Safety lecture. Prof. Claes Tingvall with Comments of Prof Richard Allsop and Klaus Machata. Brussels.
Freer, R., 1986. The Roots of Internationalism. 1783–1903. ICAO Bulletin 41 (3).
Freer, R., 1994. ICAO at 50 years: riding the flywheel of technology. ICAO Journal 49 (7), 19–32.
Hale, A., 2006. Method in Your Madness: System in Your Safety. Valedictory Lecture, 15th September 2006, Delft University of Technology.
Hendrickx, L., 1991. How Versus How Often. The Role of Scenario Information and Frequency Information in Risk Judgement and Risky Decision Making. Doctoral Thesis. Rijksuniversiteit Groningen.
Hollnagel, E., Nemeth, C., Dekker, S., 2008. Remaining Sensitive to the Possibility of Failure. Resilience Engineering Perspectives, vol. 1. Ashgate Studies in Resilience Engineering, Ashgate.
Hollnagel, E., Pieri, F., Rigaud, E., 2008. In: Proceedings of the Third Resilience Engineering Symposium. October 28–30, 2008 Antibes – Juan-les-Pins, France. Mines Paristech. Collection Sciences Économiques.
Johnson, K., 2007. Key Note Address to ITSA Meeting 16th May, 2007.
Kahan, J., 1998. Safety Board Methodology. In: Hengst, Smit, Stoop 1998, Second World Congress on Safety of Transportation. 18–20 February 1998, Delft University Press, Delft University of Technology.
Katsakiori, P., Sakellaropoulos, G., Manatakis, E., 2008. Towards an Evaluation of Accident Investigation Methods in terms of their Alignment with Accident Causation Models. Paper accepted for Safety Science, November 2008.
Kletz, T., (1991) *An engineer's view of human error*. Second Edition. Institution of Chemical Engineers. Warwickshire, UK.
Lees, F., 1960. Loss Prevention in the Process Industries, vol. 1. Oxford Butterworth Heinemann.
Mertens, F., 2006. Toezicht in een Polycentrische Samenleving. Inaugurele rede Technische Universiteit Delft, 26 April 2006.
Michon, J., 1971. Psychonomie Onderweg. Inaugural lexture at the University of Groningen, November 2nd 1971, Groningen, Wolters-Noordhoff.
Moray, J., 2007. The human factor of complex systems: a personal view. In: Dick de Waard, Bob Hockey, (Eds.), Human Factors Issues in Complex System Performance, Peter Nickel and karel Brookhuis. Snaker Publishing.
Rasmussen, J., 1997. Risk management in a dynamic society: a modeling problem. Safety Science 27 (2/3), 183–213.
Rasmussen, J., Svedung, I., 2000. Proactive Risk Management in a Dynamic Society. Karlstad, Sweden, Swedish Rescue Services Agency.
RIVM, 2003. Coping Rationally with Risks. Rijksinstituut Voor Volksgezondheid en Milieu. RIVM Rapport 251701047. Bilthoven, The Netherlands.
Roed-Larsen, S., Stoop, J., Funnemark, E., 2005. Shaping Public Safety Investigations of Accidents in Europe. An ESReDA Working Group Report. Det Norske Veritas.
Roelen, A., Lin, P., Hale, R., 2011. Accident modeling and organizational factors in air transport: The need for real models. Safety Science 49 (1), 1–106.
Rosenthal, U., 1999. Challenges of crisis management in Europe. In: International Conference on the Future of European Crisis management. The Hague, November 7–9th, 1999.
Steenhuisen, R., Van Eeten, M., 2008. Invisible trade-offs of public values: inside Dutch railways. Public Money &Management, 147–152.
Sklet, S., 2004. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 111, 29–37.
Slovic, P., et al., 2004. Risk as analysis and risk as feelings: some thoughts about affect, reason, risk and rationality. Risk Analysis 24 (2).
Stoop, J., 2004. Independent accident investigation: a modern safety tool. Special Issue of the Journal of Hazardous Materials. Papers from the JRC/ESReDA Seminar on Safety Investigation of Accidents, Petten, The Netherlands, 12–13 May, 2003. vol. 111, 2004, pp. 39–45.
Stoop, J., Dekker, S., 2008. In: Proceedings of the Third Resilience Engineering Symposium. October 28–30, 2008 Antibes – Juan-les-Pins, France.Mines Paristech. Collection Sciences Économiques.
Stoop, J. 2009. History of ITSA. <www.itsasafety.org/images/uploads/HistoryofITSA.pdf>.
Strauch, B., 2002. Investigating Human Error: Incidents, Accidents, and Complex Systems. Ashgate.
Swuste, P., 2009. You will only see it, if you understand it or occupational risk prevention from a management perspective. Human factors and Ergonomics in Manufacturing 18 (4), 438–4523.
TCI, 2004. Tijdelijke Commissie voor de Infrastructuur. Onderzoek naar infrastructuurprojecten. Reconstructie HSL-Zuid: de besluitvorming uitvergroot. Tweede Kamer, vergaderjaar 2004–2005, 29283, nr. 8, SDU, Den Haag.
Ten Hove, C., 2005. The Crisis After the Disaster. Aircrash Aftermath: A True Story. Aircrash of the Martinair DC-10 at Faro, Portugal. Wolf Legal Publishers, Nijmegen, The Netherlands.
Van Ravenzwaaij, A., 1994. Risico-informatie in het veiligheidsbeleid. Een analyse van de bruikbaarheid van kwantitatieve risico-informatie in het Nederlandse externe veiligheidsbeleid. Doctoral thesis, University of Utrecht, 1994.
Van Vollenhoven, P., 2006. RisicoVol/High Risk. Intreerede/Inaugural Lecture, Universiteit Twente 28 April 2006.
Vaughan, D., 1999. The dark side of organizations: mistake, misconduct and disaster. Annual Review of Sociology 25, 271–305.
WRR, 2008. Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid. Uncertain safety, responsibilities about physical safety. Wetenschappelijke Raad voor het Regeringsbeleid. Amsterdam University Press (in Dutch).
Young, C., Braithwaite, G., Shorrock, P., Faulkner, E., 2005. The (R)Evolution of human factors in transport safety investigation. ISASI Forum. July–September 2005.