

Accident modelling: from symptom to system

John Stoop^{1,2} & Sidney Dekker²

¹Delft University of Technology, The Netherlands

²Lund University, Sweden

Abstract

A series of surveys on accident investigation models show a wide variety of models, dedicated to specific industrial applications, domains and investigation aspects. In particular the investigation of human factors is exposed to a wide diversity of models. In reviewing such models, the majority proves to be a derivative from the Reason's Swiss Cheese causation model or the Rasmussen model on system hierarchy. Most of the models origin from the process industry and the energy sector. Application in the aviation industry has revealed their conceptual limitations. Due to their simplifications and lay interpretations, their intervention potential in practice is limited to linear solutions. In order to cope with socio-technological interactions in a multi-actor perspective, a full systems engineering design approach should be applied in a mission specific operating envelope. Such an approach is submitted to three paradigmatic shifts in investigation methodology. First; disengagement is required between event modelling and systems modelling. Second; a distinction in two design classes is required. A distinction is made between linear interventions within the existing design envelope and second order interventions focusing on expansion of the design solution space. Third; designing safer solutions in a multi-actor systems environment requires prototyping, virtual system model simulation and testing of limit state scenarios. Based on these constraints, a framework for safety enhancement is described, derived from experiences in the aviation industry itself. This framework is based on a new view on human error, a dynamic systems engineering design approach, analytical forensic abilities and institutional conditions for independent and qualified accident investigations.

Accidents and causation

Although accident models have been applied on a large scale in practice, a reflection on their methodological assumptions, scope and deficiencies reveals several schools of modelling. Several surveys indicate consecutive generations of models, their poor methodological basis, absence of a systems approach and a focus on the application of models by lay people (Benner, 1975, 1985, 1996, 2009; Sklet, 2004; ESReDA, 2005). The first accident causation models as derived by Heinrich in the 1930's referred to accident analysis by metaphors, such as the Iceberg Principle and Domino Theory. In a second generation of the 1970's Bird and Loftus applied a linear causality, while Kjellen introduced the deviation concept. Multi-causality was

In D. de Waard, A. Axelsson, M. Berglund, B. Peters, and C. Weikert (Eds.) (2010). *Human Factors: A system view of human, technology and organisation* (pp. 185 - 198). Maastricht, the Netherlands: Shaker Publishing.

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, in the 1980's 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. While Reason developed his model on organizational accident causation, a next step was taken by Hollnagel (2008) who identified the system as the full context in which errors and accidents occur. A gradual development of accident modelling shows three generations of human error modelling, from a sequential accident model, via human information processing accident models towards systemic accident models (Katsakiori et al., 2009). 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 modelling 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 and technical systems levels and exclude the technological nature and development of the inherent hazards. Sklet concludes that this means that investigators, focusing on government and 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 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., 2009).

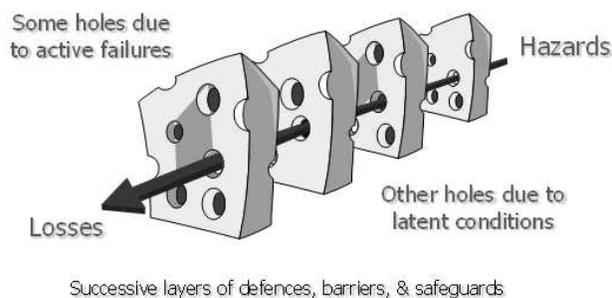


Figure 1. Reason's 'Swiss Cheese' model of organizational accidents

Similar to a technical toolkit for repairing technical systems, an accident investigator has to be able to choose proper methods analyzing different problem areas (Sklet, 2004). This raises the issue of ethics involved in selecting an investigative method. It is of particular significance that hypotheses can be validated and falsified during the investigation process. If not, it requires additional losses to validate hypotheses and to permit a pattern recognition or statistical analysis (Benner, 1985). Finally, such modelling 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).

Developing such methods in the domain of human behaviour will require a shift of focus from inferred and uncertain states of mind towards characteristics of human factors (Dekker & Hollnagel, 2004). Rather than allocating the cause of an accident to human error by complacency, loss of situation awareness or loss of control, the analysis could focus on falsifiable and traceable assertions, linked to features of the situation and measurable and demonstrable aspects of human performance (Dekker & Hollnagel, 2004). Rather than focusing on hypothetical intervening variables, more manifest aspects of behaviour should be recorded during an investigation. While accuracy and comprehensiveness are rarely criteria for explanations, plausibility and credibility are. In addition, it becomes a necessity to shift the focus from the performance of an individual towards the performance of a joint system, according to the principles of systems engineering. The analysis should look at the orderliness of performance rather than the mental states of operators. If such an orderliness of performance breaks down, this can be the start of further hypothesizing and investigations. This raises questions about the rationale why the performance seemed reasonable to the operator at the time of the event (Dekker, 2006). Such a shift towards the systems level in identifying new knowledge during air crash investigations has been proposed by Benner, applying an event based analysis, defined in terms of relations among events, set in a process and operating context. Such an approach permits a distinction between knowledge of systems processes and their operation and knowledge of the accident process. Such an event based analysis should be favoured because of the amount of new knowledge discovered, the relative efficiency of the search and the timely availability of corrective action guidance. Such knowledge can provide more valid indications of comparative performances and events (Benner, 1985).

The Rasmussen model

Rasmussen takes this modelling issue one step further (Rasmussen, 1997). He distinguishes the stable conditions of the past, versus the 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 modelling is done by generalizing across systems and their particular hazard sources. Risk management should be modelled by cross-disciplinary studies, considering risk management to be a control problem and serving to represent the control structure involving all levels of society for each particular hazard category. This, he argues, requires a system-oriented approach based on functional abstraction rather than structural

decomposition. Therefore, task analysis focused on action sequences and occasional deviation in terms of human errors, should be *replaced* by a model of behaviour 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. 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. Modelling task sequences and errors is considered not effective for understanding behaviour. One has to dig deeper to understand the basic behaviour shaping mechanisms. Rather than striving to control behaviour by fighting deviations, the focus should be on making the boundaries explicit and known and by giving opportunities to develop coping skills at boundaries. For a particular hazard source, the control structure must be identified, including controllers, their objectives, performance criteria control capability and information available about the actual state of the system. 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’.

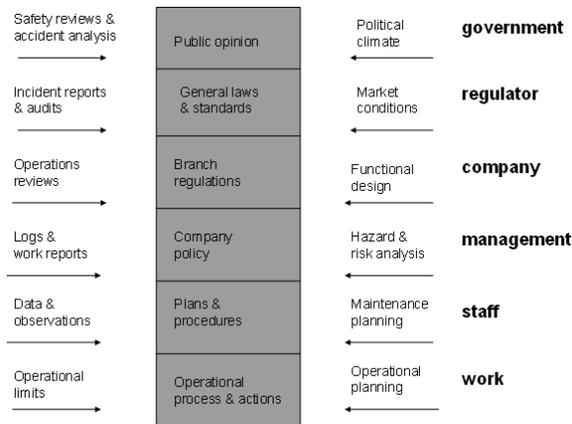


Figure 2. Rasmussen's systems hierarchy modelling

Depending on the nature of the hazard sources, three different categories are defined, characterized by their frequency of accidents and the magnitude of loss connected to the individual accident:

- occupational safety, focusing on frequent but small accidents. The average level of safety is typically controlled empirically from epidemiological studies of past accidents.
- protection against medium size, infrequent accidents. Safety systems evolve from design improvements in response to analysis of the individual, latest major accident. Safety control is focused on particular, reasonably well defined hazard sources and accident processes.
- protection against very rare and unacceptable accidents. In such cases the design cannot be guided by empirical evidence from past accidents due to the very large mean-time between accidents. Design and operation must 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*.

It therefore should be useful to develop more focused analytical risk management strategies and a classification of hazard sources in order to select a proper management policy and information system. The dimensions of a taxonomy for classification depend on the nature of the hazard source and the anatomy of accidents. Rasmussen identifies only a limited series of hazards: loss of control of large accumulations of energy, from ignition of accumulations of inflammable material, 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.

Defenses can be based on predictive analysis. The design of barriers is only accepted on the basis of a predictive risk analysis demonstrating an acceptable overall risk to society. When the predicted risk has been accepted, the process model, the preconditions, and assumptions of the prediction then become specifications of the parameters of risk management. Preconditions and assumptions must be explicitly stated in a Probabilistic Risk Assessment. In this view, 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 priori 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.

According to Rasmussen, the models required to plan effective risk management strategies *cannot be developed by integrating the results of horizontally oriented research* into different features of hazard sources and systems configurations. Instead, *vertical studies of the control structure are required* for well bounded categories of hazard sources, characterized by uniform control strategies (Rasmussen & Svedung, 2000).

Expansion towards 'real' models

In accordance with the desire to create more encompassing models in a dynamic environment, the Reason and Rasmussen model are superseded by a new series of risk management models. In shifting from accident investigation to other system performance indicators and their data on a daily basis, there is a need for modelling all possible causal event sequence scenarios in order to understand what is happening. Such an analysis should include technical, human and organizational factors, deeming the Reason model to be insufficient, due to its theoretical and partial modelling and the amount of occurrences that have to be processed every day (Roelen et al., in press). There is a need for 'real' models, covering every aspect and systems level, requiring a substantial mathematical background and user friendly software tools. Such models should incorporate fault trees, event trees and influence diagrams, which were adopted in the nuclear power industry already in 1975. Sophisticated PRA methods should provide establishing a relation between cause and effect, while influence diagrams should represent the influence of the context. Since airline safety analysts, safety managers and chief pilots have detailed knowledge but fail to identify systemic shortcomings, a framework is needed to help them to see the whole picture. Most of the effort is in classification of the data entry, with relatively little effort spent on analysis (Roelen et al., in press). Such a 'real' model should be integrated in order to represent the complexity and interdependencies, quantitative, transparent and should provide reproducible results, covering the whole aviation system.

This approach does not favour the introduction of new concepts or models. The concepts of Dekker to see socio-technical complexity as a web of dynamic, evolving relationships and transactions or the Leveson concept of systems as interrelated components that are in a state of equilibrium by feedback and control are not considered useful (Roelen et al., in press). The aviation industry should be too conservative and too slow responding in accepting new ideas, while Reason's Swiss Cheese model is still relatively new. An event model that fits current practice should make more sense than develop new models with a completely different concept, however correct these concepts might be (Roelen et al., in press).

Modelling accidents

Across the various domains, accident investigation and event modelling has seen different point of departure. On one hand there is a bottom-up approach in occupational risk and road safety: prevention of accidents, separating process safety from personal safety. Focus on isolated causational factors and single actor strategies (corporate management or the three E's of Engineering, Education and Enforcement.

On the other hand a top-down approach is applied in aviation, railways and shipping aiming at systems change and learning without separation between personal safety, process safety, external safety or rescue and emergency handling (ETSC 2001). Modelling accidents by decomposing accidents into a limited category of hazards and a predefined set of generic failure types deprives the analysis of two major components.

First, learning lessons for prevention of similar events. Prescriptive modelling of accidents forces the decomposition and description of the event into the format of the model. It also forces the event into an assessment of the correctness of the event in terms of compliance with the models normative assumptions and notions. In particular with human error modelling, such normative assessment remains implicit and obscures an explanation of the behaviour, based on motives, conditions, constraints and context. Prescriptive modelling denies local rationality at the operator level. In particular where pilots, mariners and drivers have their discretionary competence, such modelling rather obscures than clarifies human behaviour in high tech operating tasks. Their adaptive potential to new situations and ability to respond and recover in a flexible manner is the basis of their learning. It is a part of their internalization process of processing experience into knowledge. In a normative assessment, the operator is assumed to have a timely and full transparent oversight over all the available information, systems properties and of all his actions and their consequences. Such an investigator hindsight bias obscures the decision making in uncertainty which the operator is submitted to in practice (Kletz, 1991; Dekker, 2006). Such an analysis in which operator performance is assessed against normative behaviour is in contradiction with learning theory. In particular in complex high-tech systems, such an assumption of full and transparent information supply is not realistic and hence in conflict with bounded and local rationality theory.

Second, cross-corporate dissemination of lessons learned. In the Durkheimian and Weberian tradition, social sciences copied the notions of the most prominent scientific domain of the 19th century, the natural sciences, to mirror themselves to their merits and to surpass them by adapting their methodology (Matthews, 1978). This mechanism in establishing scientific esteem seems to be repeated in the 20th century, by mirroring management control modelling against engineering design principles. Already in 1972, the psychologist Edwards claims a more prominent role for the behavioural sciences in the integral design of aircraft and postulates the HELS model (Edwards, 1972). A 'traditional' focus on technical components should be unjustified, the 'linear' design method an anachronism. This claim is even more interesting because it is stated at the very moment of the development and roll-out of the major aviation innovation at the time: the first of the wide body generation of commercial jet aircraft, the Boeing 747. In his plea for involving psychology into aircraft engineering design, Edwards also criticizes accident investigation in aviation: the value should be limited, the frequency too low to draw useful conclusions, while the complexity should prevent an adequate analysis. Edwards follows the criticisms of Frank Lees in 1960, who did not see an added value for accident investigation in the process industry (Lees, 1960). Frank Lees shift a preference towards incidents, loss control and risk management. According to

Edwards, accident investigations should only be based on negative experiences, instead of positive experiences as well. Accident investigations should only be descriptive and lack explanatory potential. However, international aviation is a global, open transport network that can function exclusively on basis of mutual harmonization and standardization, high level performance demands and open access to the global network. Learning from accident in aviation therefore takes place at the international and sectorial level, not on national or corporate level, such as in the process industry or nuclear power supply. This learning is focused on technological improvements and open exchange of information at the level of international institutes such as International Civil Aviation Organization ICAO instead of national governmental inspection and limiting learning to the level of the private, multinational company. Safety as a societal value is a prerequisite for the international transport community due to its existence as a public transport system.

If we shift from managerial control strategies towards applying an engineering design approach to safety at the socio-technical level, what does this mean for the accident investigation process? How do we substantiate such an engineering design approach in the accident investigation methodology? How do we substantiate the concept of resilience engineering in practice (Hollnagel et al., 2008)? Two steps are to be taken into account: identification of the design solution space and the use of empirical evidence as an input for safety design specifications based on forensic engineering principles.

Towards new concepts

Safety enhancing interventions can be categorized in two main classes:

- Linear interventions and first order solutions. Simple problems allow restricting the design space. This is valid only if the number of solutions is small, the number of design variables is small, their values have limited ranges and optimizing within these values deals with sacrificing of aspects among the limited set of variables. Such interventions reinforce the design space in the detailed design phase by reallocation of factors, more stringent compliance with rules and regulations, elimination of deviations, applicable to simple, stand alone systems
- Complex interventions and second order solutions. Complex dynamic problems demands expansion of the design space. Such solutions focus on concepts and morphology, reallocation of functions to components, reconfiguration and synthesizing of sub-solutions, involvement of actors, aspects, teamwork, communication, testing and simulation. Such an expansion of the design space occurs in the functional design phase by developing conceptual alternatives and prototypes, applicable to complex and embedded systems.

When first order solutions have failed and did not prevent an event, a redesign of the system becomes necessary. In order to achieve such redesign, the event must be redefined in the first place by applying an engineering design methodology (Stoop, 1990; Dym & Little, 2004):

- *decompose the event* to identify contributing variables and their causal relations
- recompose the event by *synthesizing safety critical variables* into credible scenarios
- provide *analytical rigor* to the scenarios by identifying their explanatory variables, based on undisputed empirical and statistical evidence and scientific research
- make the *transition from explanatory variables towards control and change variables*
- develop *prototypes* of new solutions
- test the prototypes by *exposure to the accident scenarios* in a virtual simulation environment.

Designing safer solutions

In designing safer solutions, two fundamental questions are raised about:

- how to design safer solutions?
- how to generate the requirements for such a design?

In contrast with linear interventions and first order solutions, in complex systems there is no direct relation between a single contributing factor and its remedy. In redesigning safer solutions, there are three different focus groups for communication of the safety solutions: operators and actors within the system able to achieve a safe performance, knowledge providers for a better understanding of the system behaviour and change agents, able to govern and control the system. Each of these parties has a specific set of communication means, applying respectively metaphors, models or prototypes. Each of these parties applies its own vocabulary and reference frameworks, but should share a common notion in the end by a common means of communication. Applying a 'barrier' notion is a powerful communication metaphor, but does not help in case of a scientific modelling of the issue or applying a prototype in testing a solution.

Synthesizing solutions is necessary in order to establish a shared solution, based on the credibility, feasibility, compatibility, selection of preferred alternatives in order to create consensus among all parties involved in accepting the solution. Synthesizing is about recreating interdependencies into a new concept, network or configuration based on shared values. Complexity then can be defined as the interdependences of variables, choices and design assumptions. To deal with this complexity, it is not sufficient to decompose a system or event into its contributing variables and explanatory variables within its existing solution space, but also the design variables must be identified in order to serve as input for the systems engineering design process.

In addition, dealing with complexity and context is *not* adding more detail and levels to an event by increasing the decomposition, but *providing transparency at higher systems levels* with respect to its functioning and primary processes, and clarification of the conceptual properties, its configuration and composition. Increasingly complex accident modelling such as Accimap or STAMP does not make the transition from the event towards systems characteristics (Rasmussen and Svedung,

2000; Leveson, 2004). If the inherent properties of a system are not identified during design, they will manifest themselves as emergent properties during operations. Such properties are to be specified by stakeholders, actors and other parties which are to be exposed to the systems operational consequences and formulated in an overall Program of Requirements, leading to design specifications.

To assess the integral performance of the system, a synthesis should take place of all aspects in an encompassing Program of Requirements. Such a Program of Requirements becomes a consensus document, in which all actors involved have had the opportunity to express and incorporate their requirements, constraints and conditions during the assignment phase of the redesign.

A language issue; creating scenarios

In reconstructing an event sequence, we easily refer to the mechanical reconstruction from an engineering perspective. In unravelling the event sequence from a psychological or sociological perspective, we might prefer the phrasing of re-enactment of the event or re-configuration of the system state and operating environment.

Re-composition of an event enables event analysis. In order to communicate, a common reference framework is required, clarifying the various perspectives in recomposing the event:

- a technical perspective dealing with a *re-construction* of the physical system performance
- a behavioural perspective dealing with the *re-enactment* of decisions and discernable actions
- a systems perspective dealing with the *re-configuration* of the systems state and operating environment.

In order to create a common understanding among actors a common language and common notions are necessary. In risk discussions, the perception and acceptance of risk varies across actors, dependent on their position and interest. They may apply either a frequentistic or a scenario approach, dealing with either the frequency or the consequences of an event, a technological or a sociological approach or may apply a rationalist or an empathic approach (Hendrickx, 1991). These different approaches each have developed their own notions and language. In order to be able to communicate, there is a need for either a common language or a translation between these languages. This implies an understanding of each of the languages in the first place with respect to its linguistics, syntaxes, grammar and vocabulary. Decomposing such a language identifies the elements and building blocks of the language and facilitates analysis of their meaning and usefulness. For communication purposes however, a language cannot be spoken at such a decomposed level. A recomposition of these elements and building block takes place into a more complex communication structure to facilitate meaningful conversation. In analogy with music, poetry and literature, such a communication language is also applicable for accident analysis. The scenario concept provides such a common language, creating event narratives which form the basis for common understanding and agreement on

the description of accident phenomena in their context (Stoop, 1990). Achieving consensus on such accident scenarios provide a basis for a common risk assessment and shared solution space.

Shared solutions; redesign and prototyping

In complex interventions, the focus is on events in a systems context rather than on isolated factors and generic aspects, such as is the case with linear interventions. The reconstruction of events takes place by identifying and synthesizing explanatory variables into scenarios in their specific operating environment and constraints. Such synthesizing is primarily evidence based. The redesign of the systems is conducted along the lines of engineering principles by generating design alternatives in the enlarged design space into the form of a limited set of prototypes. These prototypes contain a relocation and addition of functions, changing the morphology and configuration and incorporate additional actors and aspects. The testing of these prototypes is conducted by running scenario tests, definition of limit state loads and simulation of complex, dynamic systems in virtual reality. Analyzing system responses, before they are put into practice, are based on First Time Right and Zero Defect strategies. The responses of a system can be determined by a gradual enlargement of the disruptions which are inflicted upon the system, until oscillation and instability occur. Responses of systems may become visible by a gradual or sudden transition to another system state by passing a bifurcation point. After such a transition, the safety of the systems can be assessed according to the acceptability of the new safety integrity level.

Technology in itself contains many forms, incorporating invisible knowledge, notions, principles and decisions from previous life cycle phases. The physical appearance of a product and process does not disclose inherent properties, principles or interactions to end-users in their operational environment. Design decisions are frequently made under conditions of high uncertainty. Safety margins and design standards, identification of failure mechanisms, probability assessment, consequence analysis and identification of a design envelope should reduce the uncertainty again to an accepted level. Designers deal with optimizing performance, and are not in a position to gain oversight into all uncertainties and unforeseen behaviour of their designs (Petroski, 1991; Carper, 2001). Such behaviour however can be designed into their processes such as with the Japanese design philosophy of Limit State Design or Critical State Design methodologies. Designers need an intellectual counterpart in assessing the safety of their design; accident investigators as forensic engineers play such a role.

Forensic engineering

Historically, designers needed a technical investigator, capable of recomposing the actual and factual sequence of events, the operating conditions and context, the factual technical functioning of the designs in practice. Such re-composition facilitated the drafting of redesign requirements. However, a re-composition ability should not only reproduce the physical reality, but also should encompass the knowledge, assumptions, decisions and safety critical issues which have been taken

into account and assessed with respect to their acceptability. Such ability should also incorporate the ability to recompose the socio-technical context and operating environment (Stoop, 2004; ESReDA, 2009).

From an investigator perspective, three kinds of systems designers should be supplied with a counterpart, each qualified with diagnostic and analytical skills from a technological/engineering design, organizational/managerial or governance/control perspective in order to cover the architecture of the overall socio-technical system. This can be expressed in the DCP diagram.

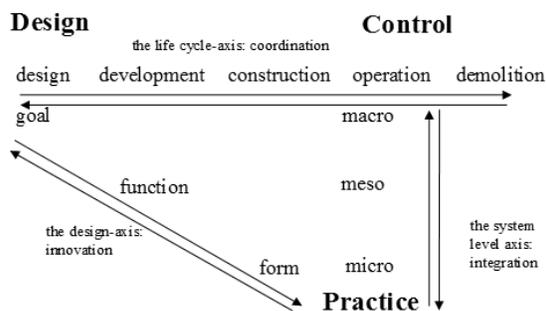


Figure 3. Stoop's DCP diagram

These three design-counterpart roles for investigators have been developing gradually over the past decades. Initially, with the development of technology, the technical investigator has matured, creating specialist approaches in many technological domains such as propulsion, structures, avionics, stability and control. Although the domain of human factors has seen major progress over the last two decades, the notions that have been developed in this domain are not yet readily applicable for investigation purposes (Strauch, 2002; Dekker, 2006). Translating theories on human factors into investigation tools is progressing, developing notions on bounded and local rationality, naturalistic decision making theories, a blame-free view on human error, high reliability organisations and resilience in organisational design. In the domain of governance and control the development is in an even earlier phase: this domain is developing classification schemes on failure, but is not yet in a phase of developing general concepts and notions of systems governance and control. Consequently, a framework and toolbox of investigation methods for conducting accident investigations at a systems level is not yet fully developed. Designers need counterparts for the assessment of their designs. Such a role is provided by accident investigators.

Conclusions

Although the Reason and Rasmussen models may well serve risk management in the process industry and nuclear power supply, there are doubts about their generalization towards the aviation industry. In practice, they are exposed to the risk of serving as reference metaphors and standards for generating generic, linear

solutions. On methodological grounds, Reason's model shifts the focus from accident causation towards human error analysis, while Rasmussen's model replaces accident investigation by management control in a socio-technical systems context. Consequently, both models do not comply with the needs of accident investigation theory and practices and systems engineering design needs in the aviation industry. Consequently, engineering design methodology may provide an alternative for improving the safety performance of complex systems at a socio-technical level.

The potential for systems engineering design in providing safer solutions requires to:

- Identify inherent properties before they manifest themselves as emergent properties
- Deal with complexity and dynamics by focusing on functions rather than on factors
- Focus on design principles and properties rather than optimizing performance
- Introduce systems dynamics by synthesizing interrelations into accident scenarios
- Apply a proof of concept by testing solutions in a dynamic simulation environment

Therefore, it is necessary to:

- develop event scenarios separated from systems models
- develop prototypes of safer solutions
- create dedicated virtual systems models, representing their specific characteristics
- facilitate testing and validation in these models, parallel to the real system

References

- Benner, L. (1975). Accident theory and accident investigation. In *Proceedings of the Society of Air safety Investigators Annual Seminar*, Ottawa, Canada, 7-9 October 1975, Sterling USA.
- 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*. Washington, USA: National Transportation Safety Board. The Investigation Process Research Resource Site.
- Benner, L. (2009). Five Accident perceptions: Their implications for Accident Investigators. *Journal of System Safety*, September-October 2009, 17-23
- Carper, K. (2001). *Forensic Engineering. Second Edition*. Florida, USA: CRC Press.
- Dekker, S. & Hollnagel, E. (2004). Human factors and folk models. *Cognition, Technology and Work*, 6, 79-86
- Dekker, S. (2006). *The Field Guide to Understanding Human Error*. Farnham, Surrey, UK: Ashgate.
- Dym, C. & Little, P. (2004). *Engineering design. A project based introduction. Second Edition*. New Jersey, USA: Wiley International Edition.

- Edwards, E. (1972). *Man and Machine: systems for safety*. Loughborough University of Technology. Loughborough, United Kingdom
- ESReDA (2005). Roed-Larsen, Stoop and Funnemark. *Shaping public safety investigations of accidents in Europe*. An ESReDA Working Group Report. February 2005, Det Norske Veritas, Oslo, Norway
- ESReDA (2009). *Guidelines for Safety Investigations of Accidents*. ESReDA Working group on Accident Investigation. June 2009. Oslo, Norway
- ETSC (2001). *Transport accident and incident investigations in the European Union*. Brussels, Belgium: European Transport Safety Council.
- Hendrickx, L. (1991). *How versus how often. The role of scenario information and frequency information in risk judgment and risky decision making*. Doctoral Thesis. Groningen, the Netherlands: University of Groningen.
- Hollnagel, E., Pieri, F., & Rigaud E. (2008). *Proceedings of the Third Resilience Engineering Symposium*. October 28-30, 2008 Antibes-Juan-les-Pins. MINES, Paris, Collection Sciences Economiques. Antibes, France
- Katsakiori, P., Sakellariopoulos, G., & Manatakis E. (2009). Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. *Safety Science*, 47, 1007-1015.
- Kletz, T. (1991). *An engineer's view of human error*. Second Edition. Warwickshire, UK: Institution of Chemical Engineers.
- Lees (1960). *Loss prevention in the process industry. Vol 1*. Oxford, UK: Oxford Butterworth Heinemann,
- Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, 42, 237-270.
- Matthews, E. (1978). *Max Weber, Selections in translations*. In W.G. Runciman (Ed.). Cambridge, UK: Cambridge University Press.
- McIntyre, G. (2000). *Patterns in Safety Thinking*. Farnham, Surrey, UK: Ashgate.
- Petroski, H. (1992). *To engineer is human. The Role of failure in Successful Design*. New York, USA: Vintage Books.
- Rasmussen, J. (1997). Risk management in a dynamic society: a modeling problem. *Safety Science*, 27, 183-213.
- Roelen, A., Lin, P., & Hale, A. (in press). Accident models and organizational factors in air transport. The need for real models. *Safety Science*.
- Rasmussen, J. & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.
- Sklet, S. (2004). Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials*, 111, 29-37.
- Stoop, J. (1990). *Safety and the Design Process*. Doctoral Thesis, Delft University of Technology. Delft, the Netherlands: Delft University Press.
- Stoop, J. (2004). Independent accident investigation: a modern safety tool. *Journal of Hazardous Materials*, 111, 39-44
- Strauch, B. (2002). *Investigating Human Error: Incidents, Accidents, and Complex Systems*. Farnham, Surrey, UK: Ashgate.