Jens Rasmussen Inge Svedung

Proactive Risk Management in a Dynamic Society

Räddningsverket
Swedish Rescue Services Agency

Jens Rasmussen, HURECON, Smørum, Denmark and
Inge Svedung, Risk Center, University of Karlstad

Proactive Risk Management in a Dynamic Society

Karlstad, Sweden
Swedish Rescue Services Agency

Acknowledgement
Mr Nils Olof Bäck has converted the structure for request of information described in appendix B and developed it into the preliminary version of the event reporting system based on a platform program discussed in chapter 9. He has also performed the data collection and analysis behind the statistic data and activity models presented in chapter 11.

Proactive Risk Management in a Dynamic Society

Risk & Environmental Department,
Swedish Rescue Services Agency, Karlstad
First edition, 2000
Graphic Design: Karin Rehman
Typeset: Ytterlids InfoDesign AB
Printed by: Sjuhäradsbygdens Tryckeri, Borås
Ordernumber: R16-224/00
ISBN: 91-7253-084-7

Abstract

The objectives of the present study are to better understand the mechanisms of major accidents in the present dynamic and technological society. From this understanding, guides to improved strategies for industrial risk management are sought.

It is important to consider carefully the present changes in a modern society when planning for industrial risk management. We are facing a period of technological change, deregulation, fierce competition, and increasing public concern. In a dynamic environment, hazard sources, their control requirements, and sources of disturbances change frequently and risk management can no longer be based on responses to past accidents and incidents, but must be increasingly *proactive*. That is, risk management must apply an *adaptive*, closed loop *feedback* control strategy, based on a measurement or observation of the level of safety actually present and an explicitly formulated target safety level. Due to human flexibility and creative intellectual powers, a human organization presents a particular potential for such an adaptive control, given the right conditions – people are a very important safety resource, not only an error source.

In this approach, risk management can only be discussed in depth when considering carefully the decision making involved in the *normal operation* of the hazardous processes posing potential for major accidents.

A key problem in this context is the information flow among the decision-makers at all levels of society: How are objectives, values, and operational targets communicated? How are the boundaries of safe operation identified and communicated? How is operation monitored through routine operational reports and reports from incidents and accidents? What do guidelines look like when an improved, consistent "safety control" must be established from a proactive control point of view?

The book discusses these issues on the basis of the present rapid evolution of new cognitive approaches to the study of decision making in action and dynamic, learning organizations, and the rapid change of modern information technology with its potential for design of effective decision support systems.

Table of Contents

1. Introduction

The background of the research program presented here is several contemporary trends. On one hand, the present dynamic and competitive society requires new approaches to risk management. On the other hand, the rapid development of information technology offers new opportunities for designing effective decision support tools.

Risk management in the present context is directed toward control of the risk related to the dynamic course of events following a disturbance of a potentially hazardous physical process. Risk related to long term exposure to the influence of hazardous substances or improper work conditions is not considered.

The following chapters discuss the requirements to an effective risk management strategy and suggest some promising avenues for development of operational tools for accident analysis, organizational safety reviews, and proactive risk management strategies for various different hazard domains.

A taxonomy of hazard sources and their respective control requirements is suggested to have a consistent basis for development of proactive risk management strategies suited for a dynamic, competitive society.

2. Risk Management in a Dynamic Society

Injuries, contamination of the environment, and loss of investment all depend on loss of control of a physical process capable of injuring people or damaging property. The propagation of an accidental course of events is shaped by the activity of people that either can trigger an accidental flow of events or divert a normal flow. Safety, then, depends on the control of work processes so as to avoid accidental side effects causing harm to people, environment, or investment.

Many levels of politicians, managers, safety officers, and work planners are involved in the control of safety by means of laws, rules, and instructions that are verbal means for the ultimate control of some hazardous, physical process. They seek to motivate workers and operators, to educate them, to guide them, or to constrain their behavior by rules, so as to increase the safety of their performance, see figure 2.1.

Compared to the stable conditions of the past, the present dynamic society brings with it some dramatic changes of the conditions of industrial risk management.

A *very fast pace of change* of technology is found at the operative level of society within all domains, such as transport, shipping, manufacturing and process industry. This pace of change is much faster than the pace of change presently in management structures – already Savage[1] talked about "second generation management applied to fifth generation technology" in manufacturing. This trend is also found in legislation and regulation. In consequence, a problem is found in the different time constants of change at the different levels of society. The dynamic interaction among the various levels during a period of change becomes an important modeling problem.

The *scale of industrial installations* is steadily increasing with a corresponding potential for large-scale accidents and very low probabilities of accident have to be demonstrated for the acceptance of operation by society. Consequently, models should not only include the normal or average performance but also very rare conditions.

The rapid development of transport systems, information technology, and just-in-time schemes leads to a *high degree of integration* and coupling of systems and the effects of a single decision can have dramatic effects that propagate rapidly and widely through the global society. This has been demonstrated by the effects of less successful computerized trading systems (e.g., the Hedge fund loss, in 1999[2] and the Wall Street turbulence in 1987[3]). It is thus becoming increasingly difficult to model work organizations in isolation and to make small-scale, local experiments to evaluate models.

Furthermore, companies today live in a very *aggressive and competitive environment* that will focus the incentives of decision-makers on short term financial criteria during economic crisis rather than on long term criteria concerning welfare, safety, and environmental impact.

2.1 Changing Research Needs

These trends have a dramatic effect on the necessary approach to modeling system behavior in some very fundamental respects, and they raise the problems of modeling by structural decomposition versus functional abstraction and the problem of cross-disciplinary research versus multi-disciplinary co-operation.[4]

1. Savage, C. M. and Appleton, D. (1988): CIM and Fifth Generation Management; In: *Fifth Generation Management and Fifth Generation Technology*. SME Blue Book Series, Dearborn, Michigan: Society of Manufacturing Engineers.
2. Coy, P., Wolley, S., Spiro, L. N., & Glasgall, W. (1998): Failed Wizards of Wall Street. *Business Week*, September 21, 1998, pp. 114–119.
3. Waldrop, M. M. (1987). Computers Amplify Black Monday. Science, Vol. 238, p. 602–604.
4. For a detailed discussion, see Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.

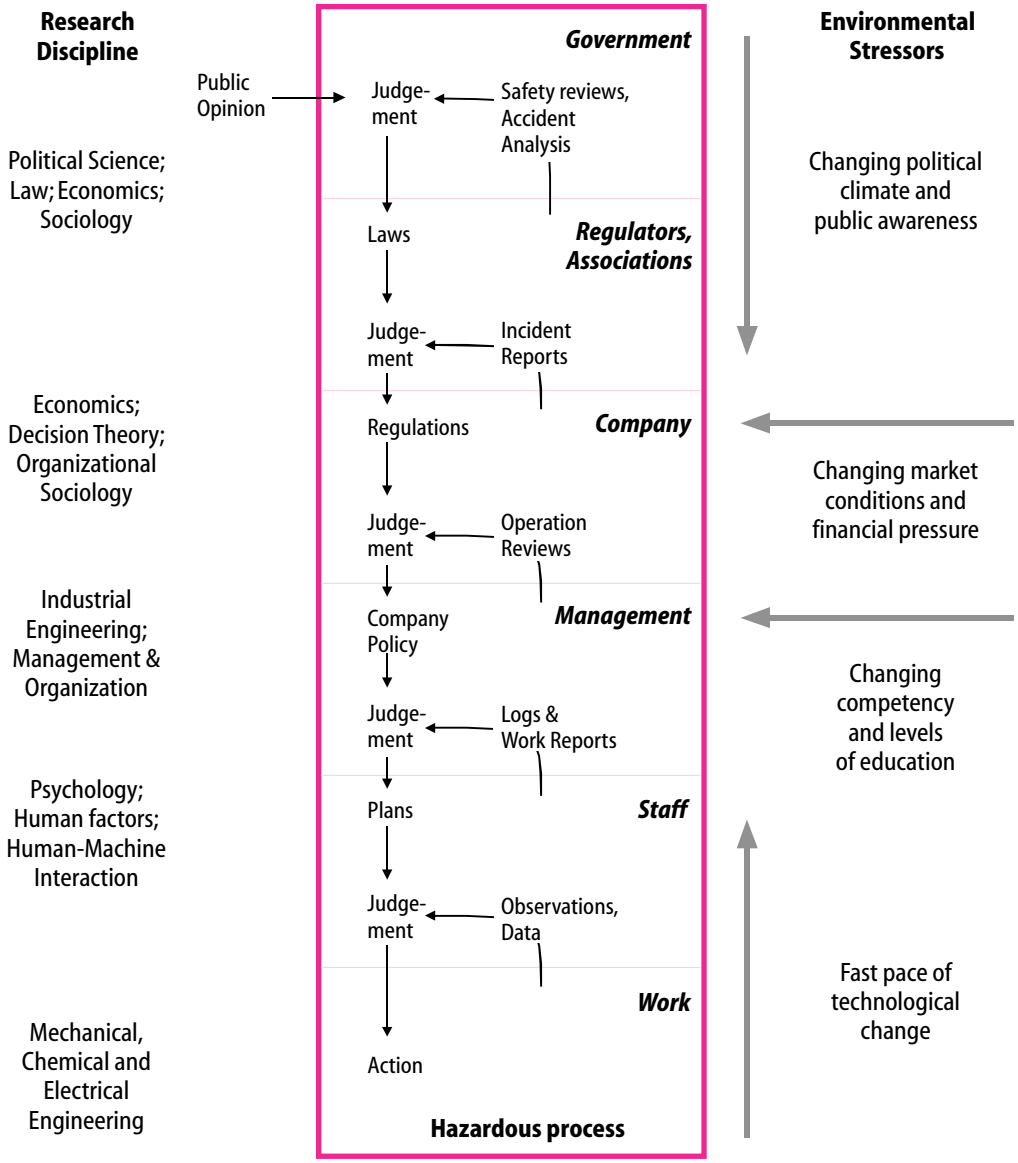
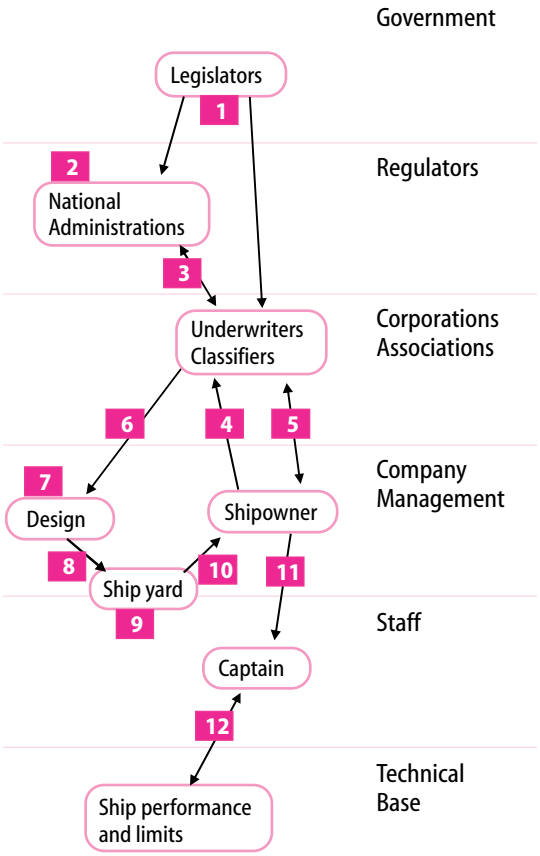


Figure 2.1. Many nested levels of decision-making are involved in risk management and regulatory rule making to control hazardous processes. This social organization is subject to severe environmental pressure in a dynamic, competitive society. Low risk operation depends on proper co-ordination of decision making at all levels. However, each of the levels are often studied separately within different academic disciplines.



Legend:
1, 2. The strategies for legislation appear to be inadequate during fast technological change.
3. Shipping industry's influence on legislators: Depressed shipping market of the 1980s leads to changes in its structure: Underwriters and National Administrations are neutralized by competition.
4. Ship owners influence classification societies.
5. Owners and classifiers co-operate and do not inform legislators adequately.
6. Communication from classifiers to designers is inadequate.
7. Design based on established practice inadequate during period of fast pace of change.
8. Inadequate specification and documentation from design. Shipyards rely on established practice during period of rapid technological change.
9. Quality assurance of shipyard questionable.
10. Inadequate communication between design, manufacturing and operating communities.
11, 12. Inadequate guidance to captain, learning by doing inadequate during fast pace of technological change.

Figure 2.2 Map of conflicts among actors in shipping.[5]

The usual approach to modeling socio-technical systems is by decomposition into elements that are modeled separately. This practice has some peculiar effects. The socio-technical system involved in risk management is, as shown in figure 2.1, normally decomposed according to organizational levels which are the subject of study within different disciplines.

Risk management at the upper levels normally is studied with a 'horizontal' orientation of research across the technological hazard sources. Traditionally, sociological studies are based on analysis of samples of organizations or groups of people with no detailed consideration of the actual processes found at productive bottom level. Analyses are based on statistics and industry-wide questionnaires, and great effort is spent on getting "statistical significant" data. In this way, management theories tend to be independent of the substance matter context of a given organization.[6]

The same practice is found in management theories in a

5. Sources: Shell, (1992): A Study of Standards in the Oil Tanker Industry, Shell International Marine Limited; May 1992.
Estonia. (1995): Accident Investigation Report; Part Report covering technical issues on the capsizing on 28 September 1994 in the Baltic Sea of the ro-ro passenger vessel MV ESTONIA. The Joint Accident Investigation Commission. Stockholm: Board of Accident Investigation.
Stenstrom, B (1995): What Can We Learn from the ESTONIA Accident? Some observations on technical and human shortcomings. The Cologne Re Marine Safety; Seminar Rotterdam; 2728 April 1995.
6. Barley made a similar observation when studying a particular work domain – radiological work in medicine. See Barley, S. R. (1988): On Technology, Time, and Social Order: Technically Induced Change in the Temporal Organization of Radiological Work. In: F. A. Dubinskias (Ed.): *Making Time*; Philadelphia: Temple Univ. Press.

business school context. To be manager is regarded as a profession, independent of what you are managing; a hospital, a manufacturing company, or a bank. Also the aim of commercial companies presently appears to change from being organizations serving a particular substance matter domain toward a narrow focus on financial operations.[7] What are the implications of this situation on the societal control of the safety of industrial installations? Following a Scandinavian ferry accident (Scandinavian Star fire), a marine safety official noted on a TV interview that we might see a decrease in naval safety, since ships were increasingly operated by banks and investors rather than shipping professionals.[8] Also commercial conflicts appear to influence the inter-organizational relationships, see figure 2.2. Such fierce competition together with de-regulation raises concern also in aviation[9] and nuclear power.[10] We need more studies of the vertical interaction among the levels of socio-technical systems with reference to the nature of the technological hazard they are assumed to control.

While a *system* traditionally is modeled by structural decomposition into structural elements, the dynamic *behavior of systems* and their actors is modeled by decomposition of the behavioral flow into events, acts, decisions, and errors. Such decomposition is the basis for identification of activity elements in terms of 'tasks' and task elements in terms of 'acts.' The problem is, that all work situations leave many degrees of freedom for choice by the actors, even when the objectives of work are fulfilled. To complete a description of a task as being a sequence of acts, these degrees of freedom must be resolved by assuming additional performance criteria that appear to be 'rational' to a task analyst or instructor. They cannot, however, foresee all local contingencies of the future work context. In particular, a rule or instruction is often designed separately for a particular task in isolation whereas, in the actual situation, several tasks are active in a time sharing mode that poses additional constraints on the procedure to use.

These constraints are often not known by designers and work planners. In consequence, rules, laws, and instructions practically speaking are never followed to the letter. Strikes by civil servants take the shape of "working-according-to-rules." Even for highly constrained task situations such as nuclear power operation, modification of instructions is repeatedly found[11] and the operators' violations of rules appear to be quite rational, given the actual work load and timing constraints. One implication in the present context is that following an accident it will be easy to find someone involved in the dynamic flow of events that has violated a formal rule just by following established practice. He or she is therefore likely to be exposed to punishment. Consequently, accidents are typically judged to be caused by 'human error' on part of a train driver, a pilot, or a process operator.[12] A task description or an instruction is an unreliable model for judging behavior during actual work, as found in a dynamic society.

Another example of decomposition of behavior is the modeling of behavioral control in terms of 'decisions.' In classic decision research 'decisions' have been perceived as discrete processes that can be separated from the context and studied as an isolated phenomenon. In field studies, however, it is often difficult to isolate proper decisions. In a familiar work environment, actors are immersed in the work context for extended periods; they know by heart the normal flow of activities and the available action alternatives. During familiar situations, therefore, analytical reasoning and planning are replaced by a simple choice among familiar action alternatives, that is, by practice and know-how. When, in such situations, operational decisions are taken, they will not be based on rational situation analysis, only on the information which, in the given context, is necessary to distinguish among the perceived alternatives for action. Separate 'decisions' therefore

7. See e.g., Engwall, L., (1986): Newspaper Adaptation to a Changing Social Environment: A Case Study of Organizational Drift as a Response to Resource Dependence. European Journal of Communication, 1, September, pp. 327341.
8. A recent critical review of the effects of this trend on management behaviour in, e.g., public health care, is found in Rees, S. and Rodley, G. (Eds.) (1995): The Human Costs of Managerialism: Advocating the Recovery of Humanity. Leichhardt NSW: Pluto Press of Australia.
9. See Schiavo, M. (1997): Flying Blind, Flying Safe, New York: Avon Books.
10. See Meshkati, N. and Butler, T. S. (1999): Potential Safety and Environmental Risks of Electric Deregulation in the United States: The Case of Nuclear Power Plants. *Proceedings of the 3' International Conference on Human Factors in Nuclear Power Operation.* Mihama, Japan: Institute of Nuclear System Safety.
11. Fujita, (1991): What Shapes Operator Performance? Proceedings of the JAERI Human Factors Meeting, Tokyo, November, 1991. Tokai Mura, Japan: Japanese Atomic Energy Research Institute.
    Vicente et al. (1995): A Field Study of Operator Cognitive Monitoring at Pickering Nuclear Generating Station. Tech. Report CEL 9504. University of Toronto: Cognitive Engineering Laboratory.
12. Rasmussen, J. (1999): The concept of human error: Is it useful for the design of safe systems in health care? In: Vincent, Ch. (Ed.): Risk and Safety in Medicine. London: Elsevier.

are difficult to identify and study of decision making cannot be separated from a simultaneous study of the social context and value system in which it takes place and the dynamic work process it is intended to control. This problem has led to skill-, rule-, knowledge distinction for cognitive control of behavior[13] and the recent paradigms of 'naturalistic' decision making.[14] In general, the present interest in cognitive science has brought with it a convergence in the economist's concept of 'decision making,' the social concept of 'management,' and a psychological concept of 'cognitive control' of human activity.[15]

Considering the problem of the frequent deviation from normative work instructions and rules, it is no wonder that it is often concluded in accident reviews that 'human error' is a determining factor in 70–80 % of the cases. Furthermore, multiple contributing errors and violations of rules are normally found, and are likely to be classified as being 'resident pathogens'[16] even when they are quite normal variations in the usual practice.

It should be considered that commercial success in a competitive environment implies exploitation of the benefit from operating at the fringes of the usual, accepted practice. Closing in on and exploring the boundaries of normal and functionally acceptable boundaries of established practice during critical situations necessarily imply the risk of crossing the limits of safe practices. Correspondingly, court reports from several accidents such as Bhopal, Flixborough, Zeebrügge, and Chernobyl demonstrate that they have not been caused by a coincidence of independent failures and human errors. They were the effects of a systematic migration of organizational behavior toward accident under the influence of pressure toward cost-effectiveness in an aggressive, competitive environment.[17] Consequently, the first step toward a *proactive* risk management strategy will not be to predict and avoid exotic causes of accidents, but to ensure operation within the design envelope, that is, to support management in respecting the preconditions for safe operation as specified during design.

To plan for a proactive risk management strategy, we have to understand the mechanisms generating the actual behavior of decision-makers at all levels. We have to identify the information needs of decision-makers both with respect to the actual state of affairs and to values and objectives, and we have to identify aspects that are sensitive to improvement and, therefore, the targets of guidelines for industrial risk management.

In conclusion, an approach to proactive risk management involves the following analyses:

- A study of the normal activities of the actors who are preparing the landscape of accidents during their normal work, together with an analysis of the work features that shape their decision making behavior.
- A study of the present information environment of these actors and the information flow structure, analyzed from a control theoretic point of view.
- A review of the potential for improvement by changes of this information environment. This involves an improved top-down communication of values and objectives through society and companies together with an improved bottom-up information on the actual state-of-affairs in terms of work reports including reports on events indicating resource limitations.
- Guidelines for improving these aspects in practical work environment for different classes of risk sources and management strategies.

For this development, we need a taxonomy of hazard sources and safety control strategies to facilitate the transfer of experiences and regulations among different industrial activity domains.

13. Rasmussen, J. (1983): Skill, Rules and Knowledge; Signals, Signs, and Symbols, and other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics. Vol. SMC-13, No. 3, 1983.
14. For a review, see Klein, G., J. Orasanu, R Calderwood and C. E. Zsambok (Eds.) (1994): Decision Making in Action: Models and Methods. Norwood, NJ: Ablex.
15. Rasmussen, J. (1997): Merging paradigms: Decision Making, Management, and Cognitive Control. In: Flin, R., Salas, E. Strub, M. E., Marting, L.: Decision Making under Stress: Emerging Paradigms and Applications. Aldershot: Ashgate.
16. Reason, J. (1990): Human Error. Cambridge, UK: Cambridge University Press.
17. Rasmussen, J. (1993): Market Economy, Management Culture and Accident Causation: New Research Issues? Proceedings Second International Conference on Safety Science. Budapest: Meeting Budapest Organizer Ltd.

    Rasmussen, J. (1994): Risk Management, Adaptation, and Design for Safety. In: Sahlin, N. E. and B. Brehmer (Eds.): Future Risks and Risk management. Dordrecht: Kluwer. 1994.

2.2 The Outlines of a Proactive Strategy

A proactive approach is thus proposed to risk management. Instead of a strategy based on attempts to remove causes of human error, an attempt is made to design a strategy based on:

- An identification of the boundaries of safe performance,
- Efforts to make these boundaries visible to decision makers and
- Efforts to counteract pressures that drive decision-makers toward the boundaries.

Since most serious accidents have been caused by operation of hazardous system outside the design envelope, the basic problem in design of improved risk management strategies is to ensure an improved interaction among the decision making and planning strategies at the various levels shown in figure 2.1. However, a scheme for improved interaction cannot be created by integration of research results from the various disciplines studying the individual levels, due to the basic differences in conceptual reference frames, research paradigms, and language of representation.

In consequence, results from present academic research must be reinterpreted and often supplemented by analysis based on a model suited to capture the function of the entire system aiming at proper control of the normal as well as disturbed operation of the potentially hazardous processes of a particular company.

Considering the dynamic nature of a modern society with companies and institutions constantly striving to adapt to a dynamic environment, the usual approach to modeling the system by decomposing it into elements and describing its function by causal interaction among these elements is not reliable. Causal explanations cannot be used for systems that include closed loop interactions and adaptive changes. Instead, models in terms of functional abstraction are required, describing the information flow structure within the entire system involved in the control of the hazardous processes. This approach can be used to design and analyze reliably a system, even when its functional elements are subject to unpredictable changes. There is a basic difference between the requirements to design and analysis of;

- systems controlled by *pre-planned strategies* and prescriptive procedures and
- systems controlled by *closed-loop feedback strategies*.

A simple example will be given below. This distinction is particularly important during a period when we are faced with a trend away from prescriptive legislation toward performance based legislation.

2.2.1 Preplanned Control

A simple open-loop example is shooting at a target with conventional artillery. Aiming involves a pre-calculation of the parabolic trajectory of the shell from an assessment of the distance to the target and the initial velocity of the shell. If the target is moving, its velocity must be estimated and the aim corrected so as to predict its location at the arrival time of the shell. In addition, compensation for the effects of disturbances such as wind, rain, etc. is necessary. In short, the shooting task is pre-planned by a detailed design of the functional trajectory of the shot and a detailed instruction is given to the gunner. Any change after the trigger has been released will cause the shell to miss its target (this mode of control corresponds to the scientific management paradigm and to the related prescriptive mode of regulation).

2.2.2 Closed-Loop, Feedback Control

To appreciate the difference between an open- and a closed-loop strategy, compare aiming of the artillery cannon to the use of an active, target seeking missile that can itself observe the location of the target (by radar, television or heat sensing). To plan a shot, it is only necessary to specify the target (the objective) to the missile that then 'locks on' to it. The location of the target is observed by the missile and is compared with the projection of its own current goal and the missile continuously adjusts its direction of travel to intersect the target. In addition to *specifying the target*, the planner/designer needs only information on the *capability* of the system such as the maximum range of the missile, its top velocity, and its maneuvering capability which all have to be adequate for the desired category of chases. Information about changes and disturbances are not needed, as long as the closed loop control system is within its capability design envelope (cf. managing by objectives).

2.2.3 Proactive, Closed-Loop Safety Control

From here it is clear that modeling the performance of a closed-loop, proactive risk management strategy must be focused on the following questions:

1. The *decision-makers* and actors who are involved in the control of the productive processes at the relevant levels of the socio-technical system must be identified.
2. The part of *the work-space under their control* must be defined, that is, the criteria guiding the allocation of roles to the individual controllers must be found.
3. The *structure of the distributed control system* must be defined, that is, the structure of the communication network connecting collaborating decision-makers must be analysed.

From here a number of questions related to the information available to the decision-makers and their capability of control must be considered:

4. *Objectives*: Are *objectives* and values with respect to operational as well as safety issues properly communicated within the system?
5. *Status information*: Are the individual decision-makers (staff, management, and regulators) properly *informed* about the system status in terms comparable to the objectives? In particular, are the boundaries of acceptable performance around the target-state "visible" to them?
6. *Capability*: Are these decision makers *competent* with respect to the functional properties of the organization, of the technical core and the basic safety design philosophy? Do they know the parameters sensitive to control of performance in a changing environment?
7. *Awareness*: Are decision-makers *prompted* to consider risk in the dynamic flow of work? Are they – continuously during normal work – made aware of the safety implications of their every-day work business decisions?
8. *Priorities*: Are decision-makers *committed* to safety? Is management, for instance, prepared to allocate adequate resources to maintenance of defenses? Does regulatory efforts serve to control management priorities properly?

This approach involves the study of the communication structure and the information flow in a particular organization to evaluate how it meets the control requirements of particular hazardous processes.

The following chapters will be organized as follows:

– First, Chapter 3 discusses the analysis of past cases that will set the priority of risk management. This will direct the attention toward the relevant sectors of industrial domains and identify the organizational bodies and decision-makers that were involved in the preparation of accident scenarios of the past.
– Next, in Chapter 4 the control objects of proactive risk management will be discussed. Different kinds of hazard sources embedded in different kinds of work system require different hazard control strategies. Therefore, a taxonomy of hazard sources and operational systems will be suggested in Chapter 5 together with the relevant proactive risk management strategies. Then follows in Chapter 6 a discussion of the preconditions for proactive risk management. The resulting approach to the design of proactive management support systems is presented in chapter 7. On this basis, Chapter 8 presents an approach to the implementation in the form of a computer-based analysis and auditing tool and Chapter 9 compares proactive risk management approaches to the current development of total quality management systems.
– Finally, Chapter 10 gives a brief discussion of an approach to emergency management and rescue services and compares with the proactive risk management approach presented in the previous chapters. Chapter 11 includes a review of a field study focused on the normal work activities within one element of the transportation of hazardous goods. In an appendix, reviews of a number of accident cases are found that have been the basis for the methodological developments.

3. Analysis of Accident Scenarios

Analyses of past accident scenarios serve to describe the socio-technical context within which accidental flow of events are conditioned and ultimately take place. This analyses have several different phases and the chapter outlines these phases and present some graphic representations we have found useful to structure the analyses and as 'conversation pieces' during interviews with involved decision-makers and actors.

3.1 Introduction

Study of decision making for protection against major accidents involves an identification of the interaction found between the effects of decisions made by different actors distributed in different organizations, at different level of society, and during activities at different point in time. We have to consider that all these decision-makers are deeply emerged in their normal, individual work context. Their daily activities may not be coupled in any functional way, only the accident as observed after the fact connects their performance into a particular coupled pattern. By their various independent decisions and acts, they have shaped a causal path through the landscape along which an accidental course of events sooner or later may be released. A release that is very likely caused by yet another quite normal variation in somebody's work performance – which very likely then will be judged the 'root cause' after the accident.

Thus we are not looking for the decision errors that are traditionally being considered causes of accident, we seek to identify all the organizational bodies that contributed to the creation of the accident scenario, whether or not they have violated rules or committed errors. For this analysis we have to develop further the traditional formats for accident analysis.

Analysis of past accident scenarios serves to identify the relevant actors and decision-makers and generalization from a set of representative accidents can define the patterns of hazards within an industrial sector that is in focus for proactive risk management efforts and thus prepare for a detailed work analysis. Finally, such a work analysis can lead to definition of the preconditions for safe operation that should be in focus of proactive risk management strategies.

Graphic representations of the causal flow of accidents have been very important tools in industrial risk management for decades. Causal trees, event trees, and cause-consequence-charts have been applied extensively to manage the complex flow of events to consider during post event analysis to understand accidents and during predictive risk analysis for design of protective systems. Such graphic representations have been very effective in creating an overview of complex occurrences and for communication of assumptions and findings within a risk analysis and design team.

Representational schemes have quite naturally been focused on the propagation of the effects of 'abnormal' events such as technical faults and human errors through the functional structure of a technical system, because a substantial part of the development has been focused on industrial process plants. It has, however, been increasingly acknowledged that organizational and social factors should be included in risk analyses leading to the development of tools such as MORT – the Management Oversight and Risk Tree.[1] Recently, we have found that the present fast technical and social changes call for a further development of these graphic tools. It has become increasingly necessary to consider highly adaptive socio-technical systems for which deterministic, causal models developed for technical installations become inadequate. Furthermore, due to the fast pace of change of technology and

1. Johnson, W. G. (1980): MORT Safety Assurance Systems. New York: Marcel Decker.

financial conditions, emphasis is increasingly on proactive risk management strategies replacing reactive methods based on analysis of accidents in the past.

The following sections present an outline of the phases of accident analyses together with a set of graphic representations, we have found useful to structure the analyses of hazardous work systems. These graphic formats have proven useful also to give an overview of the interactions in a socio-technical system shaping the landscape in which accidents may unfold themselves and, not the least, they have been very convenient as a vehicle in support of discussions during field work and system auditing.

3.2 Phases of Analysis

The phases of analysis to be discussed in the subsequent sections are:

- *Accident analysis.* A set of accident cases are selected that are representative for the industrial sector in question. For each of these accident scenarios the causal chains of events are then analyzed. From here an overview of the patterns of accidents related to a particular activity or system is generated by a cause-consequence analysis. The result is represented by a *cause-consequence-chart* (CCC).
- *Identification of actors.* For each accident scenario, the decision-makers, planners, and actors who have been involved in the preparation of accidental conditions are identified and represented in an *AcciMap*. This map then should identify the involved actors at all relevant levels of society shown in figure 2.1.
- *Generalization.* From the set of AcciMaps, a generalized map, a *generic AcciMap* is developed that can identify the organizations and groups that should be subject to a detailed *work* analysis.
- *Work analysis.* An *ActorMap* extracted from the generic AcciMap identifies the individual decision-making and planning bodies that should be subject to interviews and work-studies. From such interviews, an overlay to the ActorMap showing communication paths (an *InfoMap*) is convenient to point the attention of the analyst to weak links in the communication pattern within an organization.

3.2.1 *Accident Analysis*

The first phase of analysis will serve to identify the potential accident pattern related to an activity or technical installation together with the influence of the different protective measures. Based on a representative set of accident cases, a cause-consequence-chart is developed from a study of the causal structure of the system.

The Cause-Consequence-Chart (CCC) formalism[2] gives a detailed overview of the potential accident scenarios to consider for design of safety measures related to a particular activity or work system. CCCs have been widely used as a basis for predictive risk analysis, see figure 3.1. These charts are developed around a 'critical event' that represents the release of a particular hazard source. Several different causes may release a particular hazard source and are represented by a causal tree connected to the critical event. Depending on actions taken by people in the system or by automatic safety systems, several alternative routes may be taken by the accidental flow once the hazard source is released. Event trees following the critical event represent these routes and include 'decision switches' that represent such effect of protective actions.

A particular CCC represents a generalization that aggregates a set of accidental courses of events related to the release of a *particular hazard source* represented by the critical event. Examples are 'loss of containment of hazardous substance' or 'loss of control of accumulated energy.' When dealing with a global safety design within a work place or activity, a set of critical events will be chosen for the analysis. These critical events are chosen to structure the design of the protective measures in the most manageable way, e.g., by giving the minimal set of CCCs, or identifying the most consistent set of risk management strategies.

The concept of a hazard source and the related definition of a critical event are basic elements in a taxonomy of hazard sources, work system structure, and risk management strategies that will be described in chapter 4.

2. Nielsen, D. S. (1975): Use of Cause-Consequence Charts in Practical Systems Analysis. In: *Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of Systems Reliability and Safety Assessment*. Philadelphia: Society for Industrial and Applied Mathematics. pp. 849–80.

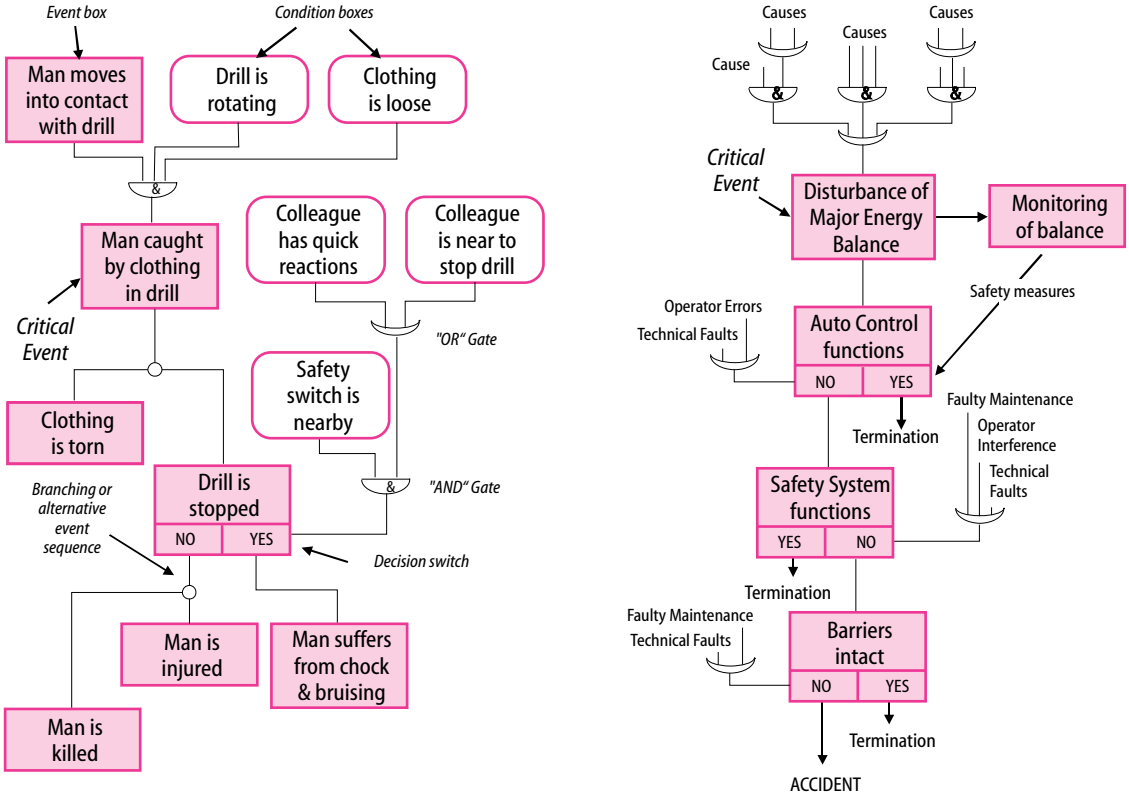


Figure 3.1. The figure shows two examples of cause consequence diagrams. The left-hand diagram illustrates the structure of an occupational accident in a rather unstructured environment. The right hand diagram represents the anatomy of accidents in an industrial process plant with multiple safety barriers.

In the CCC representation, the focus is still on events and conditions and on decisions directly influencing the causal flow of events. The analyses reflect the focus of most accident committee reports, that is, the *abnormal* and unusual events and acts. When the focus is design of improved system safety, not on identifying the guilty person, the problem is to identify those people in the system that *can make decisions* resulting in improved risk management, given the proper *normal* work conditions.

3.2.2 *Identification of Relevant Actors*

In our context, the problem with the cause-consequence-chart representation is that the landscape in which the flow will occur is unstable in a modern dynamic society. A condition which may not be too important considering long term stable technical systems, such as nuclear power plants, in contrast to more flexible domains, such as operation of Ro-Ro ferries. For such systems we have found useful a graphic notation explicitly representing the actors and forces shaping the landscape of potential accidental flow during their efforts to be cost-effective in their normal work.

Our analyses of accidents tend to show that the causal paths of potential accident scenarios often are prepared as the result of side effects of decisions made at different points in time, by different actors, who belong to different organizations at different levels of society. In most cases, the activities of these actors are functionally disconnected, only the accidents reveal a relational structure. Likewise, their decisions are usually sound from a local criterion and given the time pressure and short-term incentives shaping their behavior. In short, they are experts, doing their best to meet local conditions, and in the daily busy flow of activities, they are unaware of the potentially dangerous side effects.

The aim of an analysis then is to analyze the normal work conditions in the different organizations that may contribute to the creation of an accidental flow path to reveal the potential for a connected set of side effects. From here, the aim of risk management is to create a work support system that in some way makes decision-makers aware of the potentially dangerous network of side effects.

In short, wee need an analysis of decision making during normal work of work planners, managers, and legislators, and the influence of the stressors found in the modern dynamic society, see figure 2.1. Decision-makers at many levels are planning the landscape determining the flow of accidental events and their roles should be included in the analysis of accidents and the planning for proactive risk management.

The focus of this analysis is the control of the hazardous process at the bottom of the socio-technical system. That is, the focus of analysis is a vertical analysis across the levels, not a horizontal generalization within the individual levels as it is usually found within the various academic disciplines. In this situation, it appears that an extension of the Cause-Consequence-Chart representation to explicitly include the normal work decisions at the higher levels of figure 2.1 will be very useful for analysis of past accidents. It will serve to identify the decision-makers having a potential for improving safety, and to support communication with the various disciplines relevant for cross-disciplinary co-operation in research and design.

The "AcciMap" representation is proposed to serve these aims and is organized in the following way.

As is the case with the causal tree normally used to represent the findings from post-hoc accident analysis, the basic AcciMap is developed from analysis of one particular accident case, that is, it reflects one particular course of events. There are, however, several basic differences:

- The AcciMap is aimed at design of improved systems, not at allocation of responsibility. Therefore, the criterion for its development will not be a truthful representation of facts, but a representative identification of factors sensitive to improvement, that is, of all decision makers that could have influenced the flow by a decision different from the past practice.
- Even if the AcciMap serves to reflect the analysis of only one past accident, the "Decision/Action Box" symbol of the CCC in figure 3.1 is introduced, but simplified to only show the accidental side-effect of a decision that has served to configure the landscape of the accidental flow.
- In contrast to the conventional CCC, the analysis for development of an AcciMap should not only include events and acts in the direct dynamic flow of events. It should also serve to identify all decision-makers at the higher level in the socio-technical system of figure 2.1 that have influenced the conditions leading to accident through their normal work activities.

For clarity, the presentation of an AcciMap is structured according to the levels of figure 2.1. The layout and proposed symbols to be used are as shown in figure 3.2:

- At the bottom is a level representing the topography of the accident scene: the configuration and physical characteristics of the landscape, buildings, equipment, tools, vehicles, etc. found at the location and involved in the accident.
- At the next higher level is represented the accident processes, that is, the causal and functional relations of the dynamic flow, described in terms of the CCC convention. In the flow are included "Decision/Action" boxes connected to consequence boxes where the flow has been or could be changed by human (or automated) intervention.
- At the levels above this the "D/A" box symbol is used to represent all decision-makers that – through decisions in their normal work context have influenced the accidental flow at the bottom.

In this way, the AcciMap serves to identify relevant decision-makers and the normal work situation in which they influence and condition possible accidents. The focus is not the tradi-

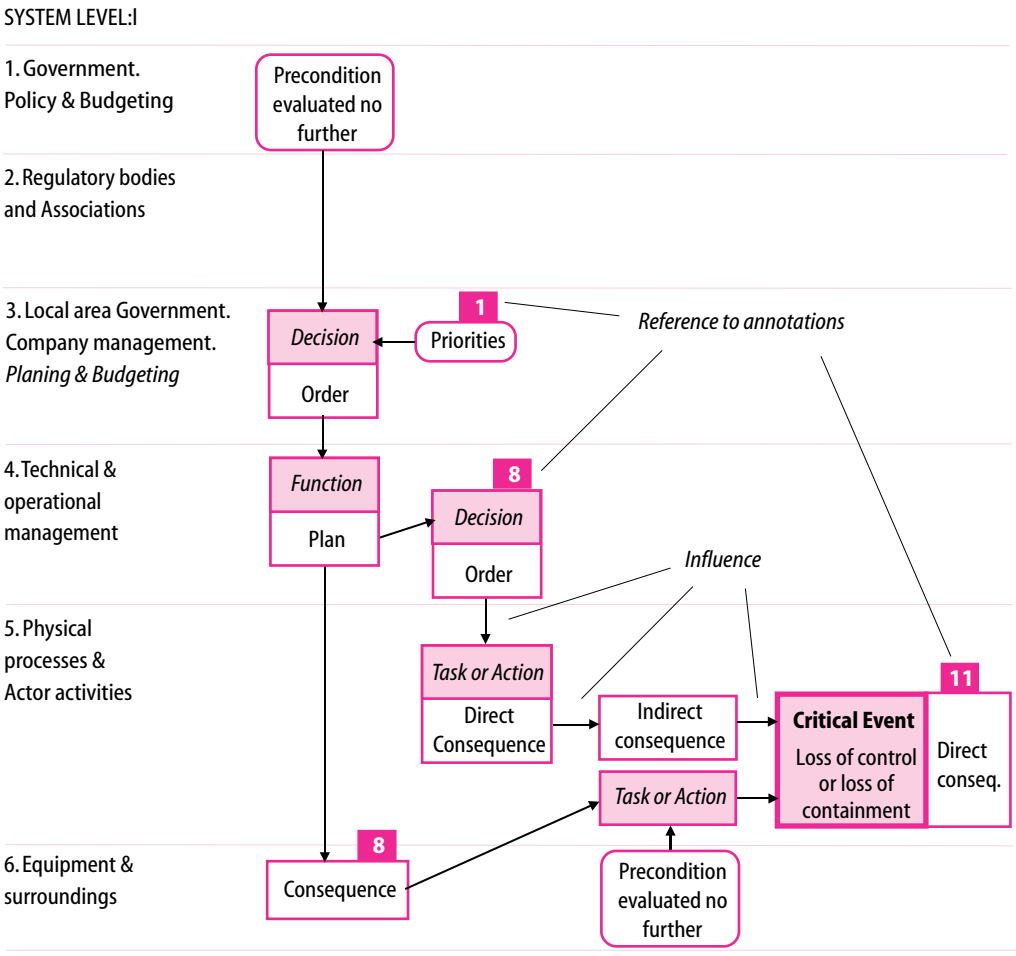


Figure 3.2. An approach to structure an "AcciMap" and a proposed legend of standardize symbols.

tional search for "management errors" and the like. Therefore, the AcciMap representing the conditioning system of one particular accident is well suited as a "conversation piece" to support discussion with the relevant decision-makers.

Figures 3.3 A and B illustrates the use of AcciMaps to reflect the results of a particular accident analysis, that is, a scenario involving transport of hazardous goods. The AcciMap shown is based on annotations from an official accident report. These annotations are numbered and enclosed in the case report found in the appendix to illustrate the format and to explain the indications in the boxes of the AcciMap.

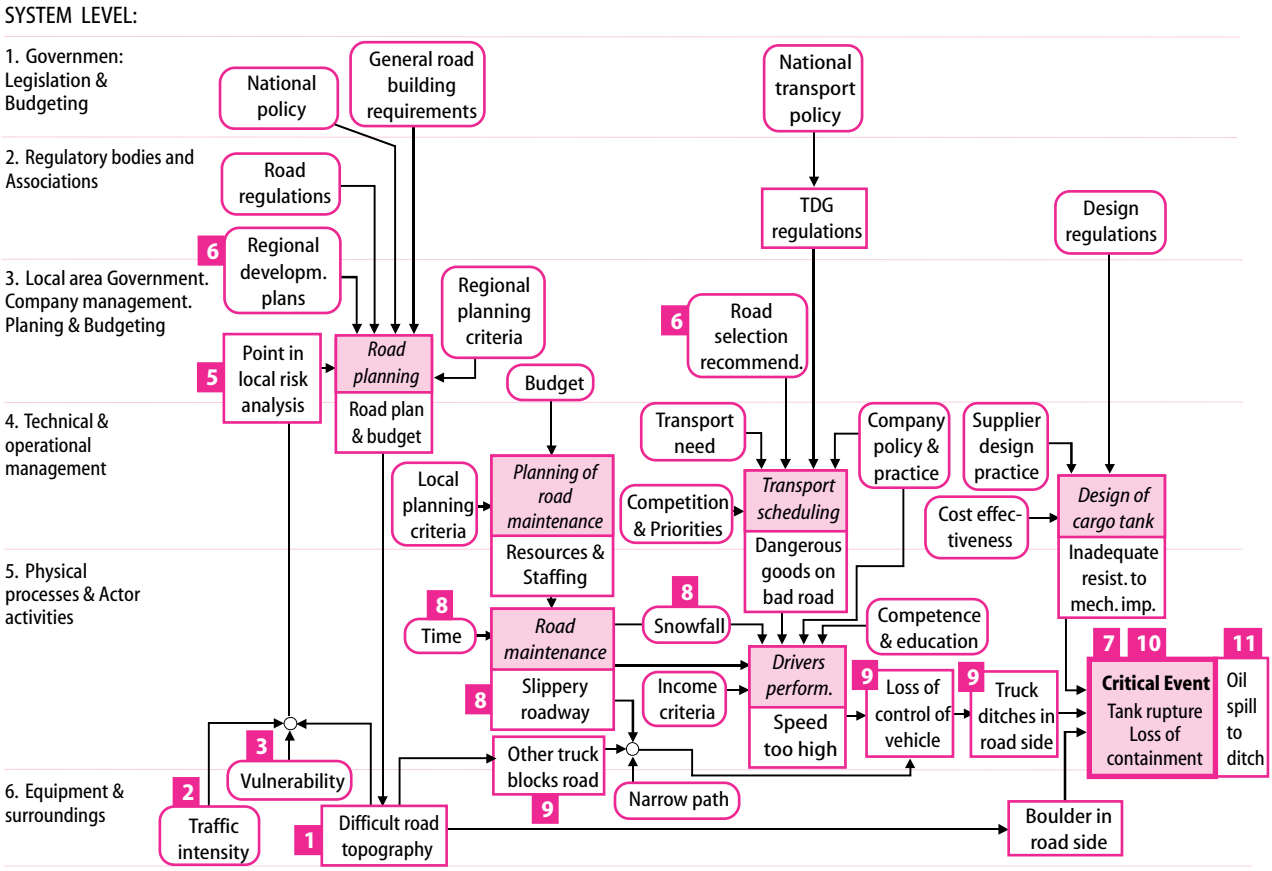


Figure 3.3A. An "AcciMap" showing the results of the analysis of a transport of dangerous gods accident involving oil-spill into a ditch that via a stream is connected to a municipal drinking water supply. The physical accident process prior to the critical event is represented at the levels 5 and 6. Also shown are decisions or activities important in conditioning the accident and performed at all levels of society together with related information sources. Numbers indicated refer to annotations based on the accident report (See Appendix A3 for annotations).

3.2.3 *Generalization*

The basic AcciMap represents the conditioning system and the flow of events from one particular accident. Suggestion of improvements by changes identified from this map therefore will very likely be ad hoc. A generalization is necessary based on a set of accident scenarios. The Generic AcciMap in figure 3.4 represents this generalization.

To complete the identification of relevant decision-makers, the causal flow represented at level 5 is based on the selection of a "critical event" defined as discussed for the CCC. The model should include all relevant, alternative flow paths following a release of the critical event and related to the prevention and mitigation strategies in place.

This representation at the causal level of the generic AcciMap should be based on a description *of the normal, causal flow of activities* within which the "critical event" is embedded. In that way it can form a basis for generalization across several accident scenarios and reflect the influence on the scenarios from *the normal work* context of decision-makers.

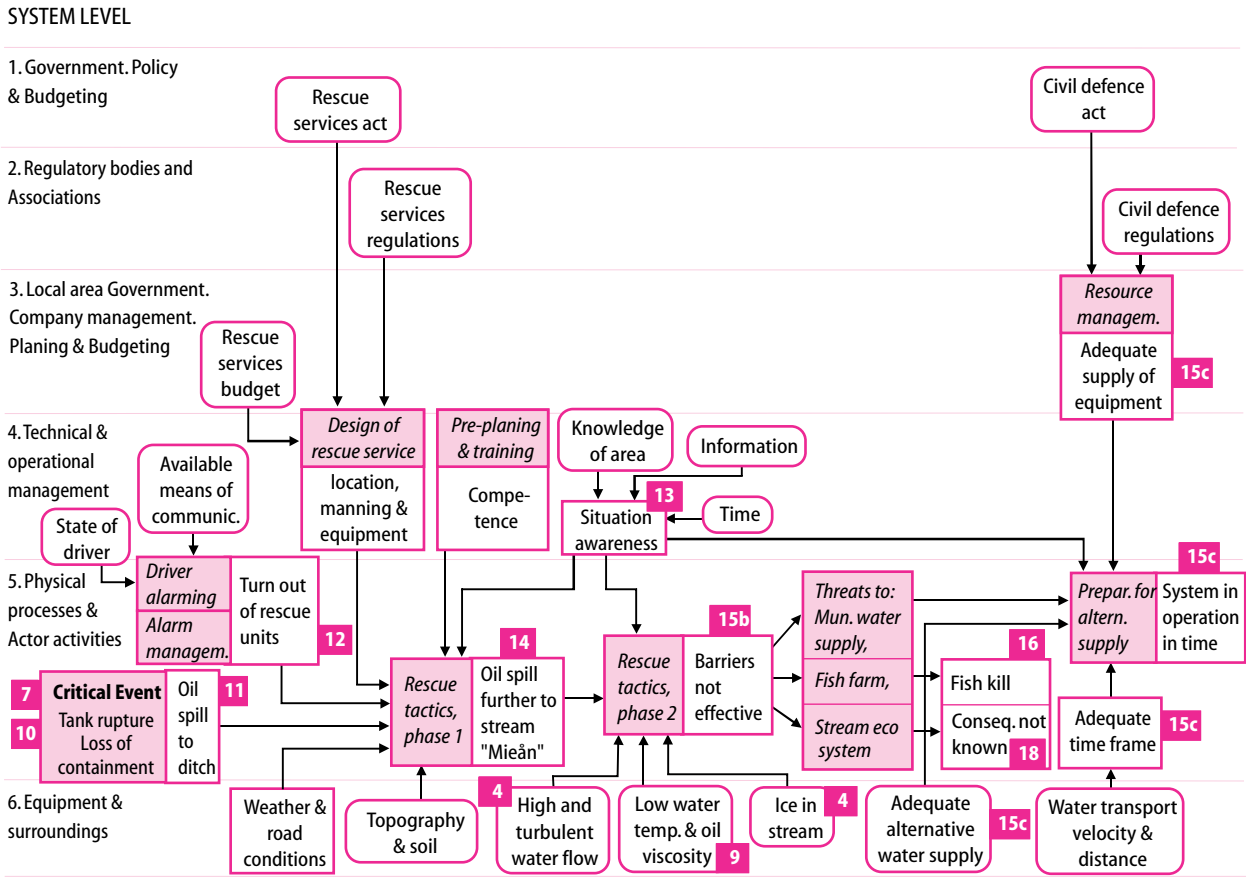


Figure 3.3B. The continuation of the "AcciMap" in figure 3.3 A describing the flew of events after the critical event. (See Appendix A3 for annotations).

For a work domain, such as "transport of dangerous goods" several different hazard sources typically must be considered for risk management; each being released and therefore several separate "Generic AcciMaps" must be included in a detailed study. For the transport case, the following critical events may be relevant: loss of containment, ignition of fire during storage, release of material during handling, etc.

3.3.4 *Preparation for Work Analysis*

The generic AcciMap gives an overview of the interaction among the different decision-makers potentially leading up to release of accidents. An ActorMap, as in figure 3.5, is an extract of the generic AcciMap showing the involved decision-makers. To support planning of the interviews and field studies of detailed work and communication analysis a more specific ActorMap like that in figure 3.6 is useful.

Such an ActorMap gives an overview of the decision-making bodies involved in the preparation of the 'landscape'

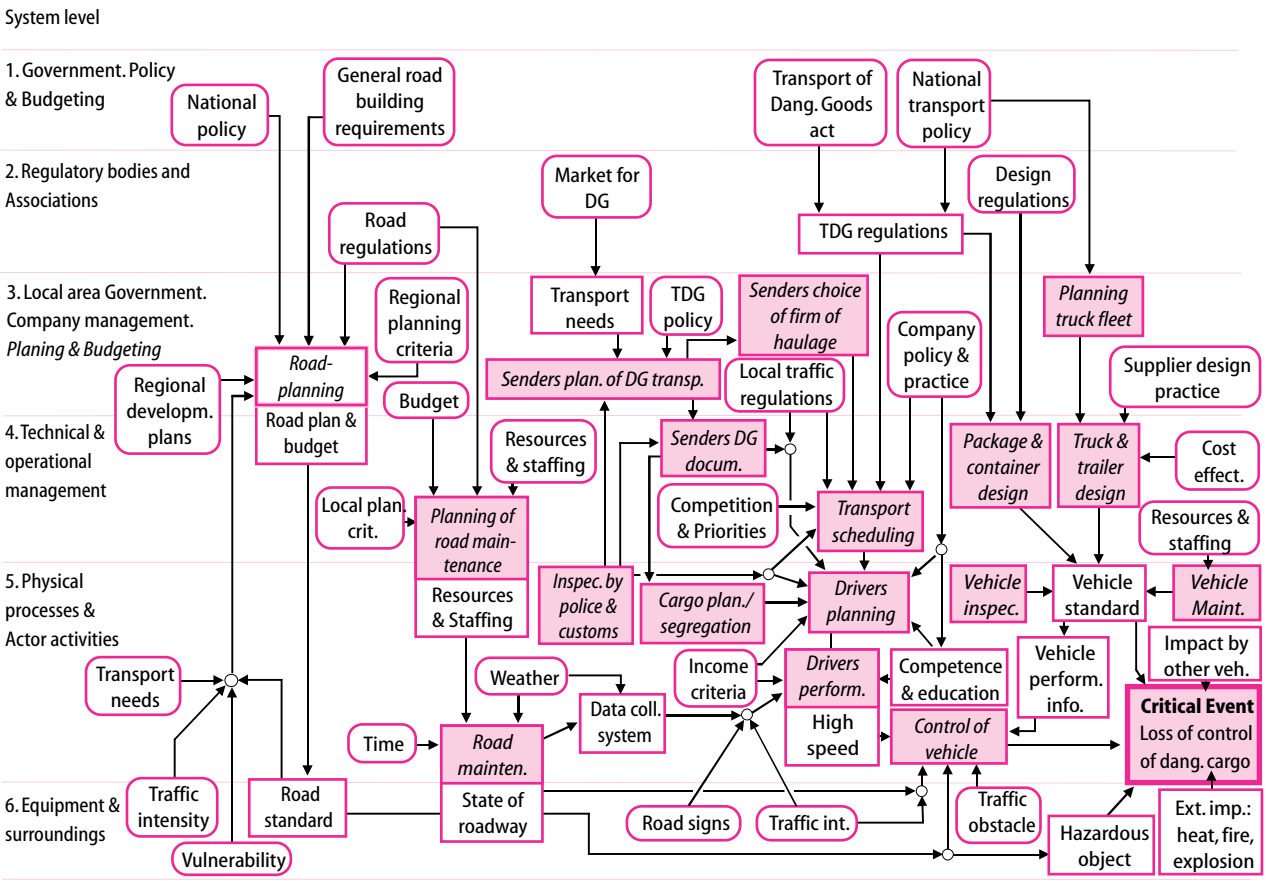


Figure 3.4. A Generic AcciMap regarding transport of dangerous goods.

through which an accidental flow of events may ultimately evolve. Based on this map, an InfoMap, as in figure 3,7, can be developed, indicating the structure of the information flow; the downward flow of objectives and values – the targets of control – and the upward flow of state information – the measurements of control. The use of such maps will be discussed in more detail in chapter 7 and illustrated in chapter 11.

In conclusion, we consider risk management as an adaptive, closed loop control function. The various actors and decision-makers then have many roles. One is to formulate the goal within their particular sphere of control and another is to identify the actual state of affairs with reference to this goal. A third role is to act to bring the state of affairs in correspondence with the goal, *while making sure that performance is optimal with respect to process criteria, such as cost effectiveness, within the boundaries of acceptable performance, as defined by the constraints given by work and safety regulations.* This analysis will be discussed after a presentation of the control requirements of different types of hazard sources and productive system structures.

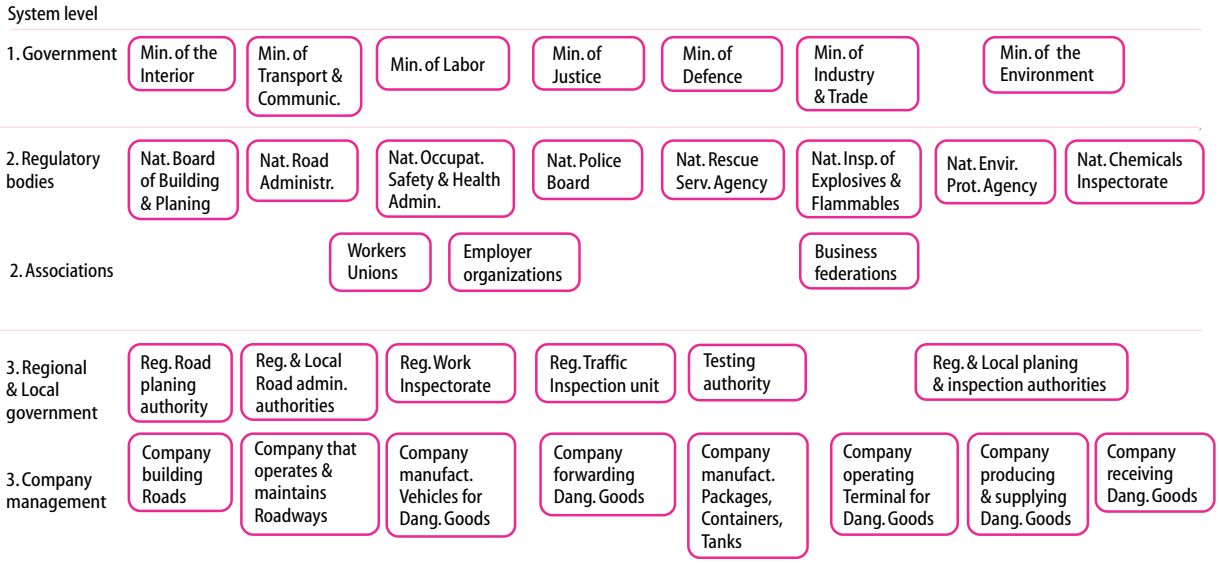


Figure 3.5. A Generic ActorMap giving an overview of the decision-making bodies involved in the system shaping the conditions for road transport of dangerous goods and thus also for the accidents that can happen in that system.

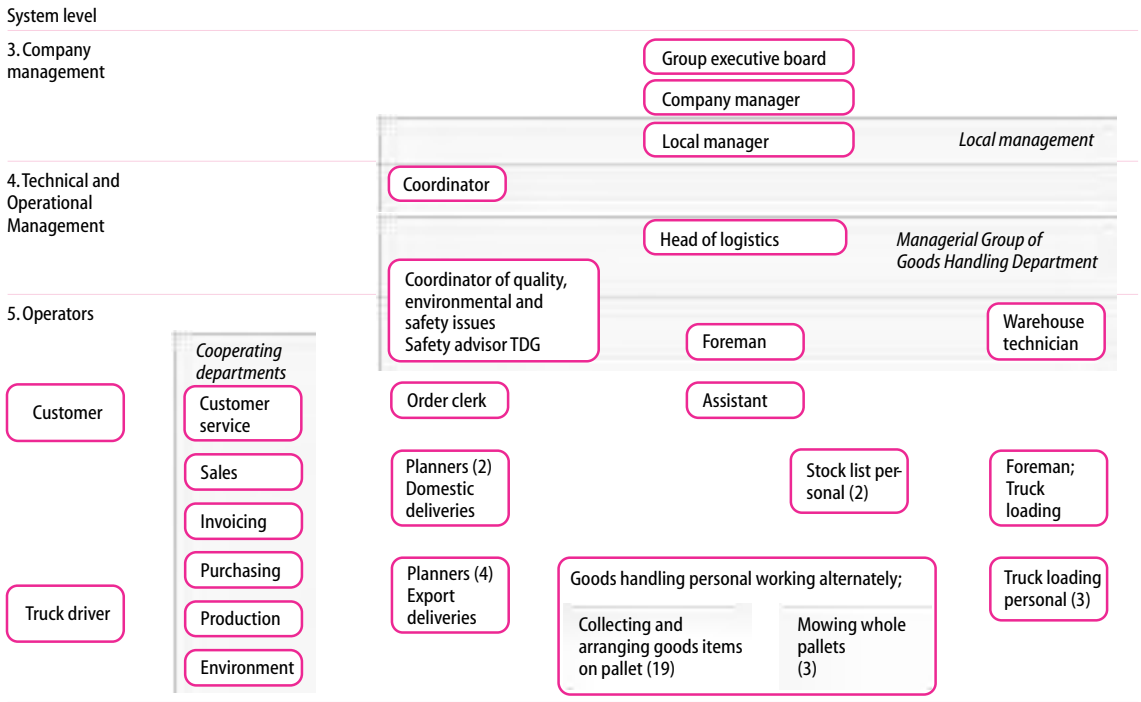


Figure 3.6. Shows an ActorMap used for a detailed analysis of the activities in a distribution warehouse.

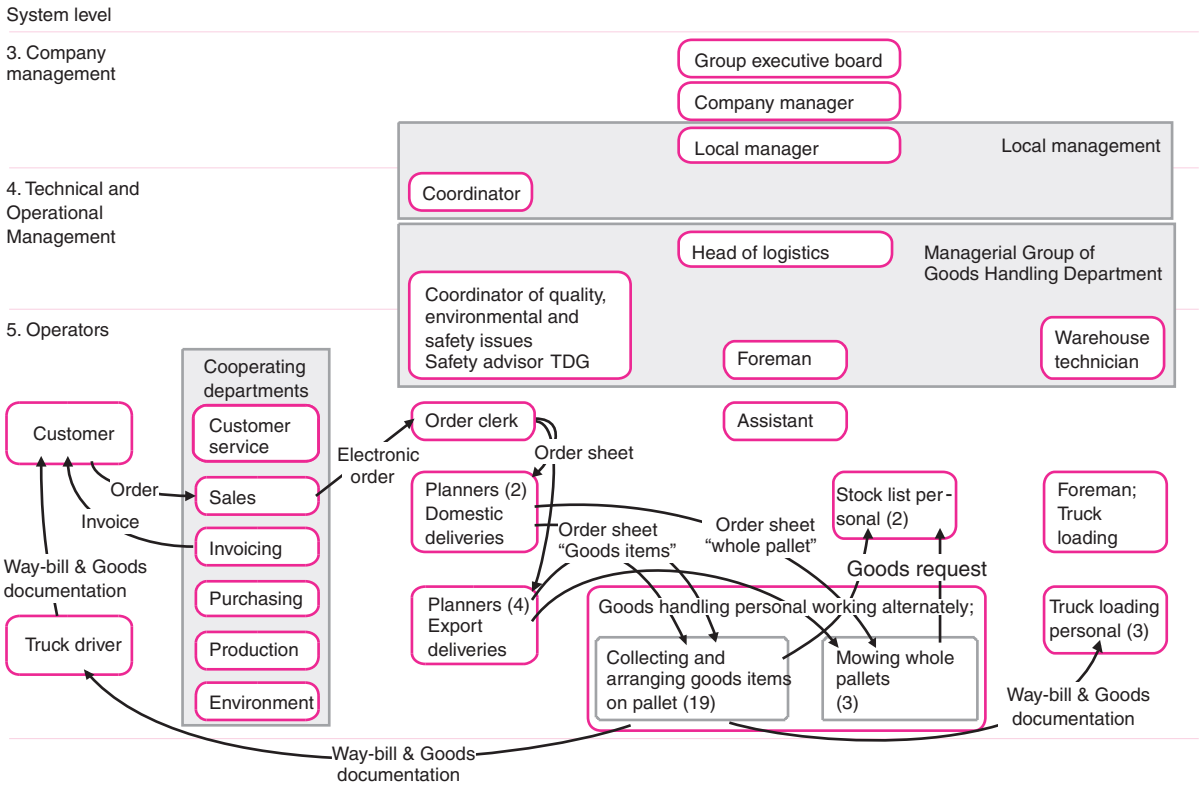


Figure 3.7 shows an InfoMap used for analysis of the communication among the actors identified in figure 3.6.

4. Hazard Categories, System Types, and Risk Management

Different work systems based on different technologies and activities present quite different hazards so different modes of safety control and risk management have evolved. In a mature society, an inverse relationship is found between the accepted frequency and the magnitude of accidents, as shown in the figure. 4.1. Different risk management strategies have evolved through time for different categories of hazards, see figure 4.2.

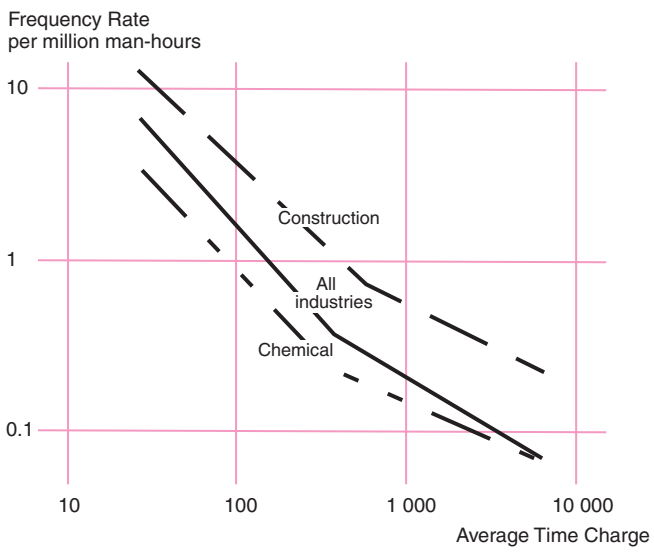


Figure 4.1. In a mature society, there appears to be an inverse relationship between the accepted accident frequency and magnitude.[1]

4.1 Accident Categories

Figure 4.2 shows the following accident categories together with the related risk management strategies:

1. *Occupational safety* focused on frequent, but small-scale accidents: The hazard is related to a very large number of work processes and the level of safety is normally measured directly by the number of LTIs (lost-time-injuries) and casualties. Consequently, the average level of safety across activities is *controlled empirically from epidemiological studies of past accidents*.
2. Protection against *medium size*, *infrequent accidents*: In this category, safer systems evolve from *design improvements in response to analyses of the individual*, *latest major accident*. Examples are accidents such as hotel fires, aircraft accidents, train collisions, etc. Safety control is focused on the control of particular accident-creating processes and, normally, several lines of defenses against accidents have been established by an evolutionary, incremental effort toward improved safety. In this case, risk management is focused on the removal of causes of particular accidents.
3. Protection against *rare*, *large scale accidents*: For industrial installations that have a potential for large scale accidents, the acceptable frequency of accidents will be so low, that design cannot be based on empirical evidence from accidents. This is particularly so, when the pace of technological innovation becomes fast, as is the case in e.g., the chemical industry where the time span from conception of a new product or process to large-scale production becomes very short. In that case, an incremental evolution of low risk systems guided by past

1. Adopted from Johnson, W. G. (1980): MORT Safety Assurance Systems. New York: Marcel Decker.

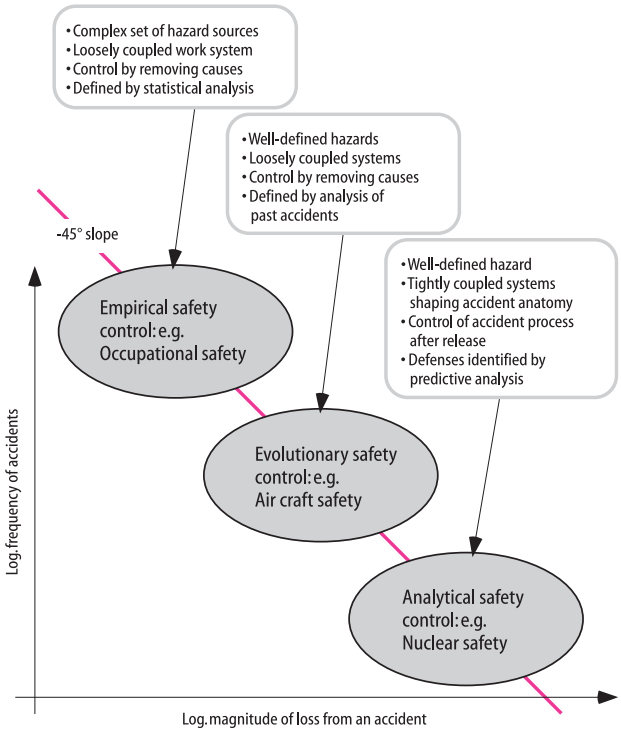


Figure 4.2. The figure illustrates the basic features of different hazard categories and the related hazard sources that have led to different risk management strategies.

accident scenarios is no longer acceptable. The risk from new industrial installations must then be *predicted from models of the processes applied and the hazards involved*. For this purpose, probabilistic risk analysis (PRA) has been developed and system design is then based on an estimation of the probability of a full-scale accident considering the likelihood of simultaneous violations of all the designed defenses. Given the level of acceptable risk, and the reliability (including maintenance) of the individual defenses (which can be determined empirically from operational data), the necessary number of causally independent defenses can be estimated. The assumption then is that the probability of violation of the defenses individually can and will be verified empirically during operation even if the probability of a stochastic coincidence has to be extremely low. In this case, the reference for monitoring the performance of the staff during work is *derived from the system design assumptions used for predictive risk analysis, not from empirical evidence from past errors and accidents*.

This review illustrates different categories of hazard sources and the related different risk management strategies that have evolved empirically in the past. It is, however, necessary to reconsider this empirical categorization in the present fast pace of change of the conditions of risk management.

From a system perspective, risk management is considered a control problem. Since the various hazardous processes have very different control requirements, an effective risk management strategy must be planned from analyses of these control requirements and the structure of the operational system in which the hazardous process is embedded. In consequence, we need a systematic taxonomy describing the relationship between hazard sources, system configurations and risk management strategies.

The empirical approach to risk management has been very effective in the past for prevention of small and medium scale accidents. Recently, however, the quest for a *proactive*, 'no-accident-is-tolerable' strategy is being voiced[2] and it appears that to further improve the general level of industrial safety in this direction, more focused, analytical risk management strategies will be necessary. Such strategies should be directed toward the control requirement posed by the various categories of hazard sources found in a modern society. A system-oriented classification scheme will be useful because different combinations of hazard sources and system structures require quite different risk management strategies. To plan an effective, operational risk management approach, an explicit description of this relationship is necessary.

2. Visser, J. P. (1991): Development of Safety management in Shell Exploration and Production. Contribution to '91 Bad Homburg Workshop on Risk Management. Published in: Brehmer, B. and Reason, J. T. (Eds.): In Search of Safety. Hove, UK: Lawrence Earlbaum.

4.2 The Structure of a Hazard Taxonomy

This classification problem raises the question of the formulation of a useful conceptual framework (taxonomy) for description of hazard sources and related control requirements. Taxonomies can be developed in many ways, and the approach taken depends entirely on its purpose. Taxonomies in natural sciences, such as Linné's classical botanical taxonomy depend on consistent definitions of the attributes of the class members. The purpose of classification is to give known objects an unambiguous name and to place new objects in one and only one category. Therefore, classification schemes must be hierarchical and exclusive and in this case, a discussion of the correctness of the taxonomy will be relevant.

In contrast, the taxonomy considered here will not be a generic, hierarchical classification system, but a multi-dimensional framework to describe the various combinations of hazard sources and the related risk management strategies.

The structure of the taxonomy and level of detail to apply should be chosen so as to distinguish cases according to the relevant safety control strategy. That is, it should be possible to characterize a particular work system according to the 'control requirement' of the underlying hazard source in order to focus analysis on the information flow required within the controlling socio-technical system for adequate risk management. In other words, the taxonomy should have a structure and set of categories that can serve to specify the information content required for proactive safety control and thus to define the 'vertical' relationships within the socio-technical system involved in risk management. Generalization across cases at the various levels of the system of figure 2.1 is thus not acceptable. Analysis of each case will render a vertical slice through that system at a particular point in time, and generalization should be made with reference to the structure of that slice.

The taxonomy will have to evolve iteratively during application experiments and the dimensions and classes described in the next chapter should only considered to be illustrative of the basic philosophy and structure. One basic issue that must be explicitly considered is the nature of causal explanations that fundamentally makes it impossible to define the attributes of the classes in the taxonomy exhaustively and objectively. In consequence, categories will have to be defined by 'prototypical' scenarios and examples that are understood and accepted by professionals familiar with the context of analysis. We will return to this issue, but we first have to review the various applications of a taxonomy and their different requirements to analysis.

4.3 The Applications of a Taxonomy

To determine the structure and contents of such a pragmatic taxonomy, we have to consider its application. For proactive risk management, the taxonomy should serve the support of the following activities:

1. Analysis of past accidents and the subsequent generalization to identify weak links in management of hazardous work processes.
2. Design of work systems including safety barriers to prevent release of potential hazard sources based on a predictive analysis of work processes and their hazard sources.
3. Design of risk management systems, that is, decision support systems for management of the *normal work performance* within the design envelope defined in 2);
4. Design of an auditing system that can serve the evaluation of current work practice with respect to the objectives and control structures defined in 3).

4.3.1 Accident Analysis

The kind of accidents to be considered in the present context includes the propagation of changes following a loss of control of a hazardous physical process due to a change in the system which normally isolates a hazardous production process from disturbances. Each accident has its peculiar characteristics, but to conclude from an analysis it is necessary to generalize, that is, to characterize the particular case by a sequence of events belonging to predefined categories. For this purpose, the taxonomy must serve creation of a *causal representation* of the accident anatomy and the system structure that can support *proactive design of* a safe work system. In other words, the taxonomy is based on a decomposition of the accidental behavior of the system into a sequence of typical events, decisions, and acts.

4.3.2 Design of Safe Work System

Proactive risk management requires an analysis of the hazard sources found in the system, a prediction of the changes of their isolating containment that will release them, and introduction of protective devices that can prevent their release or

block the accidental course of events. This design process involves the selection and aggregation of standard system components and processes, typical for the particular industrial domain. Also this process then depends on causal models based on decomposition.

4.3.3 Design of Risk Management System

The analysis under 4.3.2. defines the condition under which the hazardous process can be safely contained, that is, it defines the *control requirements* of the hazardous work process. Design of a proactive risk management strategy then involves the design of the structure and content of the information flow vertically in the entire socio-technical system of figure 2.1 serving the safety control. This control design requires a shift in modeling concepts from structural decomposition to functional abstraction, from causally connected events to the functional relationships to be implemented in a communication and information system serving the overall system integration.

4.3.4 Design of Auditing Systems

Well-structured auditing systems serve several purposes:

- Current evaluation of work practice to prevent unacceptable adaptation to the operational cost-effectiveness pressure;
- Independent evaluation by third parties to evaluate operations with reference to the accepted design criteria;
- Independent post event analysis of incidents and accidents.

The framework for evaluation must therefore integrate the causal and the relational representations underlying all the analyses described above. Causal analysis based on structural decomposition is necessary for identification of functional elements and evaluation of their functional characteristics and limits of capability. Relational analysis based on functional abstraction is necessary for an evaluation of the consistency of the overall safety control function.

The conclusion from this discussion is that the taxonomy must be based on a causal representation of the relevant hazard sources of an activity domain, the anatomy of the system that shapes the potential accidents, and the related safety control requirements. From here, the requirements for the safety management information flow should be defined in terms of a representation of functional relationships.

4.4 Characteristics of Causal and Relational Representations

Since the development of proactive risk management strategies and tools for safety auditing involves the application of causal as well as relational modeling concepts and considering that causal models are often found to be 'pre-scientific', a review of the characteristics of the two approaches may be useful.

Systematic analyses depend on study of phenomena that are separated from the complex 'real world'. This separation can be done in two ways. One is to use separation by *structural decomposition* of systems into parts and behavior into regular connections of events, decisions, acts and errors. Another is to use separation by *functional abstraction* into functional relationships among variables. The two approaches have very different characteristics and are used for different purposes.

4.4.1 Structural Decomposition

The behavior of a work system is actually a continuous flow and *causal explanations* of this flow can only be generated by decomposition of the system into objects and of its behavior into sequences of events and acts that are regular through time. Such events represent changes of the state of objects and will be classified and labeled in terms of recurring categories. This decomposition and labeling will only be continued down to a level of detail that creates categories of elements that *are familiar to the analyst in the given context*. A description of the context is therefore necessary to qualify a causal explanation and categorization. Another problematic aspect of causal explanations is that it is always possible to suggest counter examples, just by assuming a minor change of the context. A causal explanation is only valid to an audience, willing to generate a context that makes the explanation plausible, and the message then actually lies in this context. One basic consequence of this nature of causal explanations is that they cannot be judged true or false, only more or less plausible.

In other words, the elements of causal models, for instance the concept of an 'event', are elusive: the more accurate the definition of an event, the less is the probability that it is ever repeated. Completeness removes regularity.[3] The solution is, however, not to give up causal explanations as being unscien-

3. For a detailed discussion, see Rasmussen, J. (1990): Human Error and the Problem of Causality in Analysis of Accidents. *Phil. Trans. R. Soc. Lond.* B 327, 449–462.

tific, but to realized that regularity in terms of causal relations is found between types of events, not between particular, individually defined events.

The types are categories defined by reference to typical examples, prototypes, which are defined by the context in which the are used. This context will usually be defined by reference to a 'cover story' or a verbal label indicating the domain in question.

Causal representations are very effective in several respects. They are analog representations in the sense that their elements are one-to-one mappings of objects and events in the real world. Therefore they are easily up-dated to reflect changes in the system to be represented, for instance the effects of changes leading to accidents. Furthermore, their prototypical representation of parts is very effective for mental experiments because their interpretation takes shape according to the changing context during exploration and design. As Alexander[4] noted; design involves "matching an object that does not yet exist to a context which cannot be completely specified" and the analogue and prototypical nature of causal representations therefore makes them well suited for design.

One major difficulty in the use of linear causal reasoning is that it is unreliable for analyzing the behavior of systems including closed-loop, feedback functions. In that case, linear causal reasoning becomes circular.

4.4.2 *Functional Abstraction*

Relational representations depend on *functional abstraction and separation* of selected relational structures that connect quantitative variables. They represent 'practically isolated relationships' which are valid for a variety of systems, and they have long been considered the only acceptable scientific representation of phenomena.[5] The *internal* consistency can be proved mathematically, their validity in the world can be tested (falsified) experimentally in a variety of experimental configurations with controlled conditions. This type of model does not necessarily represent the actual, in-the-world behavior of the phenomena of interest, but is effective for understanding basic mechanisms and to define limits of performance and conditions for optimal function. Relationships *determine* variables, no causal direction is found, that is, causality is irrelevant.

Relational models based on functional abstraction are useful for representation of system including closed loop functional relationships and their quantitative representation of physical variables is very useful for optimization of productive processes during design.

Relational models also present their characteristic problems. No simple mapping of 'real world' objects is found. The objects of the actual system are only present in terms of a set of parameters distributed across equations. It is therefore relatively difficult to modify the model in response to changes in the physical world. In particular when studying phenomena connected to the break-down of the 'practical isolation' such as the propagation of the effect of changes, errors, faults and accidents it is generally preferred to apply causal modeling techniques.

4.4.3 *Illustrative Examples*

A couple of examples of the use of decomposition versus abstraction may be useful for clarification. A representation based on decomposition into parts and events is effective for conceptualization of a new system and for instructing novices, but will be ineffective for analysis of the actual behavior of system including closed loop relations from automatic controllers or adaptive human actors.

A classic example is James Watt's design of the steam engine that he conceived as being a backward running mine drain pump and created by rearranging its components. He added a flying ball regulator that was well known for control of windmills.[6] This system turned out to be occasionally unstable, a feature that was first understood from the analysis by James Clark Maxwell[7] who introduced an abstract mathematical representation in terms of a set of differential equations and thus actually invented control theory. The efforts to optimize the design of the steam engine by use of quantitative relational models open the field of thermo dynamics.

As a more day-to-day example consider the instruction of a novice car driver. When a novice is driving a car, the concep-

4. Alexander, C. (1964). *Notes on the Synthesis of Form*. Cambridge, MA: Harvard University Press.
5. Russell, B. (1913): "On the Notion of Cause". *Proc. Aristotelean Society*, Vol. 13, pp. 1–25.
6. Mayr, O. (1970): *The Origin of Feedback Control*. Cambridge, Ma.: MITT Press
7. Maxwell, J. C. (1868): On Governors. *Proc. Royal Soc. London*, 16; 1868, pp. 270–283.

tion of the car is based on an aggregation of system components. A driver's instruction identifies the controls of the car and explains the use of instrument readings, that is, when to shift gears, what distance to maintain to the car ahead depending on the speed, and how to use the steering wheel. In this way, the function of the car is controlled by discrete rules related to separate observations and navigation depend on continuous observation of the heading error and correction by steering wheel movements. This aggregation of car characteristics and instructed input-output behavior of components makes it *possible* to drive; it initiates the novice by synchronizing him/her to the car functions.

However, when driving skill evolves, the picture changes radically. Behavior changes from a sequence of separate acts to a complex, continuous behavioral pattern. Variables are no longer observed individually; complex patterns of movements are synchronized with situational patterns; and navigation depends on the perception of a 'field of safe driving'.[8] The driver perceives the environment in terms of his driving goals. At this stage, the behavior of the system cannot be decomposed according to the structural elements. A description must be based on abstraction into functional relationships.

This example indicates that even if the design of protective systems for a work system involving human actors can be based on causal analysis of potential accident scenarios, the evaluation of the actual behavior of the system must be based on relational models based on functional abstraction.

8. Gibson, J. J. and Crooks, L. E. (1938): A Theoretical Field-Analysis of Automobile Driving. The American Journal of Psychology, Vol. LI, July, 1938, No. 3. Pp 453–471.

5. The Taxonomy Framework

A framework for causal representation of the anatomy of accident scenarios is an important ingredient of a taxonomy. To serve the design of safe work processes including protective barriers, this framework should be based on a schematic representation of the physical process involved in the accident, see figure 5.1. This figure shows a Cause-Consequence-Chart lumped into those more global events preceding and following a particular 'critical event' (release of a particular hazard source) that can be used as a target for safety control actions. As it is explained above, it is necessary to define the context within which a causal chain is embedded to give meaning to a causal description. A dynamic, causal context will normally be communicated in terms of a 'cover-story', that is, a short verbal description representing a 'prototypical' scenario. Such a typical accident scenario should define the accident category for a professional analyst, with reference to an effective risk management strategy.

A structure and a set of preliminary categories for an analytical tool emerge from this:

a. The *targets* of hazards. This dimension represents the objectives of the safety control strategy: Who or what is being protected from injury or damage.
b. The physics of the *hazard source*. This dimension serves to define the source of hazard that may be accidentally released and define the process that is in focus of the safety control efforts.
c. The safety *control strategy*. Depending on the nature of the system in which the hazard source is found, the safety control efforts can be directed toward one or more of the phases of the accidental course of events shown in figure 5.1.
d. Finally, the context of the analyzed accident scenario should be identified by a '*cover story*' that defines the context to a professional audience.

Tentatively, these four dimensions seem to span a universe that maps on to established practices and regulations in a handy way. However, being pragmatic, the dimensions are not orthogonal in the sense that the categories are independent and mutually exclusive.

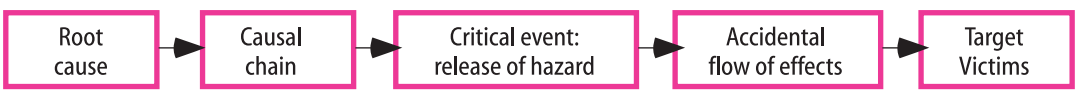


Figure 5.1 shows the anatomy of an accident, A critical event releases the hazard source. A causal tree connects possible 'root causes' to the potentially critical event. Release of this event activates a chain of effects.

5.1. a. Target of Hazard

The target of hazard is an important dimension because it represents the ultimate objective of the safety control function. Therefore also the present regulations and political discussions typically are structured according to these categories. Finally, the dimension reflects the natural priority judgements underlying overall risk management of a particular organization.

a.1. Individual Actor

The victim of released hazards in this category is the individual actor, as is normally the case in occupational accidents. Protective measures are directed toward the individual and often have to be planned on occasion for particular work settings because the physics of the work situation of an individual depends on the details of a local work place.

a.2. Staff

This category includes accidents by which several people within the organization are endangered, as is the case by fires, explosions, release of toxic material. While the previous class is related to smaller scale occupational accident kind of scenarios, the present category reflects medium scale scenarios calling for more global protective measures.

a.3. Environment

Damage to environment, explosions, pollution, etc. is a topic in focus of the present debate, and regulations are developing rapidly.

a.4. Harm to General Public

This category includes accident scenarios in which the objective of safety control is to protect the general public from injuries and fatalities due to major accidents, fires, or release of hazardous substances. Also this aspect is in public focus following the recent industrial, shipping, and airline accidents. The control problems are very much influenced by a fast pace of change of technology, extensive deregulation, and aggressive competition.

a.5. Loss of Investment

Loss of investment must be considered for a realistic safety management strategy because protective actions imply loss of production. Formulation of a safety strategy therefore will be a trade-off between degree of protection found necessary and the loss connected to a too conservative protection.

5.1 b. Physics of Hazard Source

Protective measures depend on the physics of the hazard source and, consequently, influence from the natural sciences on taxonomies of hazards has been seen in the past. An early attempt to define a system-oriented taxonomy of hazard[1] was based on an exclusive classification of forms of energy that could harm people. This approach was not, however, very influential. Forcing all hazards, e.g., in occupational safety work, into energy classes turned out to be somewhat artificial (e.g., in what energy class belongs cutting oneself in the hand? And referring poisoning to the class of 'chemical energy' solves no problems). Here, a more pragmatic classification of sources is suggested.

The categories of hazard sources to include in the scheme are those physical phenomena that may lead to damage if not adequately controlled, that is, are related to a well defined 'critical event' defining a family of accident scenarios. As an example: 'kinetic energy' is included as a separate class, because risk management strategies will bee directed toward efforts to control this energy and its possible release paths, whereas 'potential energy' is not. Potential energy is hazardous only when transformed into kinetic energy. In general, measures will not be directed toward control of potential energy. Similarly, the class of toxic material includes all substances that are harmful when released, depending on the magnitude of release and the particular acceptable limits of exposure, that is, toxic and corrosive chemicals, radioactive substances, etc.

Pro-active planning of risk management strategies depends on information about the physics of hazard sources and the related safety control requirements. Considering the fast pace of technological change, communication of basic information on these matters from the primary conceptual designers to the system constructors and further on to the users is a crucial question. During stable periods, established standards and practices and the competence of professional people reduce the needs for communication, see section 7.5. Recent accidents (e.g., Chernobyl and Estonia) demonstrate that careful consideration of the communication of basics about hazard sources is urgently needed.

Concerning the categories B.1 to B.3, identification of the relevant hazard sources, the relevant physical properties and

1. Johnson, W. G. (1980): MORT Safety Assurance Systems. New York: Marcel Decker.

related control requirements is typically an engineering question and extensive methods for analysis and experimentation are developed for evaluation during system design. The basic question is to find adequate ways to select and formulate the information to communicate down stream to builders and users.

b.1. Energy Accumulations

Hazards in the form of energy accumulations typically can be monitored by measurements of process variables, such as speed, temperature, or pressure. When detection of approaching loss of control can be inferred from unintended changes of such process variables and when time constants are not too short, safety actions can be introduced (control mode C.3).

- *High temperature-pressure liquids.* Energy accumulated e.g., in water/steam power plants. Loss of control of an energy balance or pipe breaks can result in steam explosions.
- *Chemical processes, fires, exothermic processes.* Accumulations of inflammable material with presence of oxidizer can release energy by combustion or explosion.
- *Kinetic energy.* Examples are release or conversion kinetic energy by loss of control of fast moving objects, such as e.g., trains, cars, air craft; fall from high altitude.

b.2. Accumulation of Toxic Substances

In this category, hazards are released by the critical event 'loss of containment' of toxic material, leading to release of toxic fumes, leak of chemicals into drinking water reservoir, etc.

Loss of containment can be caused gradually by corrosion or abruptly by impact from missiles or collision with vehicles.

b.3. Structural Integrity and Stability

Complex structures may be only conditionally stable, e.g., the vertical stability of ships, towers, and bridges. Detection of approaching hazard release may be difficult, even if some potential for detection is found in analysis and monitoring the amplitude, damping ration, and frequency of oscillation in response to disturbances (wind surges, sea waves).

b.4. Others, Mixed

Hazards in this category include damage from interaction with sharp edges, rotating machinery, wild animals, bad weather, etc. This mixed category is particularly relevant for minor hazards in unstructured work places. Traditionally, information for control of hazard sources has been derived from epidemiological analysis of accident reports by regulators and communicated to users by means of standards and guidelines.

Pro-active work safety during periods of fast change, however, necessitates a risk management strategy based on a predictive hazard and risk analysis. For categories B1–B3 this is often possible to apply during work system design because the hazard sources are rather well defined and bounded. For a mixed hazard category such as for instance found with occupational safety on a construction site, predictive analysis can only be done on site and occasion by the involved actors. For this, work planning through systematic 'tool box meetings' at work start has been developed in Japan.[2] This requires communication of the basic physics of hazard sources directly to the involved staff.

5.1 c. Means for Safety Control

The ends and means of an effective control of a hazard source depend on the physics of hazard source and the nature of the system in which the hazardous process is confined both of which are shaping the course of accidental events. As discussed in section 3, the hazard scenarios relevant for a work place can be represented by a set of cause-consequence-charts. A cause-consequence chart is developed from a 'critical event' representing the release of a hazard, preceded by a tree of potential causes of release and followed by a tree of potential paths of consequences. Safety control then depends on means to break or divert the flow of accidental events which can be done in a number of different ways depending on the physics of the hazard source and the confinement of the related process, see figure 5.2 and 5.3.

Figure 5.2 illustrates that one industrial installation involves several different hazard sources that may be contained within differently structured systems. In a petrochemical plant, for instance, the system to consider for release of the hazard related to loss of containment depends on circumstances such as the location and size of a leak in a complex set of pipes and

2. Identifying Occupational Safety Hazards: A Compilation of Promotional Methods for Training in Prediction of Potential Hazards, with Illustrated Situation Sheets. Edited by: The Committee for Hazard Protection Training. Compiled by Japan Industrial Safety and Health Association.

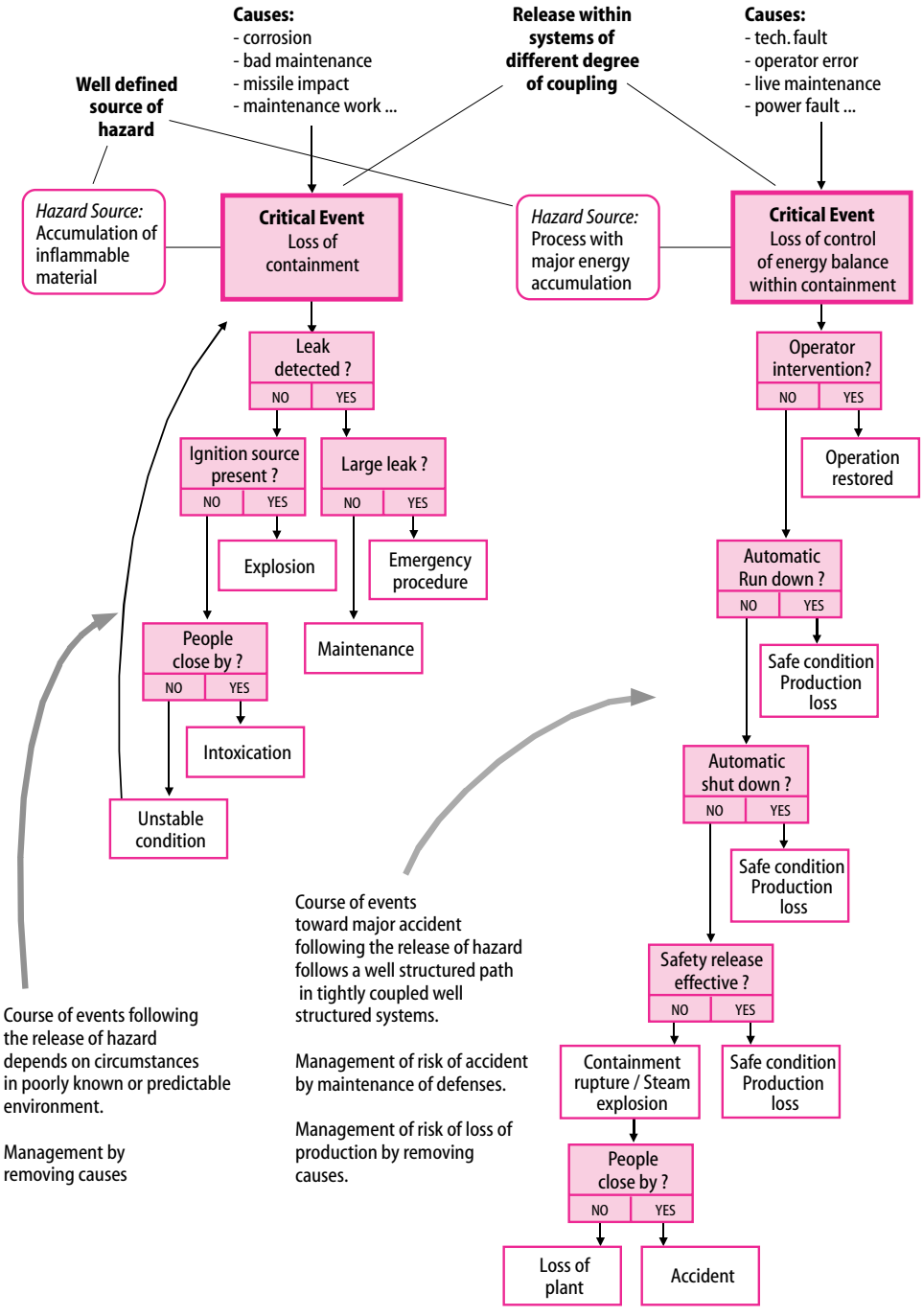


Figure 5.2 shows the anatomy of two accident scenarios within a petrochemical installation belonging to different categories of hazard source, system structure, and management strategies.

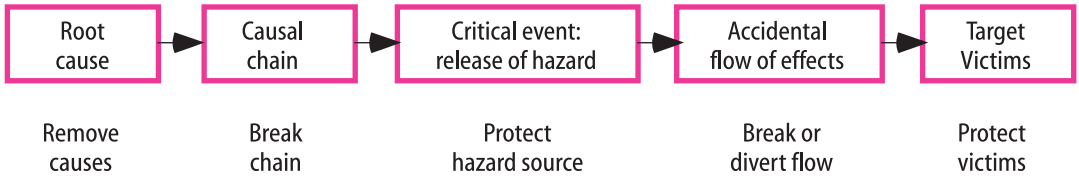


Figure 5.3 shows the anatomy of an accident from figure 5.1 and illustrates how an accidental chain of events can be interrupted by several different protective actions. The actual choice depends on the nature of the hazard and the structure of the system.

vessels. In contrast, the system to consider for loss of control of energy in one of the main production processes is well structured when the plant is designed with multiple barriers against the flow of released energy. This leads to two different management strategies, based on removal of causes of release, respectively on breaking the flow after the release.

Every work place in this way has many different, potentially hazardous activities and, consequently, risk management strategies to be adopted by a company will include a set of controls directed toward several different hazard sources. Therefore, consensus among decision makers at all levels of the socio-technical levels of figure 2.1 with respect to the characteristics of the hazard sources within a company and their control requirements is necessary. This will support effective planning of risk management strategies and the required formats for communication among decision-makers for direct hazard control, for management planning, and for regulatory monitoring.

It is therefore useful to characterize different means for hazard control to be considered for an overall risk management strategy in order subsequently to define the information required for effective control by the various actors in the socio-technical system. Considering a generic cause-consequence-chart as shown schematically in figure 5.1, four basically different safety control strategies can be distinguished, depending on the focus of the protective measures:

c. 1. Accidents can be counteracted by making the confinement of the hazard source less sensitive to the 'critical event'.

c. 2. The hazard source can be protected by fighting causes of its release.

c. 3. The flow of accidental events following release of the hazard can be controlled.

c. 4. The victims can be protected by emergency and rescue services.

c.1. Reinforce Hazard Containment

This is clearly a basic design issue, aimed at decreasing the sensitivity of a hazard containment to potential disturbances, to the 'critical event' defining the particular cause-consequence chart. This can be done in several ways such as e.g., by distributing substances or energy in several separate containments or by applying more resistant containment design or material.

c.2. Fight Causes of Hazard Release

A frequent reaction to system failures is to look for the 'root cause' in terms of equipment failures or human error. Such causes are then counteracted by use of reliable and/or redundant equipment, training of personnel, standard operating procedures, and redundancy in procedural steps or in allocation of tasks to personnel. The left-hand side of figure 5.2 illustrates this category.

We consider here two approaches to fighting causes of accidents:

– Efforts to block the branches of the causal tree close to their connection to the critical event by barriers and:
– Efforts to prune the tips of the branches, that is, to remove 'root causes' or decrease their probability.

c.2.1. Barriers Against Hazard Release

One effective safety control strategy to protect hazard confinement against disturbance is to break or block the flow of events along the branches of the causal tree leading to the 'critical event' and in this way to prevent a release of a particular hazard source. This strategy depends on a reliable identification of the branches of this causal tree and it is, practically speaking, applicable only for systems that are reasonably well structured and stable. The sources of information to consult for a reasonably complete identification of the branches to block by barriers depends very much on the magnitude of the hazard, that is, whether very rare causes are relevant or not.

The branches of the causal tree connect sensitive parameters of the hazardous process to the potential effects of events within activities around the process system. The *base* of the trees in which barriers should be inserted can be identified from a sensitivity analysis of the hazard source, while the particular *branches* to consider should be identified from an analysis of the surrounding activities. The activities to screen for potential origins of disturbances – that is the '*root causes*' found at the *tips* of the branches – depend on the degree of completeness required, that is, the magnitude of potential accidents.

For **moderate size hazards** rare causes are irrelevant and the necessary barriers and interlocks can be designed from a backtracking from the sensitive parameters to disturbances originating from errors and mishaps during the normal activities in the system. In this category, the planning of barriers and interlocks can be part of the control system design and evaluation, and the analysis will not require intimate knowledge of the actual work situation. Since protection is aimed at blocking the most likely causes of disturbance, not the rare contributors, the information necessary for design of protective measures will typically be available to the control system designer and protection is part of the normal control system design.

An illustrating example is the protection of the continuity of production by an industrial process plant, which is an important issue in highly protected industrial systems. Safety shut-down of a plant is a costly event, and to start the system and bring it up to power again often is a very complex and time-consuming experience. Consequently, protection of normal production will be based on barriers and interlocks to prevent that potential causes of disturbances can release safety shut down, see figure 5.4.

Protection against **major hazards** must consider more seldom events. Search for potential disturbances therefore cannot be based only on the analysis of routine activities around the system. Interference with operation can be caused by less frequent, erroneous acts by people working on quite different parts of the system, such as:

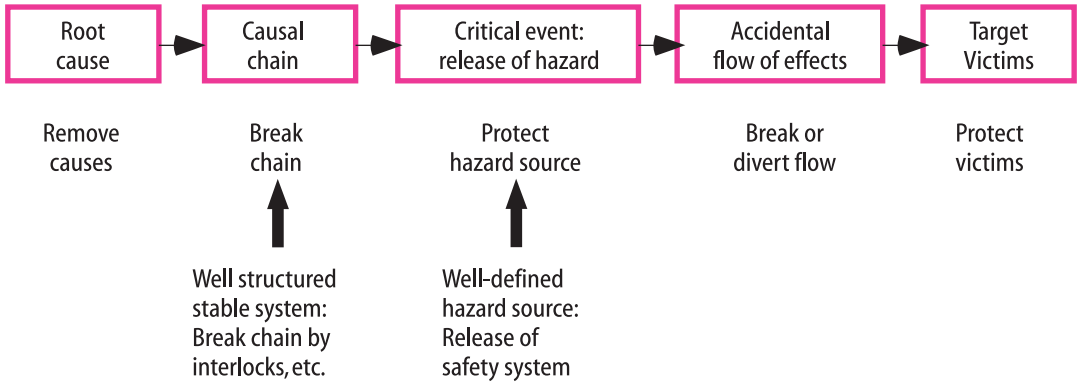


Figure 5.4 shows the typical intervention to protect operation of a well-structured and stable system such as an industrial process plant against spurious release of safety systems

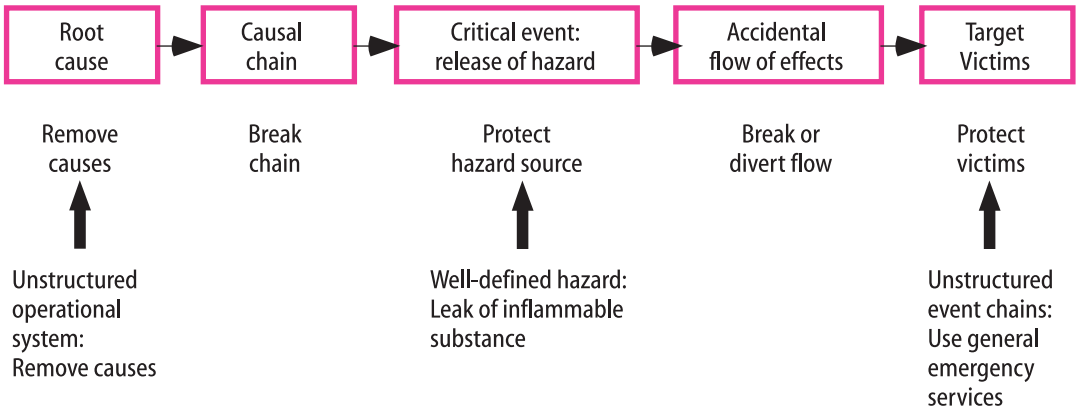


Figure 5.5. Protection against leaks and fires in petrochemical installations is an example of cases when removing causes and protecting the victims/targets are typically used, see left-hand side of figure 5.2.

– Disconnection of cables to facilitate vacuum cleaning;
– Interference from manipulation of electric welding gear;
– Short circuits from dropped tools;
– Damage to safety system by flooding from upper floor drain systems.

These types of disturbances must be found by a search guided by a topographical proximity criterion – analysis of all activity close to the part of the system in question. Furthermore, psychological proximity should be considered. It happens that features of an unfamiliar situation demanding a special procedure instead release an automated routine belonging to other task conditions, especially if parts of the two task sequences psychologically speaking are very similar.[3]

This control mode is particularly important to consider for well structure, tightly coupled technical systems during major maintenance and revision periods, when the protection by the normal 'defense-in-depth' protection of normal operation is ineffective.

c.2.2. Fighting Causes of Hazard Release

In some systems, the physical implementation of a hazardous process depends on local circumstances and the branches of the causal tree leading to a potential release of the hazard are less stable and therefore difficult to predict. In this case, protection based on barriers or interlocks blocking branches of the causal tree is less effective. Efforts to control safety then will typically be focused on a removal of 'root causes' or a decrease of their probability rather than on introduction of barriers and interlocks. See figure 5.5 for an example.

Considering **small and moderate scale** hazards found in unstructured and less stable work systems, such as construction sites, identification of causes of accidents will typically be guided by epidemiological analysis of past cases as found in reports to regulatory bodies.

A clear trend is, however, found toward request for 'zero-accident-strategies' based on the use of proactive risk management strategies. In that case, hazard analysis for less structured and stable systems must be carried out on occasion, by the people involved in the activities and the search strategies to identify the branches of the causal tree mentioned above will be relevant for such 'tool-box-meetings'.

Protection against **major hazards** by fighting causes is probably rarely relevant because efforts will be toward containing large-scale hazards in well-structured systems and protected by multiple safety barriers. However, one scenario for

3. See Rasmussen: Notes on Human Error Analysis and Prediction. In: Synthesis And Analysis Methods For Safety And Reliability Studies. Edited by G. Apostolakis, S. Garribba, and G. Volta. Plenum Publishing Corporation, 1980

which the class becomes relevant, is found during periods of major overhaul and revision of large-scale technical system that are normally protected by the 'defense-in-depth' mode.

In this case, rare accident scenarios must be identified by a kind of 'morphological search' because the potential for high consequence, low probability situations typically will be related to complex situations caused by several abnormal, coinciding conditions and events. A heuristic strategy to identify such situations resembles a 'design' algorithm: First, potential for accidents such as high energy accumulations, toxic material concentrations etc. are identified together with potential targets for accidental release such as people, environment etc. Then possible accidents are designed; i.e., the technical (mal-) functions and human actions, which are necessary to form the route from source to target, are determined. Finally, it is determined how changes in the normal system together with coincident normal and abnormal human activities will meet the designed accident pattern. Such accidents are typically due to "sneak paths" which are formed by minor mishaps or malfunctions in simultaneous human activities that only become risky in case of very specific combinations and timing (figure 5.6).

In this case, an important safety control strategy will be to plan the activities in a way that potential causes of hazard release are removed or their probability decreased by functional redundancy, high reliability equipment, and effective pre-briefing and training of work force.

c.3. Control Effects after Release of Hazard

In this category, the defense against accident is effective irrespective of the cause of the release of the hazard and the proper risk management strategy is to monitor the state of the defenses with reference to the design basis.

The effectiveness of this strategy depends on the closed-loop feedback concept: The state of the hazardous process is monitored, and deviation corrected by safety actions. Similarly, the normal state of the defenses is defined by design and monitored during operation. Thus, the quality of this risk management strategy depends on the quality of monitoring and the presence of adequate resources for action (safety action and maintenance).

c.3.1. Break the Flow after Release

In tightly coupled, stable systems protection against release of a hazard source can be based on efforts to break the flow of

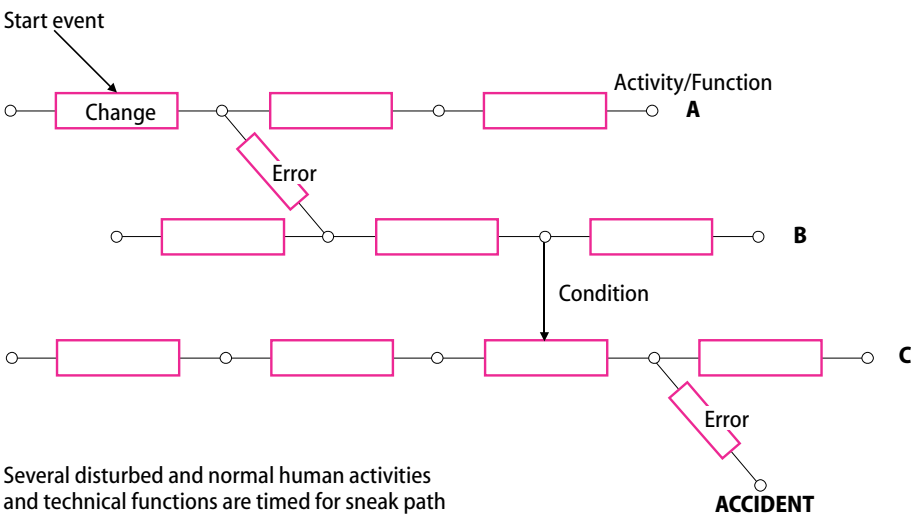


Figure 5.6. A schematic illustration of a 'sneak-path' search that can serve to identify causal chains of events not that are related to the normal functional structure of a system. Low probability, dramatic consequence chains of events can be identified morphologically. Find potential sources and targets for accident, "design" the necessary route and find errors and changes that will open it up.

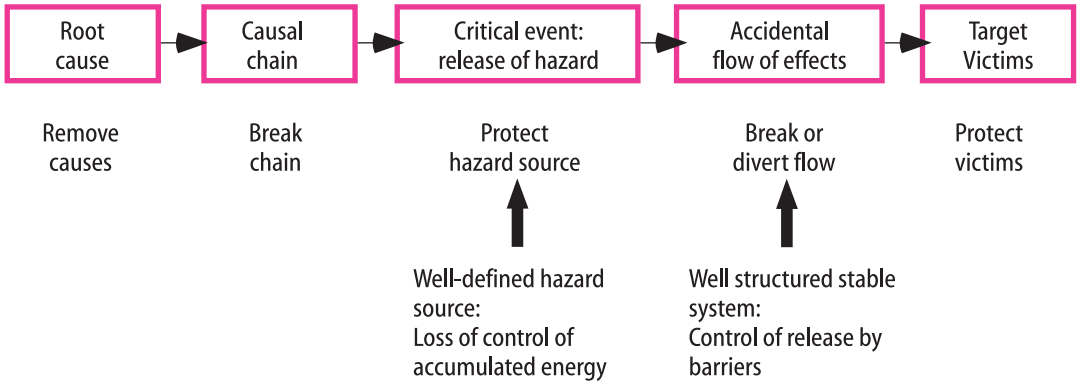


Figure 5.7. Protection against a well-defined hazard source embedded in a well-structured system can be introduced according to the defense-in-depth strategy introducing multiple barriers to break or divert the causal flow after the release of the hazard. This approach is typical for protection against 'run-away' accidents in process plants, see right-hand side of figure 5.2.

events following the release of a particular hazard. In some system, such as, e.g., industrial process plants, this protection can be based on automatic measures, see figure 5.7:

- First, loss of control of the energy balance is detected by an unplanned increase of temperature and/or pressure in the balance tank. Typically, then energy input will be cut down manually by operators in response to an alarm.
- If this act is unsuccessful, an automatic run-down or emergency shut-down will be activated.
- If the energy balance still is not stabilized, a controlled energy release will be automatically activated through safety valves or
- An emergency cooling system may be activated.
- If the system is not yet stable, physical barriers may direct the release away from people,
- and so on.

Similar protective measures by controlling the flow of events after release of hazard is found in other well-structured systems. One example is high speed driving on highways where protection of the passengers against release of the kinetic energy involves effective brakes, safety belts, air bags, crash barriers, energy absorbing car bodies, etc. The right hand side of figure 5.2 illustrates this strategy.

This control mode depends on a careful design of defenses against the effects of a released hazard, based on a probabilistic, predictive risk analysis. Such a predictive risk analysis is a theoretical construct relating the overall, ultimate risk level to a set of data on component failures and to several assumptions about operational practice, etc. This is done by means of models of the relevant accident scenarios. The input data necessary for an analysis depend on the boundaries selected for the model, which can be defined by an envelope encompassing very different segments of a socio-technical system. The farther away from the technical system and its hazardous process the envelope is chosen within the social environment, the more complex, unstable, and ambiguous become the relationships to include in a predictive model.

For a priori assessment of a system, the envelope has to include the total system affecting safety, i.e., also including operating practice, management policies and the probability of deviation from design intentions through system life time, see figure 5.8. Including organizational and management issues in predictive analysis leads to badly defined boundaries of coverage and to predictions based on 'expert judgement' methods for predicting the reliability of human behavior when empirical data are missing. In general, therefore, predictive risk analysis is considered an art and, as such, a particular analysis will be qualified by reference to the status of its author among peers. Amendola[4] dis-

4. Amendola, A. (1989): Planning and Uncertainties. Proceedings of the 2nd World Bank Workshop on Risk management and Safety Control. Karlstad, Sweden: Rescue Services Board.

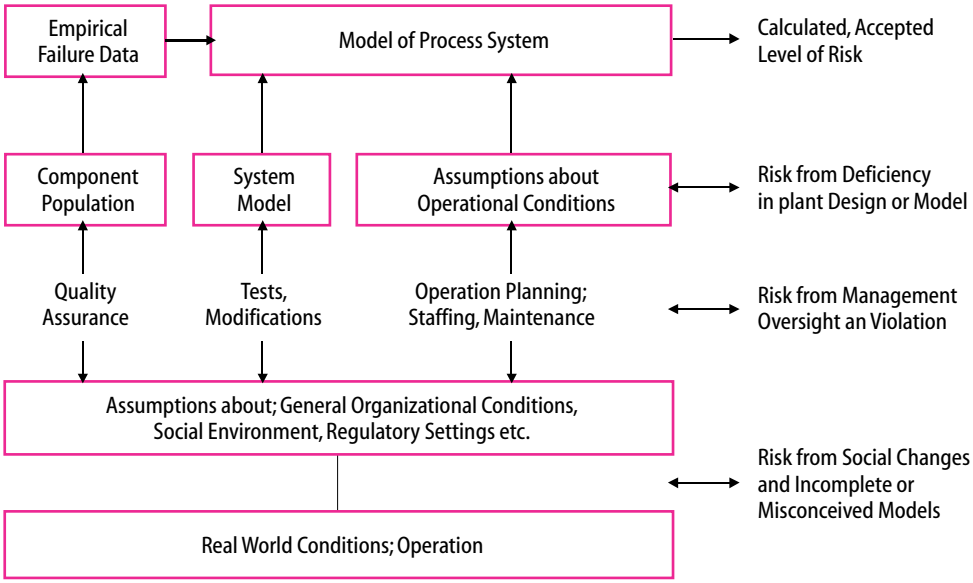


Figure 5.8. Scope of PRA for a priori acceptance of the conceptual design of a process plant must include a prediction of the performance of the operating staff, maintenance personnel, and managers.

cussed such limitations and emphasized the uncertainties of risk prediction. He referred to the results of a "benchmark-test" that Ispra had conducted among several European institutes to check the consistency of risk analysis including human reliability analyses performed independently by the different groups. The result had shown orders of magnitude differences in the result, in particular due to differences in the human performance models.

For risk management, the role of a risk analysis will be different. When a particular system is in operation, risk management is the function to monitor that the over-all level of safety matches the acceptance criteria. When it is no longer acceptable to measure the level of safety directly by the cost of accidents then it is necessary by a reliable analysis to break down the accepted level of safety, the risk, into elements that can be directly measured or monitored. In this case, therefore, the model does not have to include conditions and phenomena that can be directly monitored during operation, such as operational and maintenance practice and quality of management, see figure 5.9.

This makes predictive analysis much more reliable. For each relevant hazard source, it only has to break down its contribution to overall risk into observable preconditions for safe operation and for this only a model of the hazardous process and the defenses against release of the hazard is required. This is a much more technical issue than an overall analysis, but the framework for hazard and risk analysis will depend on the nature of the hazard source, the structure of the system in which it is embedded, and the risk management strategy adopted.

The model of functional relationships, the assumptions made on operational conditions, and data used for risk analysis then are specification for safe operation and should be used as reference for risk management decisions during operation. The source of information for risk management will clearly be the

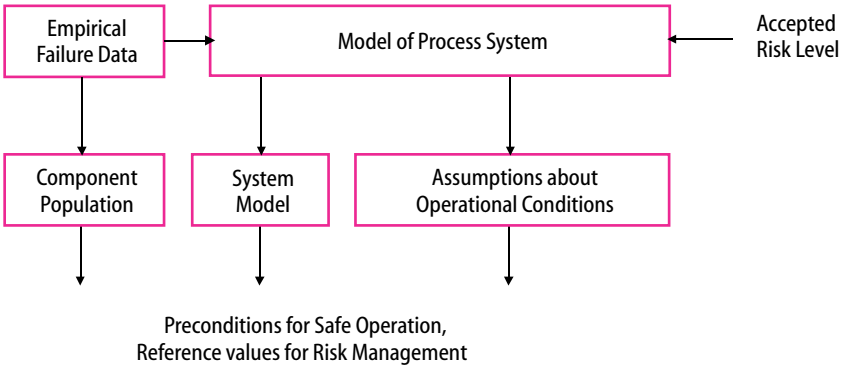


Figure 5.9. The role and scope of PRA for operational risk management is different. When the predicted risk has been accepted, the data, models, and assumptions used for the analysis of the productive, hazardous process become specification for safe operation and should be used as reference for operational risk management. Data on personnel performance can be measured and need not be predicted.

system designers, and a carefully planned communication of the preconditions of safe operation including the *reasons for the design choices* is mandatory. Since predictive risk analysis for operational risk management is different from risk analysis aimed at a priori acceptance of an installation, transfer of the approaches presently used for nuclear power is often irrelevant for safety control of hazards in other work domains.

c.4. Decrease Impact of Released Hazard

In some systems, the context shaping the anatomy of an accident is varying and depending on circumstances, and protection following the release of the hazard then depends on general measures focused on protection of the victims or support of them after the impact such as emergency management and rescue services. Reliability of emergency services typically depends on pre-planned emergency procedures to be used by the operating staff of the system and/or by special emergency service crews. We will return to this topic in chapter 10.

In this category we find life-saving and rescue services applied for, e.g., capsizing of ferries and transportation of hazardous goods.

5.1 d. The Cover Story

Considering the nature of causal categorization and explanation discussed above, the context of the scenarios described by the taxonomy must be defined by a brief narrative description, a 'cover story' that defines the context for the intended audience. This means that the degree of detail of this description will be very different whether the audience is composed by professionals from the domain or by academic researchers at a conference.

5.2 Conclusion

The taxonomy illustrates the complex relationships among the various dimensions of a framework for causal representation of accident scenarios and control strategies. They are clearly not exclusive, nor are the dimensions orthogonal, a close correlation is found between features of the various classes.

A summary of the framework is found in Table 5.1 and an overview of the relationship between system structure and hazard source – which is only implicit in the framework – is shown in figure 5.10. Figure 5.11 gives an overview of the different dimensions and points to the topics to be considered for risk analysis and system auditing.

A discussion of the relational framework suited for design of information systems and for auditing follows in the subsequent chapters.

Table 5.1
Summary of the dimensions of a pragmatic taxonomy.

The Taxonomic Dimensions
a. Target of Risk
- a.1 Individual Actor
- a.2 Staff
- a.3 Environment
- a.4 Harm to General Public
- a.5 Loss of Investment

b. Physics of Hazard Source
- b.1 Energy Accumulations
- b.2 Accumulation of Toxic Substances
- b.3 Structural Integrity and Stability
- b.4 Others, Mixed

c. Means for Safety Control
- c.1 Reinforce Hazard Containment
- c.2 Fight Causes of Hazard Release
  - c.2.1 Barriers against Hazard Release
  - c.2.2 Fighting Causes of Hazard Release
- c.3 Control Effects after Release of Hazard
  - c.3.1 Break the Flow after Release
- c.4 Decrease Impact of Released Hazard to protect Victims

d. Cover Story to Define Context of the Scenario

Hazard Source:	System Structure: Well structured and tightly coupled	Less structured and loosely coupled
Well defined:	– Hazard from well-defined physical process. – Anatomy of accident after release is defined by designed defenses. – Control by breaking accidental flow after release of hazard. – Risk management by monitoring the state of designed defenses. – Predictive Risk Analysis defines the defenses.	– Hazard from well-defined physical process. – Anatomy of accident after release depends on local circumstances. – Control by removing potential causes of release of hazard. – Risk management by monitoring potential causes of release and mitigating consequences by general emergency services. – Sensitivity analysis of hazard source is used to identify potential.
Examples:	– Run-away accident in process plant. – Fires in hotels and public assembly buildings. – Passenger safety in high speed highway diving.	– Capsizing of Ro-Ro ferries. – Transport of hazardous goods. – Disturbance of production in process plant. – Gas explosion on petrochemical site.
Poorly defined:		– Hazard is poorly defined, many sources from diverse processes. – Anatomy of accident varies widely. – Control by removing potential causes and conditions. – Risk management by monitoring behavior with reference to safe work procedures. – Epidemiological analysis of past accidents defines 'safe practice.'
Example:		– Construction sites.

Figure 5.10. A preliminary classification of hazard sources, system structures, and management strategies.

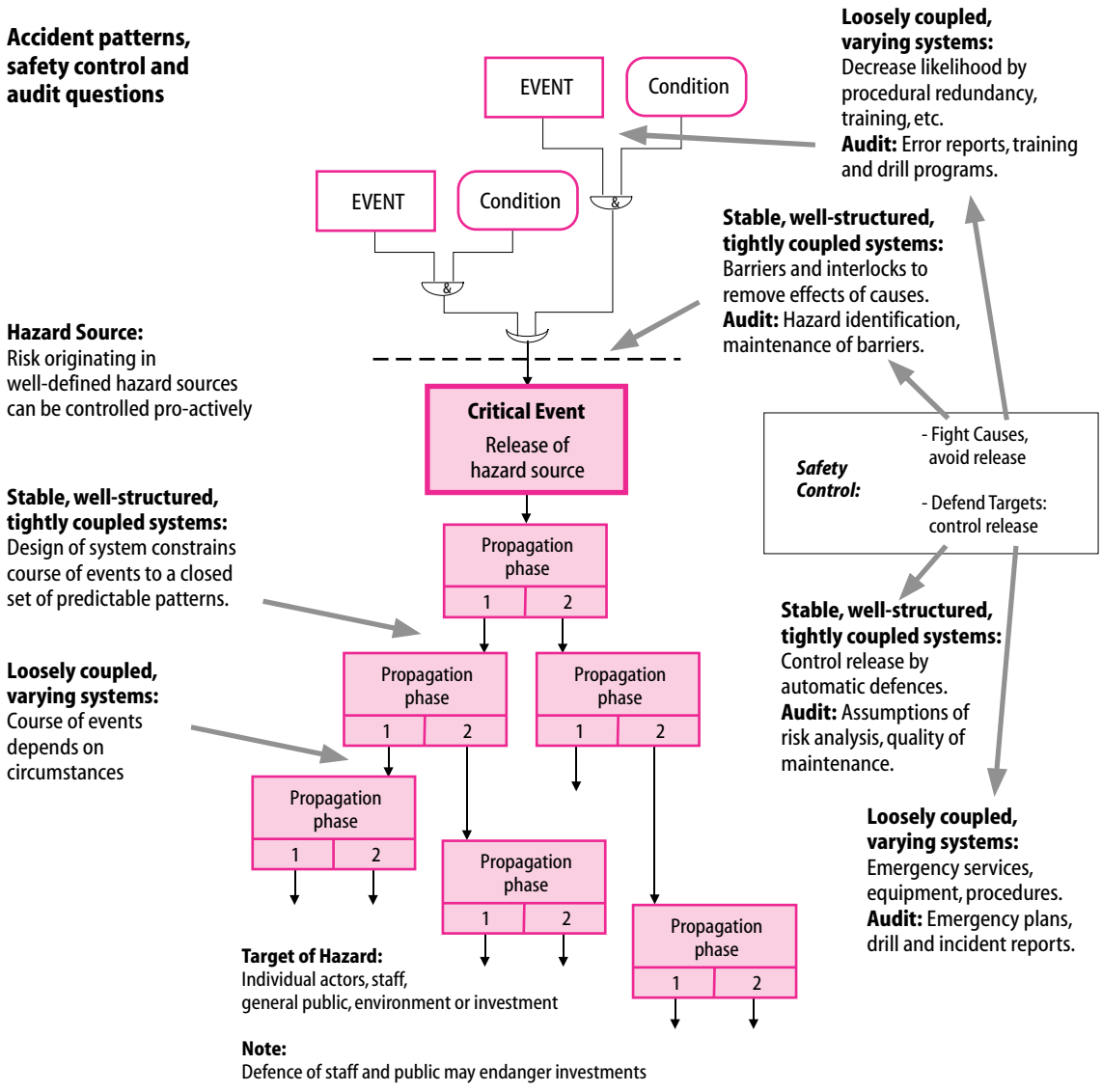


Figure 5.11. The figure shows an attempt to create an overview of classes of systems and the related safety control / audit strategies. All different patterns are relevant to all systems, but in varying degrees. E.g., safety of a well structured process plants may depend on quality of maintenance of defenses, while protection of investment, i.e., continuity of production, will depend on a strategy for avoiding release of hazard, that is on removal of causes. Similarly, protection against release of safety actions during normal operation may depend on designed barriers and interlocks, while threat from welding gear and fork-lift trucks during maintenance work call for proceduralized counter measures.

6. Preconditions of Proactive Risk Management Systems

Chapter 5 demonstrates that to be effective, risk management strategies must be planned to match the control requirements of particular hazard sources and the influence of the structure of the systems within which the hazard sources are found. Planning for a general 'safety culture' without such focus, but based on empirically defined 'resident pathogens' collected across system categories very likely will be to 'cry wolf' and will be counteracted by the competitive pressures meeting a particular system management.

6.1 Safety Viewed as a Control Problem

Risk management is basically a *control problem*. All industrial accidents are caused by a loss of control of a physical production process resulting in injuries to people, loss of investment, or damage to the environment. As discussed in chapter 2, the control system involved in this function includes the entire social system; from the operators and the maintenance staff directly in contact with the productive process, over the line management supplying the resources for this control, to the regulators and legislators that set society's conditions for accepting the operation.

In a dynamic environment, hazard sources, their control requirements, and sources of disturbances change frequently and risk management can no longer be based on responses to past accidents and incidents, but must be increasingly *proactive*. Control therefore must be based on a continuous monitoring of the actual level of safety, that is, the margin between the present system conditions and preconditions for safe operation. An adequate margin is then to be maintained by means of a closed loop feedback control strategy.

The design of this control system and tools for auditing must be based on a relational model representing the information flow structure and content necessary for control of work within the boundaries of safe operation. The present chapter will discuss the preconditions of proactive control and chapter 7 will then describe a taxonomy for design and auditing.

Analyses of past accidents and incidents still play an important role for setting priorities and identifying hazard sources. It has however been argued in the introduction that selection of means to improve safety from this analysis very likely will be ad-hoc cures of symptoms, sensitive to compensation by the normal adaptive forces within the system.

6.1.1 Proactive Safety Control

Closed-loop feedback control is necessary when the system to be controlled is subject to unpredictable disturbances. Feedback control is based on a comparison of the observed state of the controlled system with a reference value. The control action will then serve to minimize the deviation between the observation – a measurement – and a reference value. In a productive system, the target to reach and the observation – the feedback – basically refer to the specifications of the produced goods, i.e., whether they meet consumers' needs. This production control, however, must satisfy additional boundary conditions, the quality must meet standards, the cost must be minimized in a competitive environment, and operation must be maintained within safe boundaries.

Figure 6.1 shows how several tightly interconnected closed loops serve to match product specifications and quality to market requirements (quality management), to optimize the cost-effectiveness of the production process (resource management) and to ensure operation within boundaries of safe operation (risk management). Quality management and risk management serve to define the boundaries of acceptable cost-cutting in response to competitive pressures. These three management

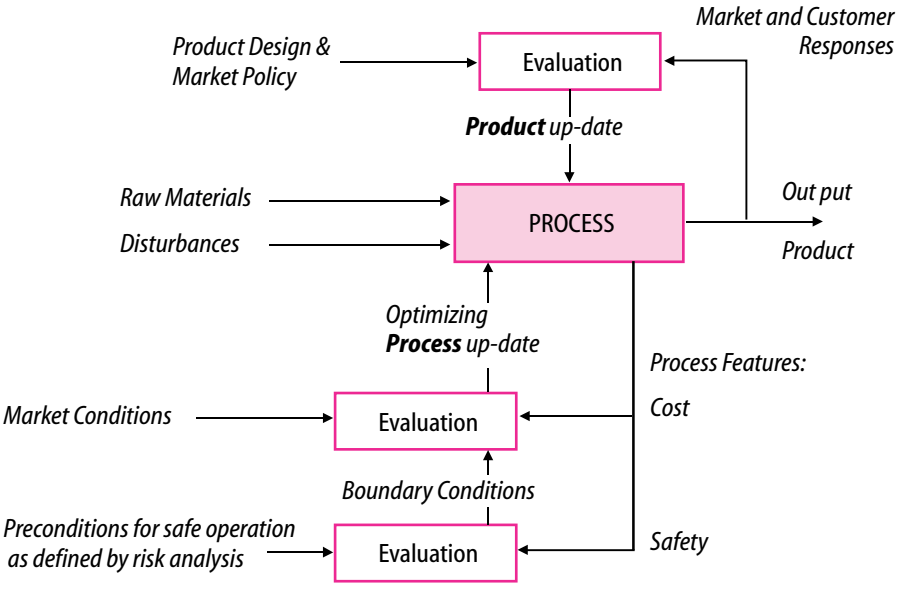


Figure 6.1. The adaptive control systems connecting control of production, cost, and safety.

functions thus cannot be separated when proactive quality and risk management is required in a dynamic society.

This interaction necessarily implies that risk management must be a line management function. From this perspective, production management in addition to *product* quality control also depends on capability to measure properties of the productive *process* in comparable, quantitative terms that will enable the proper cost-safety trade-off. Measuring *cost* and *quality* does not open special problems, but how to measure safety?

The requirements to organization of proactive risk management turn out to be very compatible with the requirements to a 'total quality management' system as required to meet the ISO 9000 standard. Comparison with quality management strategies and reference to this standard will be discussed in a chapter 8.

6.1.2 *Measuring Safety*

It is very often argued that it is difficult to define safety in other terms than by the absence of accidents and that the level of safety attained can only be measured by the number of accidents and incidents. That may be so in general terms. Recent major industrial accidents, however, have not been caused by stochastic coincidence of exotic error types or by mechanisms outside the range of the designed defenses. Most major accidents, including Chernobyl, Bhopal, Zeebrügge, Scandinavian Star, etc., have been caused *by organizations operating their systems outside the design envelope* under severe pressure toward cost-effectiveness.

The first step toward proactive safety management then is to ensure that organizations operate hazardous installations within the approved design envelope and continue to do so also under financial crises, that is, to ensure that operation is satisfying the precondition for safe operation as defined by the design basis analysis. Safety control should then be based on a facility enabling managers to compare operational conditions to the assumed preconditions of safe operation. This implies that, in the first approximation, measuring safety involves measuring the margin between the safety design envelope and the actual state of system operation, a problem that is realistic as long as the particular system design has been based on an adequate definition of the boundaries of safe operation.

6.2 Support of Operation within the Design Envelope

In conclusion, a first step toward proactive risk management would be to ensure operation of hazardous industrial installations within their design envelopes. This would have prevented several of the recent major accidents and appears to be realistic. The information required as a basis for safe operation is available within the industry, but it is not always in an explicit formulation, it is not available to the relevant decision-makers, and therefore it is not operational for the active line management.

In order to introduce proactive risk management that will be effective in a dynamic society, several conditions should be considered for further analysis. These conditions are reviewed in the following paragraphs.

6.2.1 Explicit Formulation of the Boundaries of Safe Operation

An analysis of the formulation of the preconditions for safe operation as found within different relevant industrial sectors is necessary. An explicit formulation is found within industries designed according to the defense-in-depth philosophy based on probabilistic risk analysis (Seveso directive, etc.). Less structured installations are often based on standards, industry practices, etc., and preconditions for safe operation is found implicit in such documents. Extraction and explicit formulation of the preconditions are necessary for proactive risk management when faced with changing environmental conditions.

6.2.2 Communication of Design Envelope to Operating Organization

During a period of technological change, the documentation of the boundaries of the operational design envelope and the communication to the operating staff at all levels should be carefully analyzed and redesigned.

6.2.3 Risk Management should be Part of Operational Line Management

This condition implies an integration of the information required for the safety and quality management into the information environment of the operational line management and the organizations preparing the legislation and business conditions of productive companies. For this purpose, an analysis of the information and communication systems applied by the managers is required to judge the feasibility of such an integration. It will be necessary to indicate the boundaries of acceptable operation within the context of the information environment serving the normal resource management. It is unlikely that a manager 'on the run' during normal work will consult a separate risk management tool.

6.2.4 Design of Managers' Information System Interface

Information environments systems for operation of technical systems (process plants, aircraft, air traffic control, etc.) for which the boundaries of safe operation can be defined by functional engineering analyses are presently being introduced in terms of 'ecological information systems', see the discussion in section 7.8. For the resource management level, design of ecological information system is a research issue.

7. Design of Proactive Risk Management Support System

Analyses of accidents have clearly shown that major accidents are created by the interaction of potential side effects of the performance of several decision-makers during their normal work. The control function of the risk management system of figure 2.1 then must serve to manage the potential interaction of such side effects by identification of the boundaries of safe operation for each decision-maker. For this it is necessary to ensure that information about the boundaries will be active as local constraint, visible to the particular decision-maker.

The safety control task must be based on a predictive identification of the boundaries of safe operation to be specified as a connected set of constraint for the performance of all decision makers during their normal feedback control of their local work domain. The constraints and their mutual relationship must be defined by some kind of predictive risk analysis. It is a major problem that these constraints and their relationship are dynamically depending upon the degree to which decision-makers explore the safety margin to cope with critical business situations. Ideally, therefore, this predictive identification of boundaries should be a dynamic function, based on knowledge about the control requirements of the basic productive, but hazardous, processes at the bottom level of figure 2.1. These control requirements should then be reflected in constraints on the performance of all higher-level decision-makers. This dynamic and predictive function requires an on-line, – 'live' – predictive risk analysis that presents to the decision-makers an up-dated representation of the current margin to the boundaries of safe operation.

The predictive risk analysis is only reliable as long as the model of accident scenarios used for prediction is reliable. It is therefore necessary to evaluate and up-date the model by careful analysis of the accidents that nevertheless may happen. *Post hoc accident analyses therefore have the important function to close the over-all feedback control loop involved in the long-term risk management at society level by supplying the information that can serve to update the models used for predictive analysis.*

The following paragraphs discuss the taxonomic framework to consider for design and audit of the work conditions of decision-makers that may be involved in accident causation. An analysis for design involves the following issues:

- Identification of *the decision-makers* and actors involved in the control of the productive processes at the relevant levels of the socio-technical system.
- Identification of the part of *the work-space under their control*, that is, the criteria guiding the allocation of roles to the individual controllers.
- The *structure of the distributed control system*, that is, the structure of the communication network connecting collaborating decision-makers.
- The *content of information flow* among decision-makers. That is, do the decision-makers have information about targets and the actual state of affairs in compatible terms.
- The *risk awareness* of decision-makers. Is this information given in a form that makes it active during normal, routine operations, that is, is the *form of communication operational with respect to risk awareness?*
- *Capability of decision-makers.* Are decision-makers competent with respect to hazard control? Do they understand the nature of the hazard sources and are they familiar with the factors sensitive to control actions?
- Finally, the *commitment of decision-makers* to safety must be ensured.

These requirements turn out to be very similar to the requirements to a Total Quality Management organization as it is specified in the ISO 9000 standards. This is a natural consequence of the TQM efforts also to introduce a proactive quality

management system and chapter 8 will present a reference to and comparison with the ISO requirements.

7.1 Identification of Decision Makers

The analyses of past cases serves the identification of the decision makers (*controllers*) who have been involved in the preparation of the landscape through which new accidents may also propagate. The "Generic AcciMaps" developed by generalization from analysis of a representative set of accident reports serve to identify the decision-makers who are relevant in this context. From a control point of view, the interaction among the decision-makers potentially involved in accident causation is somewhat peculiar. As mentioned in a previous section, all these decision makers will be busy managing their particular part of the work domain. Their attention will be focused on the control of the means and ends of their normal productive tasks. Their performance must therefore be studied from the point of view that they strive to meet their production targets and to optimize process criteria such as cost effectiveness under the constraint defined for their local context. One of these local constraints is to operate within the boundaries defining safe overall operation and a critical issue is that the boundaries relevant to a particular decision maker depend on the activities of several other decision makers found within the total system shown in figure 2.1.

A format of a map of the decision-makers involved in planning and implementation of transportation of hazardous goods is shown in figure 7.1.

To effectively plan an organization to include proactive risk management, the actual, co-operative structure should be matched to the control requirements (production as well as safety) posed by the work space. A review of the criteria governing role allocation in an adaptive organization is therefore useful here.

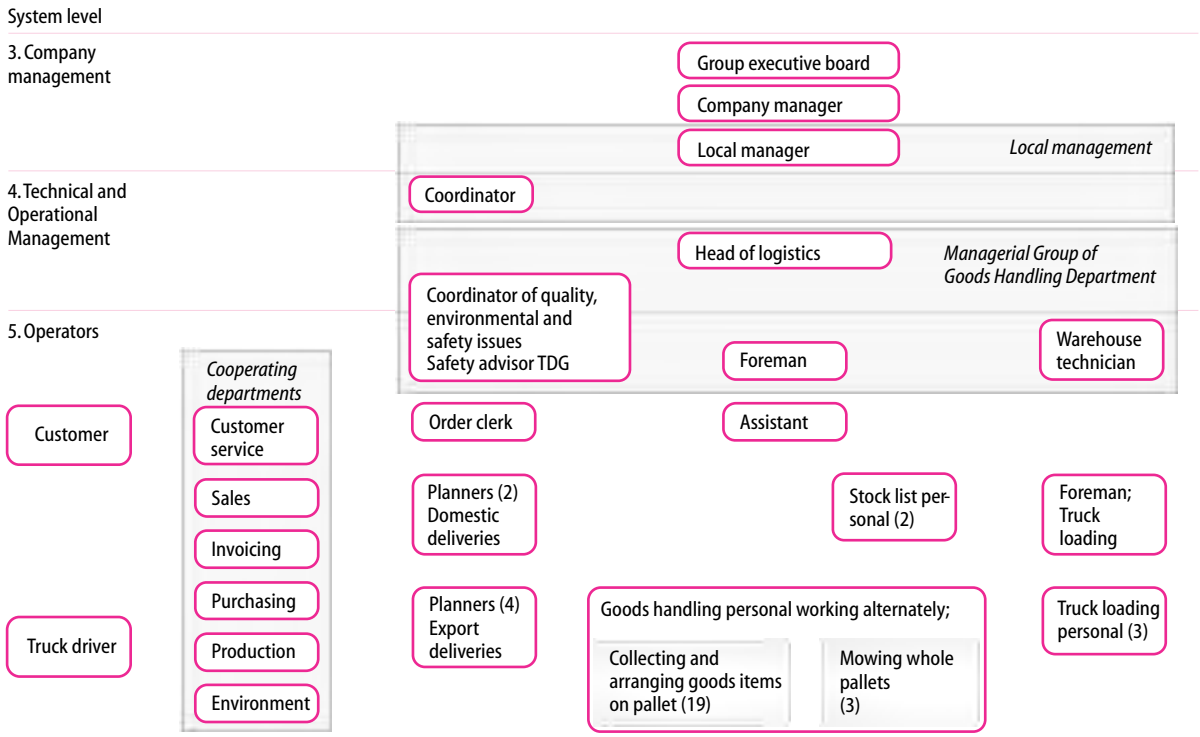


Figure 7.1. An ActorMap based on investigations into the productive every day activities within a company manufacturing, storing and delivering products classified as dangerous goods. The focus of this ActorMap is on the goods handling department whose controllers are indicated on the level of individual or type of actors. Co-operating departments are indicated on "department level".

7.2 Identification of Control Space: Role Allocation

A work place typically involves many loosely coupled activities and, therefore, requires co-ordination by an integrated control function in order to perform in a concerted way. Information processing involved in decision-making in an organization serves this purpose.

Acceptance of this systems point of view implies that the functions of decision-making and the structure of the involved organization cannot be modeled or planned without considering the basic system function (process plant properties, manufacturing processes, military missions, etc.) which the decision making is intended to control. Studies of organizations and management without consideration of the subject matter of

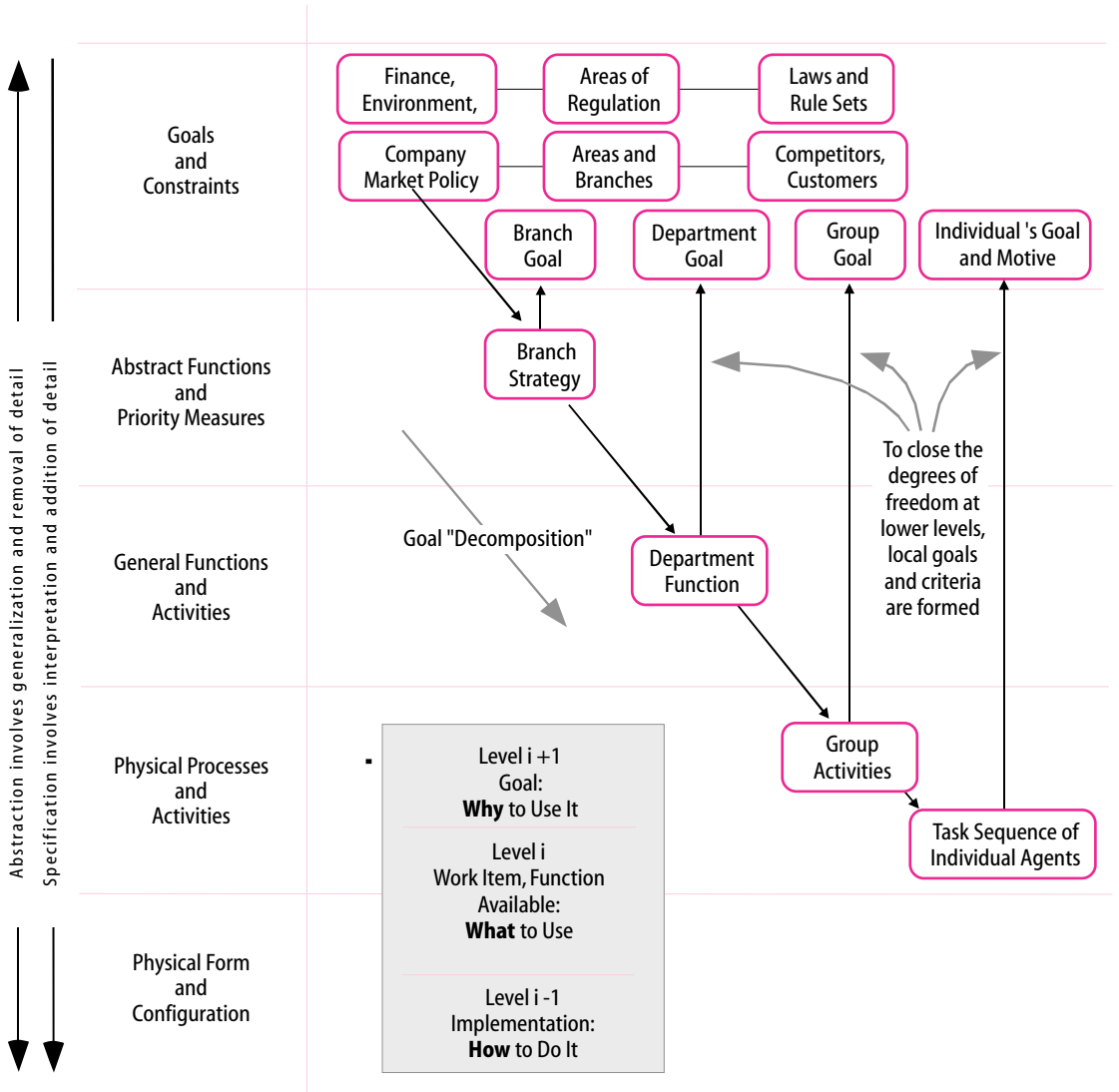


Figure 7.2. The shows a representation of a work space in terms of a decomposition-abstraction hierarchy. The problem space represents the available means for meeting multiple ends in a decision task at several levels of abstraction. The figure illustrates how company objectives are communicated downward, and reinterpreted at each level. Different decision-makers take care of different parts of this space.

management appear to be ineffective (cf. the horizontal versus vertical orientation of analyses discussed in the introduction).

Considering organizational decision-making as being a resource management problem, a representation of the work-space in terms of its means-ends relations defines the space in which decision-makers have to navigate. This approach to representation of a workspace is discussed in detail elsewhere[1] but a brief illustration is given here by figure 7.2. A more detailed discussion of the means-ends representation is found in Chapter 10.

Co-operative decision making is viewed as a distributed control function serving to co-ordinate the loosely coupled activities within the workspace shown in figure 7.2. In a modern work system the 'organization' described in formal organization charts may reflect only the formal distribution of financial and legal responsibilities, whereas, the 'functional organization' reflecting the actual division of work among actors of this system will change dynamically with the control requirements of the work space.

Following this point of view, we have to consider organizational aspects at two different points of view, see figure 7.3:

1. The *functional work organization* required to co-ordinate activities will be determined by the control requirements of the work domain. This functional organization will determine the allocation of roles to the individual actors and the *contents* of the communication required for co-ordination.
2. On the other hand, the *social role configuration* chosen by or imposed upon the individuals and/or teams depends on the management style which, in turn, influences the *form* chosen for the communication and social interaction within the functional team or organization. This latter issue will be discussed in the next section.

1. Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.

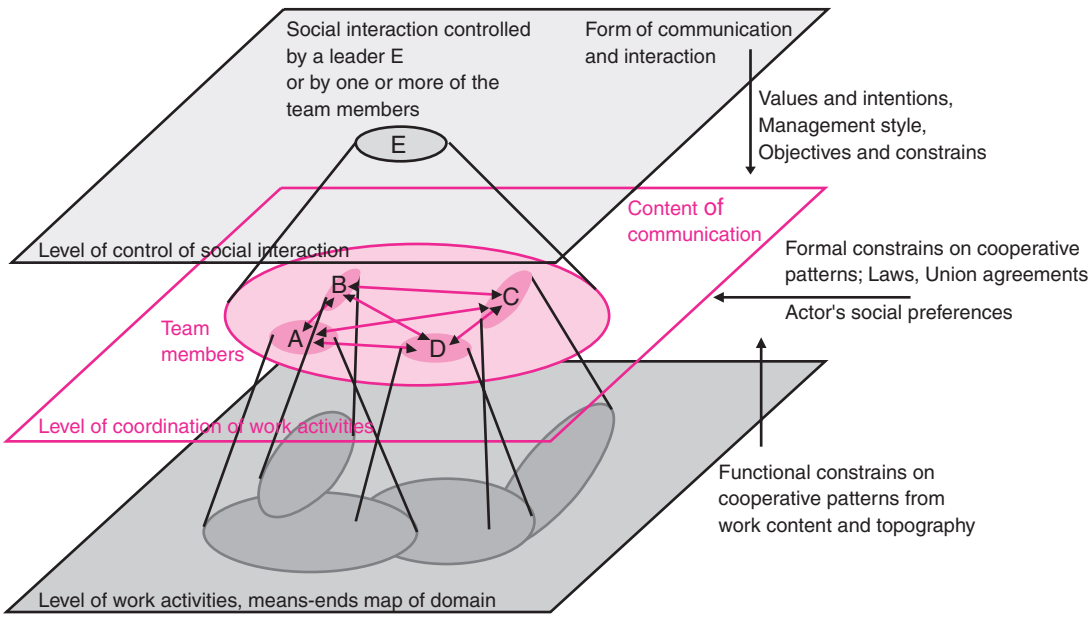


Figure 7.3. The figure illustrates schematically the forces that shape the collaborative structure in control of a loosely coupled work-space. It emerges in the interaction between the bottom-up propagating control requirements of the work domain and the top-down propagation of social practice and management style.

7.2.1 The Functional Organization

The functional work organization is emerging from the interaction between the bottom-up propagating control requirements of the work-space and the top-down propagation of social practice and management style. Figure 7.3 illustrates four agents or decision-makers each allocated particular, but overlapping 'activity windows' giving access to a part of the overall work domain. The concerted action within this, normally rather loosely coupled, work domain requires inter-agent co-ordination and communication. The structure of the communication net and *content of the communication* and, therefore, the actual work organization is determined by the control requirements of the work domain. The social organization, in contrast, is determined by the conventions chosen for the *form of the communication*, which depends on the 'management style' or 'culture'. This, in turn determines whether co-ordination of communication involves a manager as in a traditional, hierarchical organization, or negotiation among actors, as in a modern, flexible organization.

The control requirements of a work domain change over time as will the functional work organization. A particular division of activities and, consequently, a functional work organization will evolve for each situation depending on the competencies of the actors, the 'technology' of the work domain and on the external environment of the organization. Studies show that, even in traditionally tightly controlled organizations such as the military and high hazard process plants, the actual co-operative structure changes dynamically to match the actual circumstances and therefore a framework for modelling must be able to capture this adaptive feature.

In the actual work situation, ways to allocate work roles to the individual actors will depend on several criteria:

Norms and Practice. In stable systems with a long prehistory, the formal role configuration is often closely related to the actual and frequently hierarchical organizational structure and the corresponding social status rankings. Very often, this formal structure poses very strict constraints on the actual work allocation, in particular when strict boundaries between professions are established through e.g., union agreements.

Load-sharing. Frequently, division of work is governed by efforts to share work load, – both formally during work planning and informally and dynamically during the work process itself.

Functional de-coupling. This criterion reflects efforts to minimize the necessary exchange of information among actors. This criterion is particularly important in dynamic, fast acting systems for which the control requirements can be organized according to sub-units with internal high capacity-fast time response requirements, but with less and slower mutual interaction. Controllers can then be organized in a hierarchical structure according to capacity and time requirements, which normally will be reflected in role allocation.

Competency. The competence required for different tasks clearly influences the division of work.

Information access. In stable, work domains and during routine situations, span of attention of the actors, and the information access they are given, can be rather limited. However, in a changing domain and during unfamiliar situation, this should not be the case. The potential for discretionary problem solving depends heavily on the width of the information window available to the decision.

Safety and reliability. For work in a domain posing a hazard to the staff, the investment, or the environment, safety criteria, such as functional redundancy, are governing role allocation. In this case, critical functions are allocated more than one individual or team so that independently tests serve to verify the performance in a particular function.

These criteria are often competing, and their influence change with time governed by the control requirement of the work-space. For instance, even in a military organization governed by formal ranks, the control requirements of the operations occasionally take over and shape the co-operatives structure. The work of Rochlin et al.[2] demonstrates the pronounced ability of the organization on an aircraft carrier to shift between (a) a formal rank organization, (b) a self-organizing 'high-tempo' work co-ordination across ranks and organizational units and (c) a flexible emergency organization responsive to the immediate requirements of critical situations. In such cases, the dynamic control requirements overrules the formal, social organization found in less stressed periods.

An important lesson to learn from this study is that an organization can have very high reliability, if it is given the opportunity to evolve into a complex, dynamic overlay of

2. Rochlin, G. I., La Porte, T. R., and Roberts, K. H., (1987): The Self Designing High Reliability Organization: Aircraft Carrier Flight Operations at Sea, Naval War College Review, Autumn 1987.

several management modes and networks matching closely the requirement of the different critical task situations. Another important feature of the aircraft carrier case is the extensive redundancy implicit in the informal, operational networking, in which any individual is a member of several overlapping structures and 'has an eye on' his neighbors performance. In most business organizations, such redundancy will be taken to signal inefficiency and, probably, will deteriorate through the adaptive pressure of normal business.

Recent accidents present clear examples of the conflict between operational criteria such as sharing workload, and more latent criteria such as procedural redundancy for protection against rare occurrences. Adaptation of the role allocation and the co-ordination of work to local criteria during normal conditions have lead to severe consequences under unhappy circumstances. In the Clapham Junction case,[3] for instance, safety checks following modifications of signal system wiring were planned to be independently performed by three different persons, a technician, his supervisor, and the system engineer. Work force constraints and tight work schedules, however, led to a more "efficient" division of work. The supervisor took part in the actual, physical work and the independent check by him as well as by the engineer was abandoned. In addition, the technician integrated the check (a "wire-count") into the modification task itself although it was intended to be his final separate check. In short, adaptation to a more effective division of work under time pressure causes the redundancy required for protection against rare events to deteriorate.

It is clearly an issue for organizational design and auditing to identify the work division criteria that are essential for safety in the different hazard categories and to plan auditing probes accordingly.

7.2.2 The Social Aspects of Organization

The co-operative structure responding to the control requirements of the operations clearly specify the *contents of the communication*. On the other hand, many degrees of freedom are left with respect to the *form of communication* serving the co-ordination among actors, depending on the conventions chosen for social interaction. Various structures of social organization are possible and they may be more or less independent of the task and the role configuration principle adopted as well as the characteristics of the work domain.

Traditionally, however, the social organization is hierarchically organized corresponding to business professions or military rank. Then one level of decision-makers evaluates and plans the activities at the next lower level. Even within this structure different co-ordination and management styles are possible, depending on whether the communication downward through the system is based on the communication of orders (the military model), on the communication of procedures (the bureaucratic model), or on passing down objectives (the adaptive model).

Recently, a clear trend is toward more flexible 'learning' organizations to be able to respond more effectively to the present fast pace of change.

Since all types of social organization can serve properly the control requirements of a given domain, the basic difference is the *form of communication* chosen to serve co-ordination, that is, whether information is passed as neutral information, advice, instructions, or orders. The effective way of influencing the social organization independently of the work organization will be through constraints and conventions for communication formats.

7.3 The Structure of the Control System and the Communication Network

Next, the *communication channels* through which the decision-makers co-operate should be considered with respect to the normal work performance and to the control of boundary constraints. This analysis involves analysis of both the communication among decision-makers within a particular work organization (company, institution) and the communication required for the overall risk management within the system in figure 2.1. This perspective is focused on the design of the work and safety control (management) systems and the subsequent audit of its consistency.

This issue is increasingly important as the coupling between organizations become tighter, due to effective communication and transport systems. For 'just-in-time' production systems, co-ordination across organizations of suppliers, manufacturers and customers is necessary at all organizational levels.

3. HMSO (1989): *Investigation into the Clapham Junction Railway Accident*. The Department of Transport. London: Her Majesty's Stationary Office, 1989.

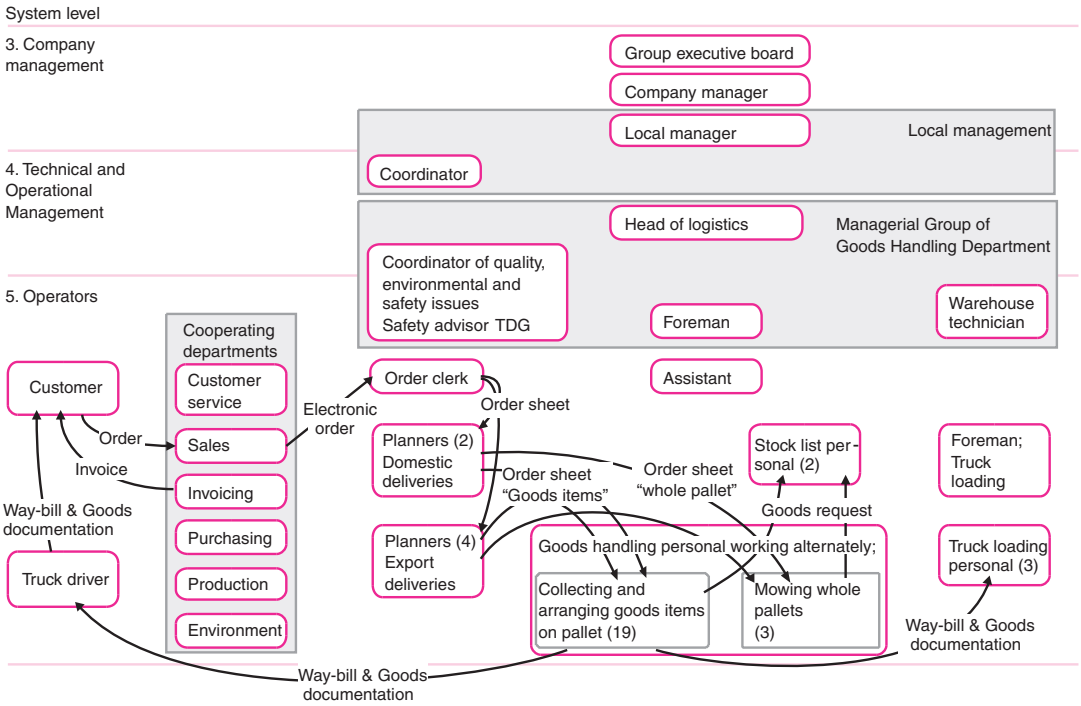


Figure 7.4. An "InfoMap" illustrating the operational flow of information amongst some of the actors in the ActorMap in figure 7.1, in connection with the normal every day work of planning, picking up, arranging and delivering goods as ordered by a customer. In a system like this, which is stable over time, the operational information flow is restricted to the operator level.

Identification and evaluation of the control structure found in an organization involves a consistent analysis of the structure of the information network and the content of communication among actors. For this purpose, a "connectivity matrix" as shown in figure 7.5 has proven useful. From information in interviews, a matrix is derived and shaped by means of row-column manipulation to identify diagonal sub-matrices. This representation of the communication structure identifies the groups needing close cooperation for a particular task situation. The connectivity matrix analysis can be a very effective tool for matching a formal organizational structure to the natural group formation.

Information Receiver

Information Source

Actor	A	B	C	D	E	F	G	H	I	J	K
A	○										
B		○	✓	✓	✓						
C		✓	○	✓	✓						
D		✓	✓	○	✓						
E		✓	✓	✓	○	✓	✓	✓	✓	✓	
F					✓	●	✓	✓	✓	✓	
G					✓	✓	●	✓	✓	✓	
H					✓	✓	✓	●	✓	✓	
I					✓	✓	✓	✓	●	✓	
J		✓								○	✓
K											○

Figure 7.5. The actual work organization can be identified by means of a communication matrix. In the figure the actors B, C, D and E form a group as do actors E, F, G, H, and I. The two groups are interconnected by actor E. It appears that actor J acts as a kind of secretary receiving messages from the group E, F, G, H, and I, and passing on the reports to actor K and to actor B.

The result of the analysis is:

a. The identification of the actual work organization as evolving from the adopted criteria for division of work,
b. The interaction between the work organization and the existing technological underlay in the lower levels of the work domain and
c. The interaction between the external surroundings and the prioritization and planning activities in the upper ends of the work domain.

Figure 7.6. The communication structure that evolves during practical work may be very complex and opaque. The figure is based on the analysis of the Vinca Gordon case, see appendix A.5.

7.4 Identification of the Flow of Control Information

When the allocation of control spaces and the communication network has been analyzed, an evaluation of the information flow from a closed loop control perspective is required.

7.4.1 *Objectives and Criteria*

It is critical for any control function that the controllers have information about proper *action targets* (productive and safety related objectives) in a form and at a level corresponding to their action opportunities.

According to the previous discussion, this is a very complex issue. For the normal work activities, basic business objectives propagate downward through an organization and will be formulated by different concepts at the different levels of the company involved. Objectives for action have many shades. They can be expressed in terms of:

– Product specifications and targets for production volume;
– Process optimization criteria such as cost effectiveness;
– Constraints on processes, such as safety, work conditions, etc.

At the higher levels, objectives and values are formulated in rather general terms. When objectives propagate downward through an organization, degrees of freedom in terms of options for action multiply since there are several ways of implementing objectives. Accordingly, objectives are to be

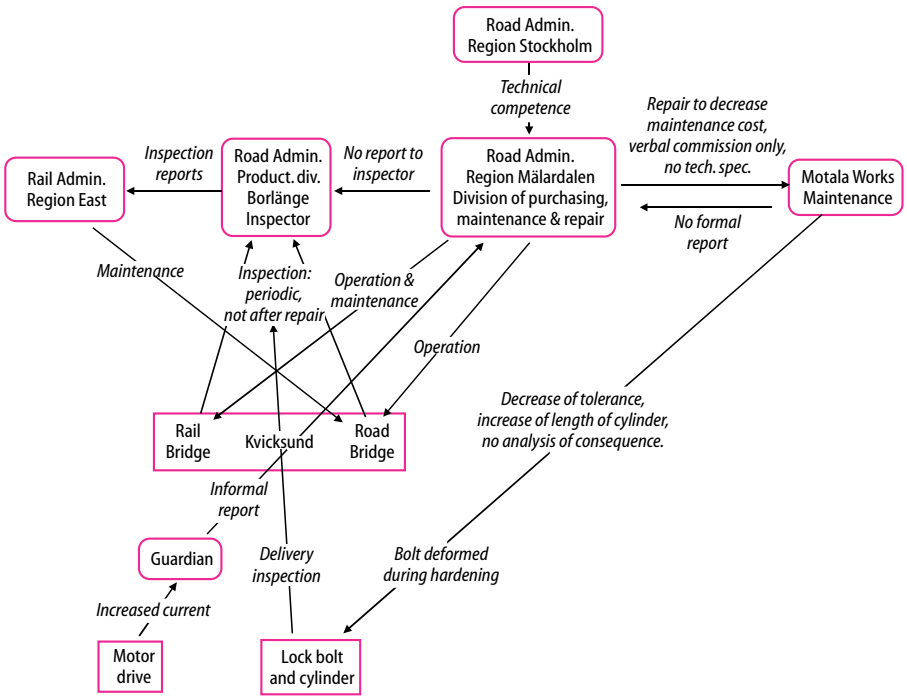


Figure 7.6 show schematically the very informal communication links found behind an accident, and demonstrates the need for a formal approach to analysis of the communication network.

interpreted according to the particular local context. For the overall risk management, similar considerations apply for the propagation of objectives downward through the socio-technical system of figure 2.1. For this propagation, special care should be taken to analyze the influence of the different time-lags in the response to change at the various levels.

The present general trend in legislation and regulation away from prescriptive rules to performance centered objectives should be considered carefully when analyzing the propagation of objectives and values downward through the socio-technical system. In Sweden efforts are found to introduce an objectives-and-result management strategy in government institutions and administrations.[4]

A similar trend is found toward performance-based legislation for several types of risks in the US. This has been most obvious regarding chemical plant accident risks, and such rules are now being applied to transport accident risks, workplace safety hazards, and food (product) contamination risks. The 1970 Occupational Safety and Health Act (OSHA) of the USA authorizes the administration to employ prescriptive standards to reduce specific hazards to worker health in the private sector. However, since the regulatory process typically requires 6–10 years to develop adequate prescriptions, the fast technological pace of change has led to the introduction of the 'general duty clause' that has substantially enhanced the agency's ability to protect workers during the latest decades.[5] This clause states that each employer "shall furnish to each of his employees a place of employment that is free from recognized hazards that are causing or are likely to cause death or serious harm to his employees".

In this way, it is required that certain generic functions are carried out to avoid accidents, leaving the details as to how the functions should be carried out to the companies (or other regulated organizations).

This approach clearly is an implementation of the closed-loop, feedback design concept and thus is based on a set of assumptions:[6].

- Each company will use the flexibility of the new rule to develop a detailed method of carrying out each function;
- The local rules will be effective and represent a generally accepted "best practice" of its industrial sector;
- They will be efficient to use because it will be compatible with the company's production functions and profit goals, and
- They will be acceptable to the company because they are not imposed by an external agency.

In this way, detailed rule-making takes place at a level where the context is known, and this change clearly also change the role of decision makers within the social control hierarchy.

For most companies, the new performance rules and reinforcement policies pose several problems. First is the big uncertainty of what it must do to carry out each function in an appropriate manner (since the rule requirements are broadly expressed). Uncertainty often translates into greater cost and difficulties for line management. The second problem is how to cope with the pressures from persons at risk who are stimulated by the disclosures. To cope with the first problem, many companies are developing their own detailed internal, prescriptive rules, so that there is now an even greater prescriptive rule culture within such companies. For the second problem, companies are using attorneys and public relations people to deal with the new pressures caused by transparency. The third problem involves uncertainties about the management system needed to prevent violations, and is being dealt with by following ISO and EMAS efforts to define good management systems.

This change of legislation strategy clearly brings with it a very substantial change of the structure of the distributed decision making system of figure 2.1. It changes the need for information about the detailed work context at the upper levels and makes the traditional, separate safety organization obsolete. It also clearly will change the need for interaction between regulatory decision-makers and substance matter experts – see the discussion of competence below.

When safety is controlled by performance objectives as is the case with generic regulation, safety becomes just another

4. Report of the Committee on Management Forms of the Administrative Authorities. SOU, 1993:85 (In Swedish). Stockholm: Statens Offentlige Utredninger.
5. For a recent review, see Baram, M. (1996): Generic Strategies for Protecting Worker Health and Safety: OSHA's General Duty Clause and Hazard Communication Standard. Occupational Medicine: State of the Art Reviews, Vol. 11, No. 1, January–March 1996.
6. Baram, M., (1996), personal communication. See also Proceedings of Symposium: Multinational Corporations and Their New Responsibilities to Disclose and Communicate Risk Information. Eds. Baram, M. and Partan, D. G., (1988). Special issue; Boston University International Law Journal, Vol. 6. No. 1.

criteria of a multi-criteria decision making and becomes an integrated part of normal operational decision making. In this way, the safety organization is merged in the line organization.

Such modern attempts to delegate decisions and to manage by objectives call for an explicit formulation of value criteria and effective means for communication of values down through society and organizations. Interesting developments have been presented for this kind of distributed organizations[7] and formal strategies have been proposed for 'ethical accounting' to ensure that the impact of decisions on the objectives and values of all relevant stakeholders are adequately and formally considered.[8]

Overall, from a risk management point of view, some important questions for systems analysis are raised:

- Are objectives formulated by principals in a way such that the interpretation and re-formulation performed by their agents are properly considered?
- Are boundaries of acceptable performance known or can be observed by agents and/or principals?
- Is an auditing function in place that effectively serve to monitor the propagation and interpretation of objectives within the entire socio-technical system?

For these questions, it is necessary to take into consideration that some objectives and constraints change with time, some are more stable and related to generally accepted, professional practices and conditions. For the present analysis, an important issue is:

- How effectively are *changes in objectives* communicated downward the organization, and how effectively are *changes in local constraints and criteria* (e.g., to change of technology) communicated upward the system to be considered for resource management and safety control?

7.4.2 *Information on Actual State of Affairs*

An important issue in a closed-loop, feedback function is the observation or measurement of the actual state of affairs and to response to control actions. No control system will perform better than its measuring channel. Important questions therefore are:

- Do controllers (decision-makers) have information about the *actual state* of the functions within their control domain and is this information compatible with (comparable to) the objectives as interpreted by the agent?
- Can a discrepancy with respect to objectives or performance criteria be observed?
- Can the margin to the boundaries of acceptable performance be determined or observed?

The general trend toward generic legislation, discussed above, has raised public concerns that it is too loose and not easily enforceable or effective because it leaves so much up to the companies. It has therefore typically been reinforced by government efforts to monitor the presence of proper feedback of performance information. Company documentation is required to demonstrate how it is implementing the rule with disclosure of the documentation to the agency that enacted the rule and to local officials and persons at risk (e.g., workers, community). This should make company implementation of the rules transparent so that the agency or persons at risk can take various actions (legal actions, community pressures, market forces etc.) to force the company to correct deficiencies. In this situation it now appears that the generic law approach has increased the fear of law-suit and, therefore, a distortion of the allocation of resources[9] for effective risk management takes place.

7.5 The Capability of Decision Makers

From a closed-loop control point of view, the question about the capability of controllers, decision-makers that is, is crucial, in particular when interpretation of generic regulation is delegated to the local decision-makers:

- Are they capable of control?
- Are they thoroughly familiar with the control requirements of all relevant hazard sources within their work system?
- Do they know the relevant parameters, sensitive to control actions, and the response of the system to various control actions?
- Can they act without undue time delays?

7. Mitroff, I. I. and Linstone, A. I. (1993): *The Unbounded Mind: Breaking the Chains of Traditional Business Thinking*. New York: Oxford University Press, 1993.
8. Bogetoft P. and Pruzan, P. (1991): Planning with Multiple Criteria. Amsterdam: North Holland.
9. Breyer, S. (1993): Breaking the Vicious Circle, Toward Effective Risk Regulation. Boston, Ma.: Harvard University Press.

Such questions of capability involves the issue of the competence of decision-makers, not only in terms of *formal knowledge*, but also *heuristic know-how* and *practical skills* acquired during work and the ability of an expert to act quickly and effectively in the work context. This latter issue also involves the question whether decision-makers are aware of the need to act. We will discuss this in a subsequent section, after a review of the relevant forms of competence.

7.5.1 Forms of Competence

The extent and content of an actor's competence determine what information is immediately available and what must be communicated in a particular situation. It also determines what kind of advice can be given – and when – without insulting a professional, competent agent.

In a normal *work context*, competence includes knowledge about functions (tasks) (*what*) to perform in a given situation, the means and resources available, that is, *how* it can be done and the objectives or ends, that is *why* it should be performed. Finally, competence includes the *criteria* and *constraints* determining the choice among options.

Knowledge of the competence of co-operating agents is necessary to judge what information to communicate, up, down, and horizontally in the system. Usually, this competence is based on formal work instruction that initiate an agent to work, while trial-and-error learning (such as, e.g., experiments to identify the boundaries of acceptable efforts toward improved cost-effectiveness) serve to generate know-how and thus to optimize performance

What to communicate and when depends entirely upon the cognitive mode of decision-making applied by the actors and the nature of 'naturalistic' decision making must be taken into account when studying the form of communication serving collaborative work.

In an instructive paper, Colas[10] from EDF – Electricité de France – has discussed the need to formulate the characteristics of operator professionalism when planning communication with plant operators, e.g., when writing work instructions. He argues that to have professional operators, it is necessary to respect their professionalism and not to instruct them in matters in which they actually are the experts.

This aspect of instruction focuses attention on the characteristics of communication among experts within an organization and its influence on safety.

Experts in work apply different levels of cognitive control of their activity, depending upon the degree to which the work situation is familiar to them. This opens another example of the problems with analysis of system behavior by decomposition into sequences of decisions and acts. In traditional decision research 'decisions' have been perceived as discrete processes that can be separated from the context and studied as an isolated phenomenon. However, in a familiar work environment actors are immersed in the work context for extended periods; they know by heart the normal flow of activities and the action alternatives available. During familiar situations, therefore, knowledge-based, analytical reasoning and planning are replaced by a simple skill- and rule-based choice among familiar action alternatives, that is, on practice and know-how. When, in such situations, operational decisions are taken, they will not be based on rational situation analysis, only on the information which, in the running context, is necessary to distinguish among the perceived alternatives for action.

This discussion demonstrates how the form of information needed to control actions depends upon the level and mode of competence brought to work by the actors. A closer look at the concept of competence will therefore be taken in the following sections. It is useful to distinguish between cognitive and meta-cognitive competence.

The cognitive competence includes all forms of knowledge about the work space that is used to control actions, represented explicitly in terms of a model of the functional properties of the work space, or implicitly in terms of know-how, practices, or manual skills.

The *meta-cognitive competence* includes the 'style of work' adopted by actors, a kind of working culture depending on factors such as 'cognitive style' and 'management style'. When the primary goal of work and its cognitive requirements are satisfied, many degrees of freedom in work performance still exist which must be closed by situational and subjective performance criteria, such as risk of failure, work load, time spent, or social acceptance. An actor's priority ranking of such criteria depends on a kind of 'cognitive style'.

10. Colas. A. (1994): *A New Stage in Improving the Operating Safety and Performance of Edf's Nuclear Power Plants by Enhancing Professionalism and Developing the Safety-Quality Culture.* Tech. Report, Version 4. EDF Nuclear Power Plant Operations – Human Factors Group

In his discussion of *professionalism*, Colas makes a similar distinction, quote:

> Fundamentally, professionalism aims to make actions more reliable by implementing appropriate work methods. These more thorough methods refer to intellectual activities (analysis, diagnostics, choice of appropriate responses, etc.) and to "culture" (perception and value accorded to safety and production) and, consequently, to the willingness to act in a certain way, which in turn flows from a state of mind, attitudes and behavior.

For the formulation of the principles for implementation of professionalism, it is therefore argued that two different aspects should be considered separately, quote:

- Knowledge, learning or know-how in its technical dimensions and conditions for taking action in order to provide a technically viable response.
- The appropriate methods and attitudes which ensure that this technically satisfactory response corresponds fully to the quality and safety requirements imposed by our industry, which are adapted to the organization of our activities.

In the following paragraphs, these two aspects of competence are reviewed with reference to the Skill-, Rule-, Knowledge-framework.[11]

7.5.2 Competence at the Skill-based Level.

During familiar circumstances, sensory-motor routines take care of the direct control of integrated patterns of movements. The flexibility of skilled performance depends on the ability to compose from a large repertoire of such movement patterns the sets suited for specific purposes. The individual patterns are activated and chained by perceived patterns that are acting as signs, and the person is not consciously choosing among alternatives.

Competence at this level thus is achieved by development of a repertoire of dynamic behavioral patterns that are synchronized effectively with the behavior of the workspace. Behavioral optimization is guided by criteria such as speed and smoothness, and how far this adaptation can be accepted is only indicated by the once-in-a-while experience gained when crossing the tolerance limits, i.e. by the experience of slips. At this level, therefore, expertise depends on a speed-accuracy *trade-off* and 'errors' have a function in maintaining a skill at its proper level.

Cognitive aspects of this competence include the repertoire of sensori-motor patterns with a scope and flexibility necessary for smooth and fast use of tools and equipment relevant to a particular profession and work place. They serve quick navigation in the work environment and identification of work items. This competence includes the ability to organize routine movement patterns into integrated patterns, synchronized with a wide variety of work situations.

Meta-cognitive aspects includes a sensitivity to detailed features of the environment thus enabling the detection of minor changes calling for modulation of the behavioral patterns. Furthermore, professionalism includes an intuitive sensibility that will interrupt subconscious, skilled performance, when resort to conscious choice or situation analysis is required.

Communication with the work environment at this level depend on perception of *time-space signals*, serving to update and synchronize behavior with the task space, as well as perception of the 'body-language' of collaborators during shared tasks.

7.5.3 Competence at the Rule-based Level

Once in a while, direct chaining of motor patterns is not possible, because two or more familiar patterns apply to the immediate situation, in which case cognitive control is switched to the rule-based level.

An actor immersed in his work is typically well synchronized with his environment. He is familiar with the situation and only have few options for action at any given time. Consequently, an expert will only need to look for the information necessary to distinguish between these few options, and he will develop a repertoire of cue-action correlations. Therefore he needs not consult the complete set of defining attributes before acting in a familiar situation. Instead, guided by the path of least resistance, he will seek no more information than is necessary to discriminate among the perceived alternatives

11. Rasmussen, J. (1983): Skill, Rules and Knowledge; Signals, Signs, and Symbols, and other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics. Vol. SMC-13, No. 3, 1983.

for action in the particular situation. Therefore, when situations change, e.g., due to disturbances or faults in the system to be controlled, reliance on the usual cues that are no longer valid may lead to error. Again, a *trade-off* takes place: Speed versus the risk of a latent change of context that may make the actor's know-how obsolete.

The *cognitive competence* at this level includes 'know-how', that is a large repertoire of cue-action sets matching a wide variety of work situations and tasks. Furthermore, professional actors should have a high sensitivity to secondary situational features that indicate the presence of invalid cues and a need for a situation analysis at the knowledge-based level.

The *meta-cognitive aspects* at this level include a proper balance among the performance criteria, such as speed, workload, and risk of failure together with a high sensitivity for secondary cues that indicate changes in the familiar cue-action set. This involves a high degree of flexibility to avoid fixation on normal procedures – an important item for simulator training. This competence also includes social skills in teamwork and sensitivity to competence and information needs of colleagues.

Communication at this level serves to control a sequence of actions. When operating on a physical workspace, an actor will select convenient cues from the information available. When cooperating with other actors, this also takes place, but in addition, the information available will depend on the formulation of messages by the other actors.

During collaboration in a professional team, an actor will be very well aware of the options for action facing a colleague and he will be familiar with the competence of his colleagues. In that case, he will very likely only communicate the information, he finds adequate to resolve the choice among the assumed options of the colleague. Observations of the communication within professional work teams in transportation of hazardous goods have shown that very little information is actually exchanged, as long as work conditions are normal. Functional information is only discussed when it is realized that changes has taken place or that demands are unusual. This change is then followed by a shift to knowledge-based control of activities.

7.5.4 Competence at the Knowledge-based Level

When situations are met, for which know-how is inadequate, control moves to the knowledge-based level, based on deduction of rules by means of a mental model. Faced with an unusual situation, a hypothetical explanation is formed and tested conceptually before action is taken. The result of the ultimate action is a test of this hypothesis. The question then is when to stop thinking and start action? The answer depends on a *trade-off* between delays due to indecisiveness and the risk of a premature decision. This trade-off depends on many subtle situational factors that usually cannot be made explicit at a later point in time. In case of an unsuccessful result it is likely to be judged a decision error, even when the decision was quite rational, given the local circumstances.

The *cognitive competence* at this level is related to the extend and quality of the understanding of the relational, causal structure of the work system, that is, a correct mental model of system function, and to the knowledge about system goals, safety conditions and regulatory constraints on performance, etc.

Also important is the ability to perform mental experiments to generate rules for action toward a certain goal and to test hypothesis about the cause and effect of abnormal system behavior. Finally, knowledge about information sources, manuals, textbooks, diagrams and the ability to use them belongs to this level.

To the *meta-cognitive* aspects belong proper ranking of production versus safety criteria guiding trade-off during ambiguous situations, including sufficient 'cognitive awareness', that is, the use of basic understanding to monitor system performance also during routine conditions and thus be sensitive to changes.

Communication. The cognitive competence is very much related to the ability to interpret the *content* of communications and observations with reference to the use of a functional, relational model of the work content.

The meta-cognitive aspects of competence required for cooperation relates to the *form* of communication, such as care when formulating messages, and not to use rudimentary short-hand messages during periods of change. Important is also the extend to which feed-back to cooperators is maintained to verify performance. Short-hand messages in cooperative context are analogs to convenient cue-action relations in direct interaction. There is, however, one important difference. Formulation and reception of short-hand messages depend on the mutual perception of competence of both the sender and the receiver. Differences in their meta-cognitive competence, or in their mutual perception of

the partner's level of competence, are likely to lead to misinterpretation, unless the feedback verification mentioned is active.

7.5.5 A Note on the Nature of Human Error

It follows from this discussion that 'human errors' reflects a kind of speed-accuracy trade-off at all three cognitive levels of decision-making. Therefore efforts should not be spent on removal of human errors that just indicates experiments on the boundary of acceptable performance. Instead, attempts should be made to make the boundaries visible and reversible and to give decision-makers the opportunity to learn to cope with the boundaries. Experts on the run in a dynamic environment often make many more errors than are cautious and slow novices. As Hadamard, the French mathematician states (quote):

> "– in our domain, we do not have to ponder with errors. Good mathematicians, when they make them, which is not infrequent, soon perceive and correct them. As for me (and mine is the case of many mathematicians), I make many more of them than my students do; only I always correct them so that no trace of them remains in the final result. The reason for that is that whenever an error has been made, insight – that same scientific sensibility we have spoken of – warns me that my calculations do not look as they ought to".[12]

Rather than to study errors, we ought to focus on strategies to recover from unsuccessful explorations.

7.6 Awareness

Even when decision-makers have the necessary information and competence their risk management will not be effective if they are not aware of the need to consider the potential risk involved in their decisions. As discussed in previous sections, decision-makers are not subject to input of information from the environment, they actively seek the information they need to act. They only look for cues to discriminate among the perceived normal options for action and need to be prompted to also consider the effect of the side effects of their decisions.

The influence on risk management of experts' adaptation to the normal features of their work conditions and their reliance on intuition about the competence of their colleagues is demonstrated by Hopkins' analysis[13] of the decision making of the management of the Moura mine in Australia.

The mine company was under considerable pressure due to a contract to deliver coal to a new power plant from its fixed start-up date. This influenced the performance criteria of managers and a number of unsafe decision making routines evolved, leading to an explosion:

- A tendency to discount unwanted evidence evolved: A culture of denial. It was generally believed that there was no significant risk and given the production pressure there was a strong tendency to dismiss any contrary evidence. This may reflect the fact that experts do not base actions on a situation analysis, but on convenient cues.
- A hierarchy of knowledge was instituted and knowledge based on personal experience was far the most influential, while information acquired by word of mouth was more influential than written information. This was not just a practice; it was a policy, spelled out in the mine's Quality Assurance system. The mining procedures had not been considered by the manager-in-charge, even though he was responsible for the underground procedures. He considered them just to reflect what was already happening in the mine. This may reflect the condition that important messages may be lost when embedded in information that is already part of the receiver's normal, professional competence.

Several observations seem to be related to the adoption of rudimentary communication within a team of experts, and to the difficulties in actually shifting to the level of knowledge-based communication:

- Managers at the levels above did not pay much attention to the reports of their deputies. It was generally expected that important information would have been communicated orally.
- When the decision was taken to seal the mine section earlier than initially intended, none of this information was conveyed to miners or deputies. The manager assumed that everyone had been informed via the 'grapevine'.

12. Hadamard, J. (1945): The Psychology of Invention in the Mathematical Field. Princeton Univ. Press. P. 49.
13. Hopkins, A. (1999): Managing Major Hazards: The Lessons of the Moura Mine Disaster. St. Leonards, Australia: Allen and Unwin.

Similar communication patterns are found in other organizations involved in major accidents, see[14] the court report of the Zeebrügge and Clapham Junction cases.

Some conclusions can be drawn for design of information systems. Considering the nature of naturalistic decision making:

- Decision-making cannot be studied separate from work context and actor competence.
- Experts are deeply emerged in work context and the alternatives for action are intuitively determined by the work context.
- Only information necessary to choose among perceived alternatives is consulted.
- Managers are running risk, not taking risk, and very likely during non-risk related decisions.

These features of expert decision making have important implications for the use of available information:

- Experts in their normal work situation need only little information to choose among their options for action.
- They actively seek the information they need, and they know where to look for it.
- Therefore, they don't read messages, they don't think they need.
- They don't see messages embedded in text they think they know
- To communicate effectively, you must know the form and content of the operational competence of the actor and not hide important messages in well-known information

Also the communication among collaborators depends heavily upon the perceived expertise of colleagues:

- Team experts know the competence of colleagues, they don't tell them what they expect to be known.
- They know colleagues' options for action, and in messages only give cues for choice between them.
- In short, expert teams rely on 'short-hand' messages during normal work and shift to functional communication during change must be prompted.

In conclusion, special care in the design of the information environment of decision-makers is necessary to prompt their risk consciousness during normal work conditions.

7.7 Commitment

Even given the right conditions so that they *can* make appropriate risk management decisions, an additional question will be: *will* they actually perform adequately? This question raises a number of basic, local issues that relate to the performance criteria and subjective preferences of the various decision-makers. One is whether the priority ranking of operational and safety objectives of the various decision-makers corresponds to an effective risk management strategy.

At the company level, this question relates to the proper social control of management commitment by legislation. This has lead to policies imposing greater penalties (even criminal penalties) on the company if it violates the rule and the violation occurred because it did not use a good internal management system assuring proper implementation. Key aspects of this policy are focused on effective management systems including company commitment (internal policies and resource commitments), employee training, internal auditing, and quick and voluntary correction of deficiencies (as outlined by ISO, EMAS, etc.).

The problem of commitment is basically related to the very different planning horizons of different decision-makers at the various levels of the socio-technical system. Management is legally responsible toward the board of shareholders that decisions are economically sound within the time horizon of the annual report. The personal career planning horizon of a young CEO will probably be a few years, while the financial corporate horizon is of the order of magnitude of a decade. However, risk management must be planned to reach a predicted mean time between major accidents in a particular installation up to 10^4–10^5 years. No wonder that management will violate the latter request during a period of financial crisis.

7.8 Design of Work Interfaces

Based on these requirements to information systems for support of pro-active risk management some characteristics of interfaces can be suggested to support actors' adaptation effectively and safely to a dynamic work environment. These

14. Appendix A1 & A2.

requirements lead to the design of 'ecological information systems'[15] as mentioned in section 6.2.4.

7.8.1 The Conceptual Content of a Display

The conceptual content of a display interface should faithfully represent the functional structure of the work system, that is, the causal and intentional constraints governing the response of the system to actions. To plan when and how actions are called for, the actual state of the system with reference to this constraint pattern should be displayed. This information can be defined at all the various levels of a means-ends representation, each having its own particular formulation depending on the related source of regularity. To support actor adaptation to changing work requirements, it is important that the actor is free to seek information at all the means-ends levels of representation and at several levels of structural decomposition as the actor's formulation of the task and span of attention changes.

Within this context representation, information should be given on the actual state of affairs, the target states, and the boundaries of acceptable operation. As mentioned, such 'ecological' displays are presently developed for control of technical systems, and research on displays for case-handling is underway.

7.8.2 The Scope of the Interface Representation

It goes without saying that the interface should represent the part of the work system controlled by a particular actor. Its is, however, important to realize that an actor may need to get information about the part of a shared work domain that is controlled by collaborators.

In team collaboration it can, as mentioned, be important for successful operation to 'have an eye' on the activities of other team members. In a more sequential sharing of activities, information about the activities of other actors (including designers and planners) at previous points in time, including the conditions of actions and the objectives and criteria underlying their decisions must be available.

7.8.3 Transformation from Relational to Causal Representation

The optimal state of operation of a work system and the coordination of functions serving a given production target are determined by quantitative relations among physical or economic variables. In consequence, important information systems are often designed to make it possible during operation to ensure that these quantitative relationships are optimal. That is, databases and decision support systems reflect the quantitative, relational models underlying analytic process optimization.

In contrast, the natural language reasoning applied by human decision-makers depends entirely on a causal model in terms of objects in a background interacting through events. Therefore, the quantitative variables and the relational structure governing their interaction must be converted at the interface to a set of symbolic objects interacting through events in a virtual environment. The interface therefore should present a map of a symbolic landscape inhabited by objects – icons – representing states of processes, interacting mutually and with boundaries around territories of varying operational significance. This is important, not only to support the reasoning by an individual user, but also to give cooperating users an opportunity to point at and to discuss an external model.

An important interface design issue when choosing the *form* of the presentation therefore is to integrate the raw measuring data into higher level objects, states, and events that match the conceptual language and the level of abstraction applied in the users' causal reasoning.

7.8.4 The Form of Display Representation

With regard to the visual representation used at the interface, two aspects are important. One is, that representations should be available that match the different levels of cognitive control that will be activated, depending on the familiarity of the situation to a particular actor. Another is the need to present information in the causal and intentional context to prompt a switch from know-how to functional reasoning in case of changing conditions. Thus a visual coding of the display

---

15. See e.g., Rasmussen, J. (1999): Ecological Interface Design for Reliable Human-Machine Systems. In: Gavan Lintern (Ed.): Special Issue on Display Design, Journal of Human Factors in Aviation. Vol. 9; Nr. 3; 1999; pp 203–225.

    Flach, J. M. and Dominguez, C. O., (1995): Use-Centered Design: Integrating the User, Instrument, and Goal. Ergonomics in Design, July 1995, pp. 1924.

    Vicente, K. (1991): Supporting Knowledge-Based Behavior through Ecological Interface Design. EPRL-91-01. Toronto: University of Toronto; Engineering Psychology Lab.

should be chosen to support the interpretation at three levels of cognitive control.

For *knowledge-based reasoning* the display should serve as a faithful, externalized mental model to support mental experiments. Therefore a display should be based on a truthful representation of the functional structure of the workspace. It should not be a 'user-friendly' design based on user involvement. A faithful functional representation is important to maintain a reliable mental model even during adaptation to daily routine. For this reason, and to avoid conflict, the visualizations that have evolved through time for explanation of concepts to novices by illustrations in manuals and textbooks should be consulted.

For *rule-based action* during familiar situations, the interface should allow formation of convenient, but reliable cue-action responses. Evolution of cue-action responses during familiar situations cannot be avoided, but the design should show cue in context to support situation awareness. For this, a display should integrate in a consistent way all the behavior relevant constraints in a work situation into a perceptual pattern, that is, it should include all relevant attributes with respect to effective actions. In other words, emerging cues for action should be complete, if not, it will very likely lead to the kind of under-specified action cues known from the traditional one-sensor-one-indicator technology.

Finally, the spatial-temporal characteristics of the display should support skill-based operation, that is, the spatial-temporal control loops must be intact through the interface mediation. This is probably particularly important for vehicle control.

Presentation of information in the situational context is important to prompt awareness of changes in work conditions. Since experts are asking very focused questions to their work environment the answers should be found immersed in a defining context. Again, a composite configured representation is to be preferred for a sequential text interface to counteract the tendency to seek 'short-hand' messages.

In conclusion, information systems need to be designed so that they can adapt to the requisite variety of natural work domains. The human variability that was "error" with respect to the designers' task analyses can be a source of stability within an adaptive system. This operator variability reflects a capacity of human operators to respond creatively to shifting contexts. This ability reflects an internal rationality (or eco-logic) that provide a more robust solution than the brittle rationality underlying the designers conception of the single "best-way".

7.9 Auditing Scenarios: Examples

An important element of organizational auditing will be an evaluation of the completeness and consistency of the information flow of an organization. This evaluation therefore is closely tied to an abstract, functional representation of the vertical flow of control information as required by a potentially hazardous process at the bottom of the socio-technical system, figure 7.7.

An audit is therefore made with reference to the information flow requirements of a consistent safety control function as outlined in chapter 4. To guide this information flow auditing, the sketchpad of figure 7.8 is used in the following discussion. The figure is based on figure 7.7 and reflects the fact discussed in chapter 4 that global company objectives at the lower levels have to be supplemented by locally derived decision criteria. The figure therefore is divided into three vertical columns. One (the right hand column) reflects the communication of state information and normal operational objectives within the operational organization. The center column represents the communication of objectives and targets downward the organization. The left hand column reflects the additional, safety related references and criteria which are not communicated downward the normal work organization, but communicated from external sources such as technical descriptions from design, definitions of preconditions for safe operation from risk analysis, together with laws and regulations.

The 'prototypical hazard scenario' is defined at the bottom of the diagram, with reference to a particular hazard source and its control requirements. It presents a brief verbal label, and the 'critical event' defining the scenario is stated. The target of the safety control strategy is indicated by the position of the arrows. Rest of the diagram specifies the information about the actual state of affairs propagating upward, the information of objectives propagating downward, and the information on system information and supplementary decision criteria inserted side-wards in the organization. The transformation and re-interpretation of information necessary to make the information operational should be reflected in the

description at each level. In other words, the analyses should highlight whether formulation of state information is comparable to information on objectives to judge correspondence, and criteria should immediately relate to the topics of operational decision making.

In the following paragraphs, two prototypical accident scenarios are discussed with reference to industrial process to demonstrate that quite different information flow requirements can be found for different scenarios within the same system.

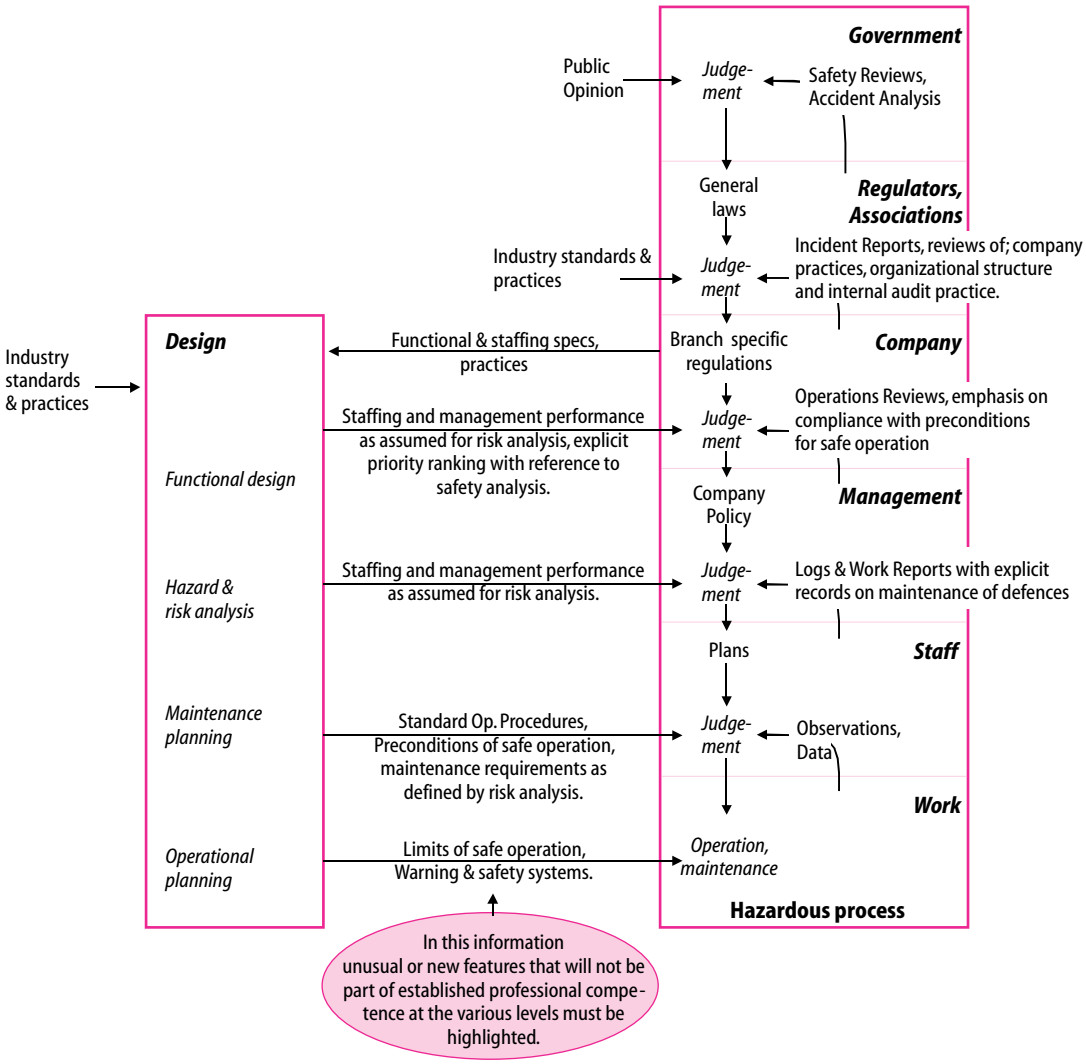


Figure 7.7 illustrates the structure of the information flow necessary for a safety control based on a predictive risk analysis.

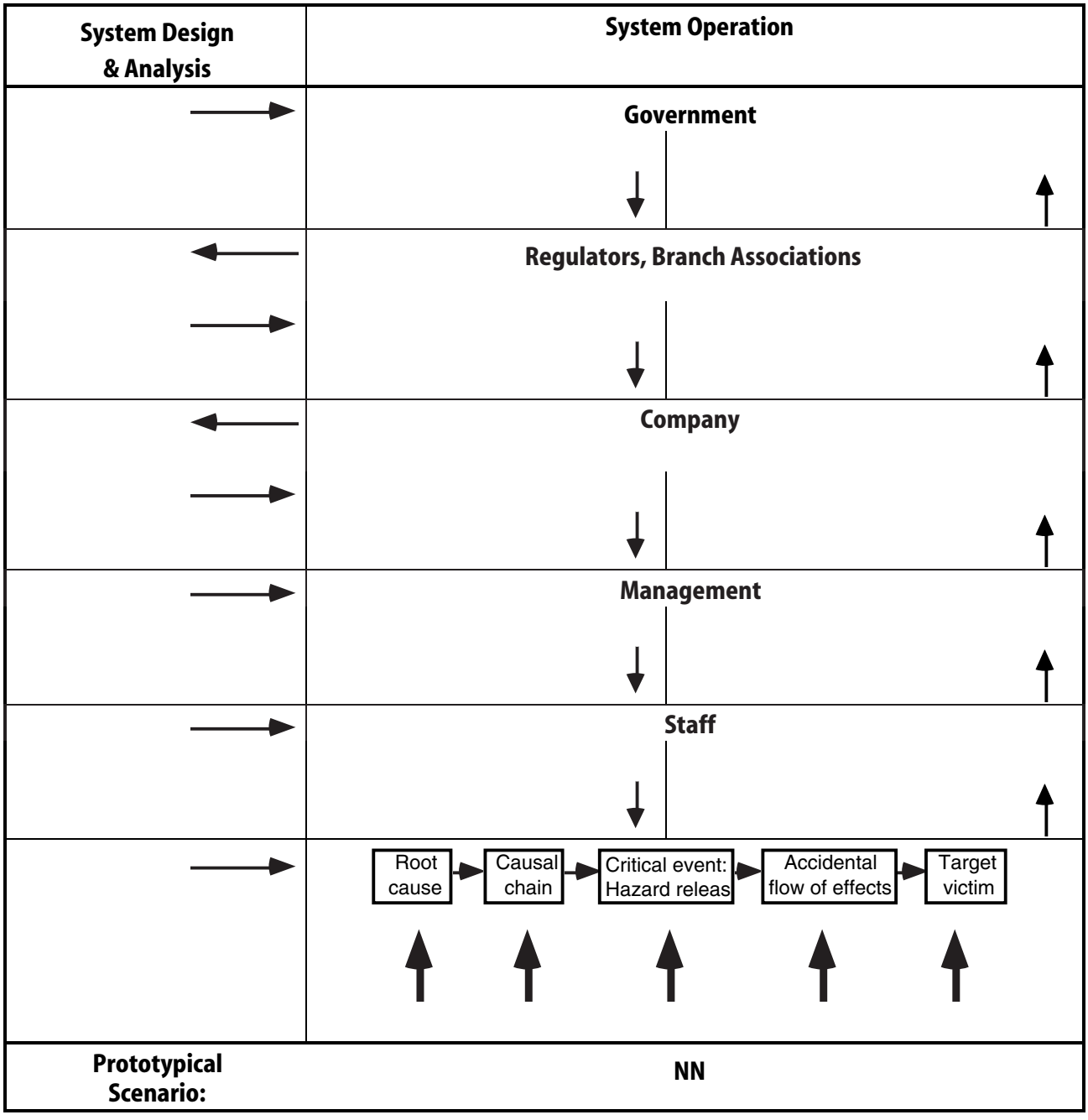


Figure 7.8. A sketch pad for representation of risk management strategies in a particular work system.

7.9.1 Process Plants

The process plant example is divided into two 'prototypical scenarios'. One is protection against major accidents during normal operation with automatic protective systems. Another is protection of continuity of operation against spurious shutdown due to interference with operation during normal control and maintenance activities.

Figure 7.9 reflects the kind of information flow required for a consistent safety control function according to strategy C.3.1. The information descriptions are only intended to be illustrative. More specific information is needed in an actual case, for instance identifying standards and regulations by name and numbers, and the actual reporting forms and sheets by examples. This however can only be done from interviews with the staff of a particular plant.

Figure 7.10 reflects the audit sheet for protection of continuity of production. In this case, side-wards, external information input normally is less influential, even if input from system designers become increasingly important due to a fast pace of technological change. Also the involvement of the higher level of society is less pronounced for this scenario.

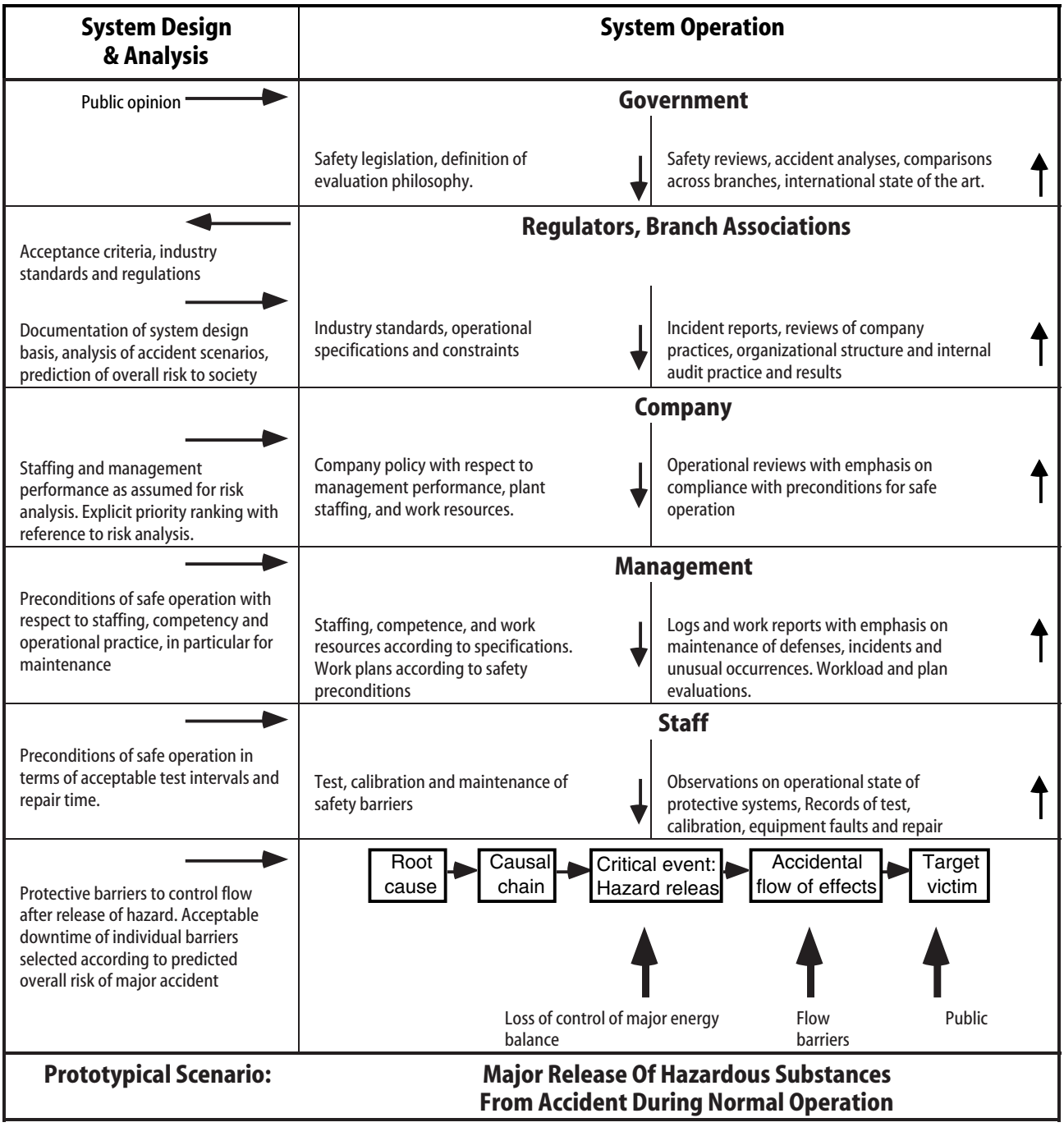


Figure 7.9. An auditing format related to major accidents in a process plant. It is only intended to be illustrative with respect to the difference between protection against major accidents, and protection against loss of continuity of production, see figure 7.10

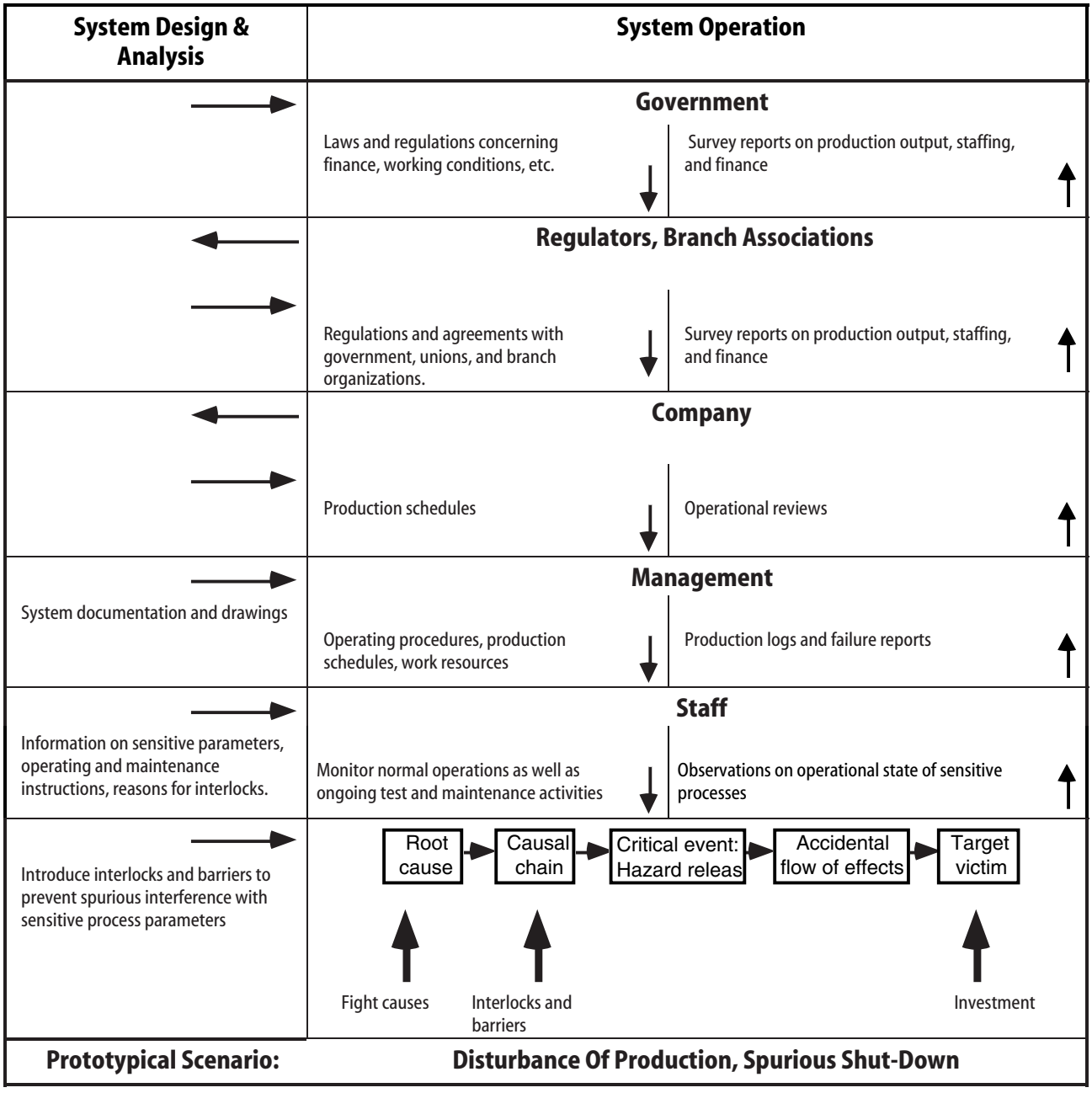


Figure 7.10. The figure illustrates the information flow related to protection against loss of production in an industrial process plant. The difference in information flow shown in figures 7.9 and 10 demonstrates that a good production record does not, as often stated, demonstrate a high level of safety.

8. Risk and Quality Management Approaches

The risk management organization and strategies suggested in the previous sections turn out to be very analogous to the Total Quality Management (TQM) concepts defined by the ISO 9000 standard and elsewhere. In fact a method, in which risk management and TQM is integrated to promote safety and accident prevention, has been developed and tested in two Swedish municipalities in 1992–1998. The method and tools implemented are assessed to be useful and to result in some safety improvements[1]. To ensure an effective and transparent quality management, a feedback control system is specified by ISO and each of the system requirements defined above are explicitly considered.

Here only a tentative comparison of the two approaches will be given, based on a brief review of recent publications. In several respects it appears to be realistic to include *process safety* as a quality parameter in a TQM centered organization. This is so because TQM and the risk management (RM) organization suggested here share several very basic requirements:

- As it is suggested for proactive risk management, TQM is the responsibility of the entire line organization, not of a separate office.
- In both cases, reactive strategies are replaced by proactive approaches. In TQM, quality control by product inspection and selection is replaced by control of product- and process-design following the work of Deming and the Japanese experiences.
- ISO 9000 does not prescribe a standard organization, but aim at the introduction of a quality management system that is matched to the characteristics of the particular production system. In that sense, it is focused on a 'vertical slice' in figure 2.1.
- Finally, TQM is organized so as to be transparent to an independent evaluation and certification body, in a way very compatible with the approach to regulatory auditing that will be required when safety legislation change from prescriptive to performance based approaches.

In the following paragraphs, a brief comparison of the two approaches with respect to the system requirements listed in the previous paragraphs will be given, based on a tentative consultation of the literature.[2]

Identification of Decision-Makers. The ISO standards call for a very careful identification of the individual actors involved in quality management among executive managers, employees, customers, suppliers, and independent certification auditors.

Allocation of Roles. One of the explicit concerns of TQM is the identification of distinct functions to achieve the different tasks of the organization, in order to prevent activities to fall into cracks between the attention of decision-makers or actors. An attempt must be made to ensure that individuals feel 'ownership' of the various functions to ensure proper commitment to quality.

Identification of the Control Structure. ISO item 4.1 concerns the responsibility of the executive management in regard to quality policies and the implementation of a quality management system.

Flow of Control Information. Central to the TQM concept is an explicit definition of quality characteristics and efforts to ensure the communication downward of policies, criteria and specifications as well as the upward communica-

1. Rosenberg Tommy (1998) "Risk and Quality Management for Safety at a Local Level", Royal Institute of Technology, Stockholm, Sweden
2. W. A. Stimson (1998): Beyond ISO 9000: How to Sustain Quality in a Dynamic World. New York: American Management Association.
   R. Joss and M. Cogan (1995): Advancing Quality: Total Quality Management in the Public Health Service. London: Open University Press.

tions of observations about product and process qualities and variations. Definite specifications of accountable records and documents are given to enable inspection and evaluation by executive management as well as independent accountants.

Controller Capability and Awareness. All ISO standards are concerned with the capability of the TQM system, both with regard to allocation of adequate resources and the competence of the managers as well as the employees. ISO item 4.18 specifies training courses to ensure proper competence with respect to quality management and allocation of resources.

Controller Commitment. ISO item 4.1 explicitly mention the importance of the commitment to quality management and to maintenance of the proper TQM system.

8.1 Certification

Certification is a form of auditing process to be performed by independent accredited bodies to demonstrate and certify the fulfillment of rules or demands, as stated in management standards, within the scrutinized organization. The process is based on extensive checklists addressing conditions that are considered to reflect the presence of a proper management system. One idea of the quality and environment standards, and much of the explanation of the success of their implementation, is that the quality management of one company or organization can get credit from the fact that its suppliers and contractors are certified according to the standards. Organizations therefore, as a part of their purchase routines, call for such certifications, thus creating a strong economical incentive for the management standards to spread.

8.2 Conclusion

In conclusion, the concepts applied in present TQM systems match very well the feedback control concepts suggested here for proactive risk management. In the TQM handbooks reviewed, control-engineering diagrams are typically used to illustrate the process and functions involved in the various TQM tasks, but in a rather inconsistent way, that is, they are merely illustrative examples. This is very likely a consequence of the general nature of the discussion. As mentioned, ISO recognizes that TQM organizations should be developed to match the individual productive systems. Therefore, the TQM organization will be a formalization of the line organization involved in the production management. A proactive risk management structure can probably be designed from an established TQM organization by explicitly defining 'safety quality' measures related to the production process from an explicit formulation of the precondition for safe operation. This will serve to supplement the TQM control of the company's products and services.

Two observations influence the merits of the ISO management standards as they are presently implemented. One is the fact that the bodies accredited to perform the certifications are not truly independent since they operate on a competitive market as contractors to the organisations seeking to become certified. This problem is regarded as one of the contributing factors behind defective safety found in the shipping industry, se the "Map of conflicts among actors in shipping" in figure 2.2. A company can be certified according to the standards primarily by demonstrating documents regarding formal organizations and routines, while the auditor is addressing neither judgements regarding their appropriateness nor the implementation of them. Hopkins states[3] that in the case of a mining company "the QA auditing system in operation was largely confined to checking paperwork".

The other observation is that it is primarily when there are direct economical implications for reporting deficiencies, in order to get economical compensation from a third part, that such reporting procedures are in operation. Also in large companies proper feed back routines are missing, routines that are of such vital importance to the management process.[4]

These shortcomings are likely to appear in any management system and they illustrate the need for proper processes to secure resources, competence and commitment if and when TQM organization is considered for proactive risk management.

3. Hopkins, A. (1999): Managing Major Hazards: The Lessons of the Moura Mine Disaster. St. Leonards, Australia: Allen and Unwin.
4. Brombacher A.C., Relation between product reliability and quality of business processes: New trends in reliability management, Safety and Reliability, Vol. 1, Ed. Schueller G.i. & Kafka P., A:A:Balkema, 1999.

9. Tool for Accident Analysis and Organisational Audit

Many actors of different background and with different roles participate in societal risk management. Many of them may be involved in collecting explicit data regarding direct and indirect causes of accidents, their consequences, the preconditions affecting the event and the process by which the accidental circumstances has been dealt with. Also in auditing, persons with different competence, experiences and roles in the system are active. The tool for data collection and analysis discussed here therefore will have to serve many actors and purposes. The discussion below is a description of an outline of such a tool and the experiences gained from a prototyping experiment.

The suggested tool is based on a hierarchical query tree, guiding the analyst to ask questions top-down from the general picture to detailed questions concerning the decision behaviour of individual decision makers. Facilities should be included that give analysts access to documents, procedures, regulations, etc., relevant for different accident categories (as identified from prior cases and auditing). In addition, facilities should be given to retrieve information from the database of the home agency by calling information from 'similar cases' at the different levels of the search tree. Finally, there should be facilities that allow automatic printout of an accident report in predetermined formats for the different services, when all relevant information is entered in the questionnaire forms.

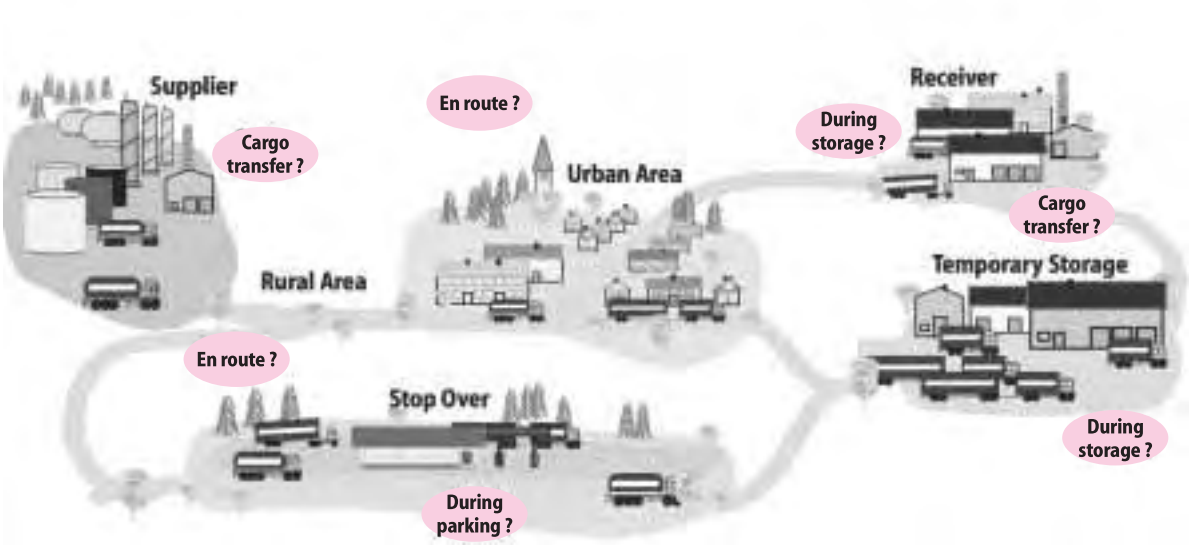
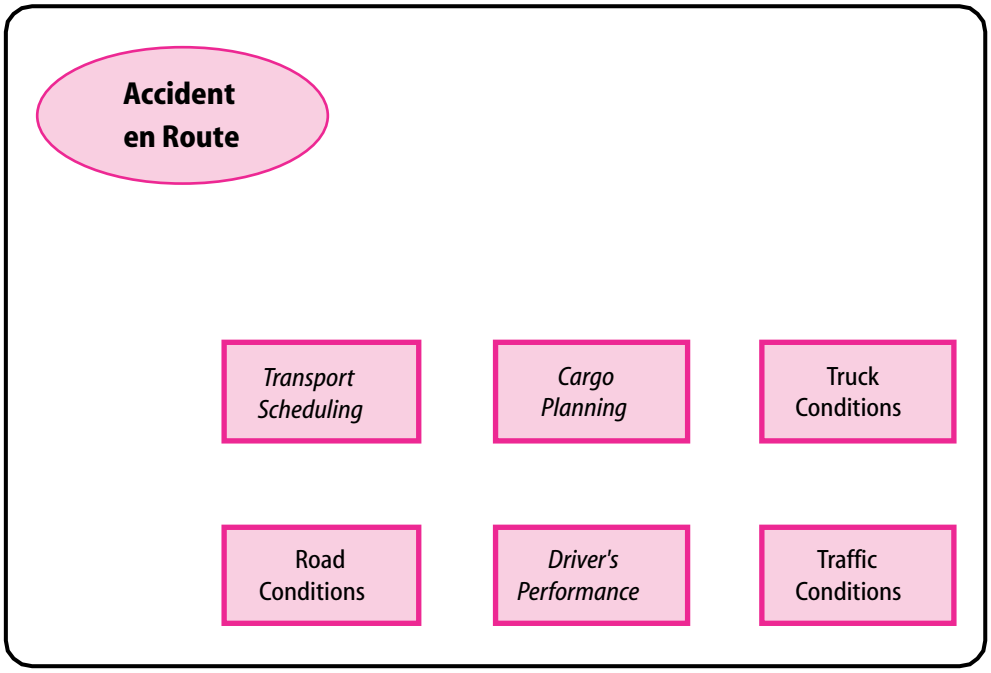


Figure 9.1. For description of an accident scenario or for auditing a transport function, "click" on the relevant coloured function knob, then page 2 comes up.



Page 9.2. This page lists the relevant transport functions for the location selected on page 1. When to make a detailed description of the pre-conditions behind a certain accident or when auditing details of a system's performance, click on the relevant function(s).

What information that is regarded relevant depends on the context and the current analyse level, how deep into the pre-conditions of an event one is searching.

The basic structure behind the query tree is a 'generic AcciMap'. A generic map represents the causal course of events and the decision situations involved in the creation of this causal flow. Such a map is related to a category of accidents, relevant for the analysing agency, such as 'transport of dangerous goods', 'major accident in process industry', or 'major fire'.

To guide questions from the global picture to the detailed conditions of an accident, a systematic, top-down breakdown of an AcciMap to identify 'causal sub-trees' should be possible. To facilitate such a structured breakdown, the generic map should be organised in a systematic, modular structure.

9.1 An outline of a Tool

9.1.1 Entrance to the Guide

The guide is entered through an opening page, which displays different situations that involve different control structures in the handling of the hazard source in question and different actors in the control. For transport of hazardous goods for instance, the mode of transport (road, rail, sea or air) should be entered first and then the type of situation where an accident may take place. In case of e.g. road transport situations such as handling of goods at the supplier, during transport, and at the delivery station, pose different control requirements and involve different organisations and actors.

The entering page of the guide then represents a general map of the activity. For road transport of dangerous goods such a map is shown in figure 1. The map is formed by a set of 'hazard situations' that matches the sub-trees of the generic AcciMap. How the map is organised and what situations to

include in the entrance figure probably require some iteration to obtain the best decomposition. Figure 9.1 is based on analysis of several cases and the attempts to define a generic map.

The map is useful to structure the approach of the interviewer, to guide the introductory discussion with interviewees, and as an illustration to point at and discuss during initial phases of the interview.

9.1.2 *Definition of Accident Situation*

An active icon presents each situation in a global picture map, as in figure 9.1, and when 'clicked' a pull-down menu or a new guide page (figure 9.2) appears. The items in this menu (page) are chosen so as to give good coverage by a reasonable small number of choices. As mentioned, this depends on the modular design of the generic map and on the basic choice made of 'critical event' for design of the underlying cause-consequence-chart.

9.1.3 *Analysis of Accident Situation*

When an icon/menu item has been activated, a detailed submap appears showing the information flow involved, see figure 9.3. Each node of the tree can be activated to call up a questionnaire, if the analyst finds one or several node elements (situations) to be a significant contributor to the case.

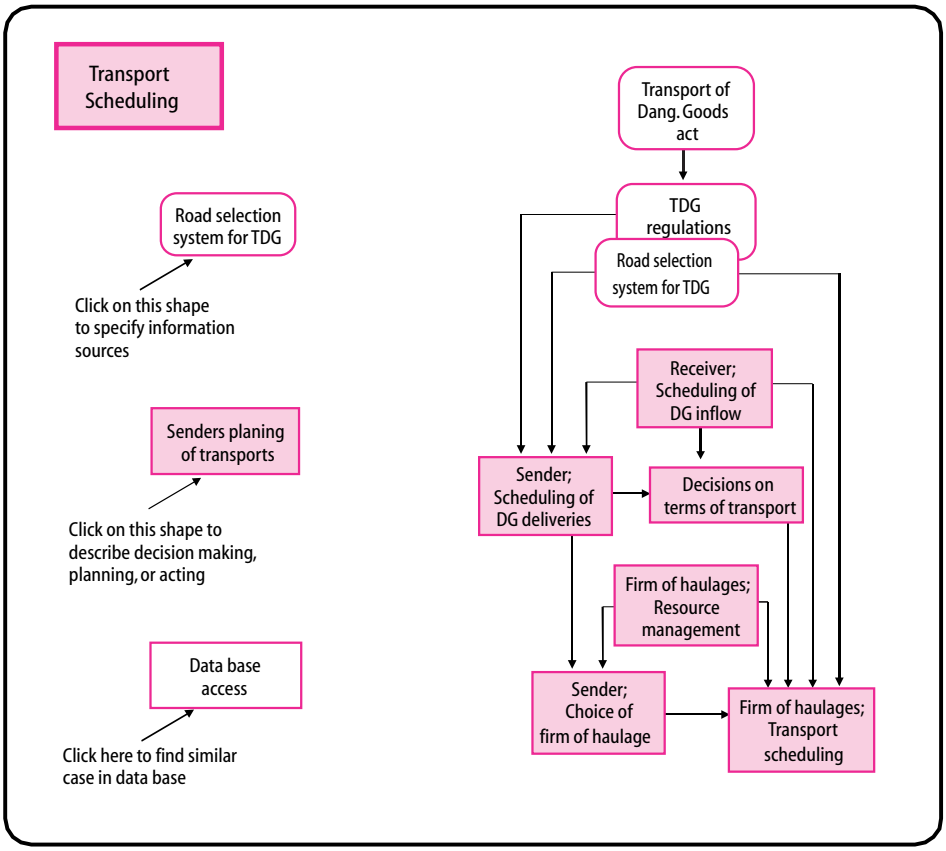


Figure 9.3. For each relevant transport function in figure 9.2, a diagram comes up, representing the planning decisions of the particular case, and the relevant information sources. For all contributing decisions or regulations, a click will generate a page for detailed report, see page 4. The information and criteria used for decision making are not included in this format, but described in detail in the following page(s).

The number of different node symbols depends on the necessary number of interview questionnaire formats and will probably increase when more accident scenarios have been analysed. In the present example in figure 9.3, two types of node are used, one for information sources, and one for decision making (action, planning, etc.). When the number of questionnaires built into the tool increases and the data looked for are more distant from the actual course of events the task of performing the data collection may be transferred to analysts with other backgrounds and roles in the system.

The guide page of figure 9.3 also includes an entry node to the database, to retrieve 'similar cases' from past analyses. Substantial inspiration for penetrating questions can be found by such search for similar cases. Such retrieval facility is connected to each level of the guide, giving increasingly detailed retrieval queries to support fast interaction in fieldwork.

9.1.4 Query Guide

The next level presents a query guide and data-entering interface for each active node of figure 9.3. The number of formats depends as mentioned on the number of node types used. In the present example, a query format is given for information sources (figure 9.4) and for decision-making (figure 9.5–7).

A separate interview page is available for each node at the level above, which makes it possible automatically to enter the data into the proper place of the AcciMap and thus to automatically format the report.

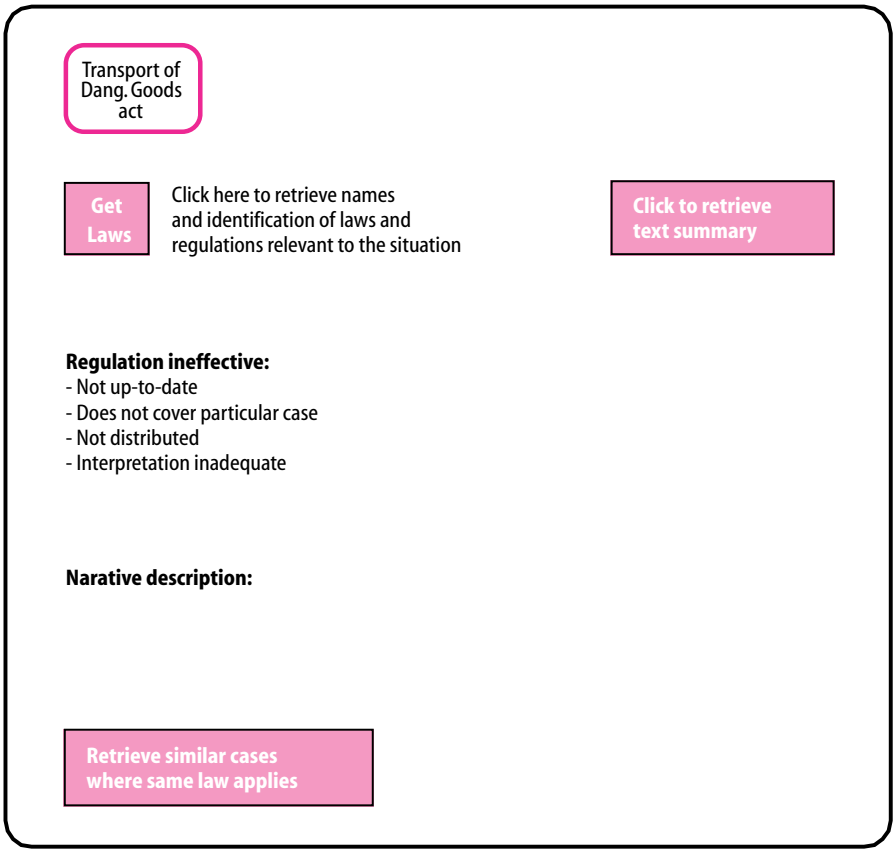


Figure 9.4. A page with a format similar to this is used to describe the conditions of information sources, such as the laws, rules, regulations, and instructions.

9.1.5 *Information Source Questionnaire*

At the information page (figure 9.4), two data retrieval icons are suggested. One for retrieval of formal information sources such as regulations, instructions, work sheets, order formats, etc. This is useful to guide interviews and to enter references in the automatic report.

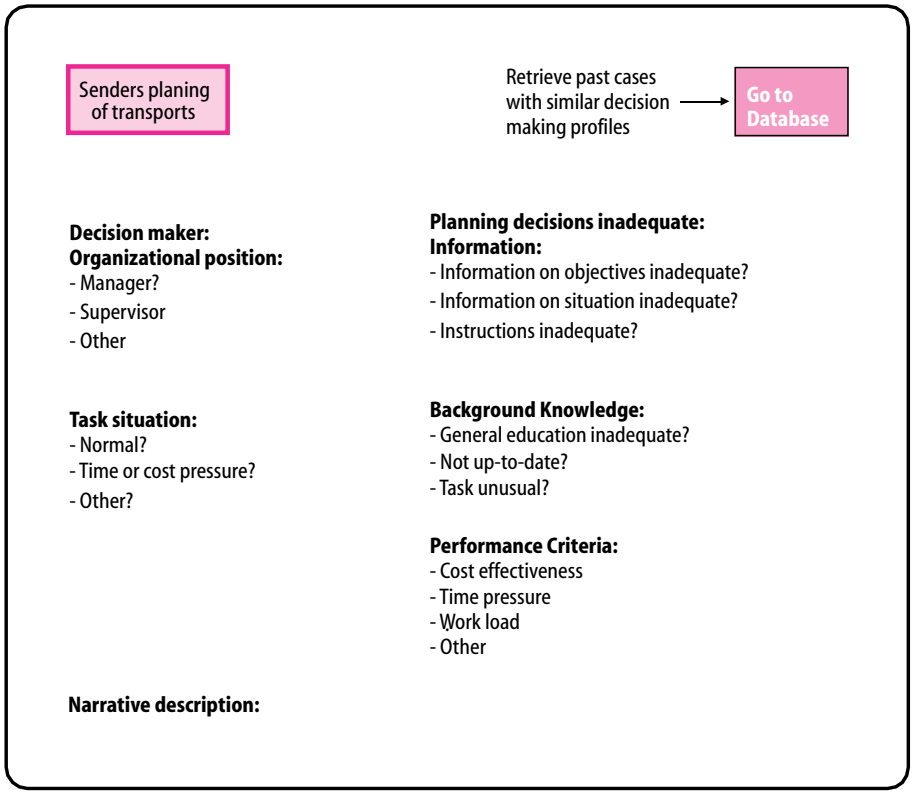
Another retrieval function is a call for 'similar cases' from the home database. When activated at this level, more detailed retrieval is effective, and detail increases, as data are entered into the form.

9.1.6 *Decision Making Questionnaire*

The decision making query guide (figure 9. 5) should assist an analyst to describe the situation of the decision makers involved in the creation of the accidental context, and to explore the information available (or not available) to the decision maker according to the closed-loop structure discussed in section 7. As is the case for other query formats, retrieval of' 'similar cases' from the home agency database is suggested.

Figure 9.5 presents a very general format that may be useful only when investigating higher management levels where decisions very likely are not directly related to the individual case.

At the lower levels, more structured query trees, as proposed in figure 9.6 and 9.7 will be useful. The content and form of such query guides should probably be related closely to the various situations in figure 9.1, and detailed formats should be designed in iteration with coming accident case analysis.



Page 9.5. A page having this format is used for detailed description of each relevant planning decision. For more detailed description of complex situations at the lower levels, see figures 6 and 7.

Road Condition: If contributing then ask:			
1) Temporal conditions, weather influence? (Road impaired by ice, snow, etc.)	Yes: Weather change?	Yes, then terminate	
		No: Inadequate road clearing. Go to local tech. admin. **LTA** (Ref. to person, address, phone number).	1) Preoccupation? 2) Staff shortage? 3) Budget limits? 4) Technical problems?
	No: Road maintenance work?	Yes: Traffic guidance adequate?	Yes: terminate No: Go to **LTA**
	No: Other temporal obstacles?	1) Traffic jam? Yes: terminate.	
		2) Traffic accidents Yes:	Proper traffics guidance? Yes: Terminate No: Go to **POLICE**
2) Permanent conditions?	1) General maintenance adequate?	Yes: terminate.	
		No: Inadequate maintenance. Go to local tech. admin. (Ref. to person, address, phone number).	1) Preoccupation? 2) Staff shortage? 3) Budget limits? 4) Technical problems?
	2) Road configuration adequate?	No: 1) Natural topography?	Yes: terminate.
		2) Road design adequate? No: Go to **LTA**	1) Road layout, Shape surface? 2) Visibility impairment? 3) Safety devices, barriers? 4) Obstacles, boulders, lampposts, trees?

*Figure 9.6. Some of the 'Accident Situation' entries at page 2, at the detailed lower level, such as accident parameters, like 'road condition' or 'driver performance' raises many questions and a guide such as the one illustrated here may be necessary. Experiments should be made to see whether a graphic page or a traditional 'botanical field guide format', as the one shown, will be best. The **BOLDFACE** labels refer to decision questionnaires at LTA: Local Technical Administration and POLICE: Police involvement.*

Truck Driving Performance: If sub-standard then ask:			
Driver Competence adequate; No:	1) General training inadequate		
	2) Unfamiliar vehicle?		
Information to driver adequate, No:			1) Road signs 2) Road maps 3) Warning signs 4) Radio information 5) Technical truck performance inf.
Road selection			
Mechanical Truck Performance	Truck Type unsuitable		
	Truck maintenance inadequate	1) Service Center performance?	Go to Service Center: 1) Budget problems 2) Poor planning 3) Time constraints?
		2) Driver performance	1) Time pressure 2) Inattention
	Use of truck	1) Overload 2) Speeding	
Outside Disturbance? Yes:	1) If road conditions; go to R. C.		
	2) Weather conditions; Yes:	1) forecast exists, driver not informed	
		2) Sudden weather change	
	3) Traffic conditions	1) Road obstruction, accident if yes go to R.C.	
	4)Distraction	2)	

Figure 9.7. A rough outline for a questionnaire related to 'driver performance'.

9.2 Requirements on a computer based Tool

In the previous sections, the structure of a tool is proposed to support data collection and analysis related to accidents and their preconditions. This outline is based on analysis of a number of accidents in the road transport sector and the representation of the generic findings in a generic AcciMap. The actual implementation depends on the database tools applied, and in the following sections the experiences from a prototyping experiment are discussed.

9.2.1 *Structure of Data Collection*

As mentioned in the previous sections, several different persons, from different agencies and with different backgrounds will be using a data collection tool, and they will consider different levels of detail during their analysis. During the planning of the prototyping experiment, the complexity of the database turned out to invite a structuring of the tool into several phases and levels of detail matching the requirements of the different users.

The prototype is therefore designed to support the following phases and levels of analysis, see figure 9.8:

a. "*On the scene*" *data collection and analysis:*
   - a.1 *Direct observations.* This level includes observation of the circumstances of the specific accident, the critical event, the preceding causal flow of events, the immediate consequences thereafter and the rescue actions taken. This phase includes information from interviews on location.
   - a.2 *Judgements.* A more penetrating phase considers the pre-conditions judged to have shaped the course of development events, such as decisions and activities of work planners and equipment designers. This phase may involve other specialists in interviews of planners.

b. '*Follow-up*' *data collection and analysis:*
   - b.1 *Observations;* Supplementary basic information, circumstances, developments and rescue actions as under point A.1 and information on activities such as rest value securing, decontamination of land and property and estimates of long term effects and costs.

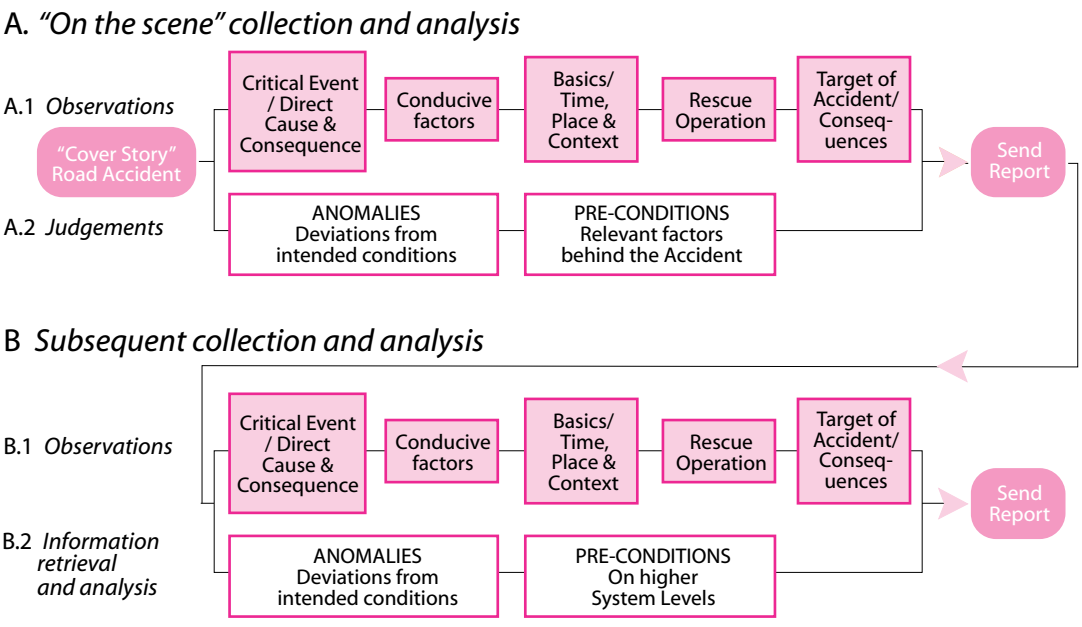


Figure 9.8 A scheme of the Accident Reporting and Audit Process to be supported by the computer based Tool.

b.2 *Information retrieval and analysis;* An audit of the organisations and agencies shaping the pre-conditions that are judged in the previous steps as relevant for the occurrence and development of the event.

A set of data-types has been created based on the AcciMap analysis performed of accidents within the transport sector. The focus in these analyses has been on the direct course of events, their pre-conditions, the functions and actors on different system levels involved and the information and criteria governing their decisions. The observations and data are recorded in corresponding categories. To some extent, the data-types chosen have to relate to regulations and instructions. Some data are included to ensure the continuation of existing accident reporting routines. Appendix B shows the data-types and the way they are categorised. The structure reflects the phases and level of details described above.

The set of data-types suggested for the tool is extensive and complex. Therefore the structure including several phases and levels of detail has been chosen in order to reduce the complexity facing the individual analyst in any specific case.

The analysis or audit phase (B.2) will to a large extent be based on generic data retrievable from different data sources and on data collected from analysis of previous accidents. Here the capacity of modern database-systems is very valuable. Large amounts of different kinds of data can be stored in a retrievable way and search-engines enables effective use of the inter- and intra-nets in the process. The data to search for and the way to analyse them are discussed in chapter 7.

In short the auditing process is as follows:
- Collect information on the preconditions for safe operation in the actual case.
- Identify the authorities, the organisations and the departments involved in the processes behind the factors indicated as relevant in connection with the accident. Use a generic ActorMap as in figure 3.5 as a support and create a Map specific of the actual case as in figure 3.6.
- Identify the normal work activity of the actors when they influence these factors together with their performance criteria.
- Describe their activities, as described in part 7.9, regarding the form and content of:
  - The information propagating downwards in the system about what to achieve and how
  - The information directed upwards about the actual condition.
  - Regulations, rules and design decisions affecting the activities

  Use the sketchpad in figure 7.8.
- Analyse for mismatches regarding information-flow and preferences of co-acting units.

9.2.2 The Platform program

The tool has to be an application of an existing platform program. Several programs on the market are useful for applications when data is to be collected, stored, retrieved, and shared by many persons for analysis. These programs are under continued development and designed to support the implementation of tools within many application domains.

The following requirements were listed as a basis for the choice of database platform, and after a product review the platform program FileMaker Pro (version 5.1) was chosen for the prototyping experiments.

The platform should facilitate the following functions:
- *Upgrade-ability*. The audit tool can run in upgraded versions of the platform program without adjustments.
- *Easy to adjust*. The tool can easily be rebuilt and the layouts adjusted when requirements are altered. A number of functional options are available for presenting and inserting data and directing the data collection process. These can be designed to support the conceptual understanding of the underlying model of the tool and the type of data requested.
- *Easy to run*. During import of data and notations these can easily be altered and data alternatives can be presented in the form of "pop-up-menus".
- *Run-ability*. The platform program and thus the tool can run on personal computers in both Windows and Mac OS environments and it can be integrated with Microsoft Office applications.
- *Accessibility*. The tool can be installed on a server and made accessible on inter- and intra-nets. It can also be distributed to different users in the form of a royalty free "runtime application" enabeling them to run the tool. (The tool is distributed together with a version of the platform program on which the application can run)

- *Tool and data protection*. The tool design, the interface and the organisation of data categories and the specific data collected can be protected by restrictions placed on specific functions and data fields. Such restrictions can vary for different users identified by user codes.
- *Ability to co-operate with other databases*. The platform program supports Open Database Connectivity (ODBC) which is an accepted Application Programming Interface (API)
- *Possibility to assess data*. Official information, like laws and regulations, statistics on accidents, trade, transports, geographical information, different regulating bodies, firms and other organisations etc. retrievable on the www can, in the analysing process, be integrated with the case specific data and notations gathered.
- *Possibility to analyse data*. Data can be stored together with indications of how they are related to other data. This enables analysis and facilitates data import. The ability to co-operate with other programs supports this function.

9.3 The Interface

9.3.1 The interface of the "on the scene" reporting Tool

Below are five displays shown to indicate the way the platform program can be used to design the interface between the analyst and the database.

9.3.2 The interface of the Tool for Subsequent Audit

The audit activity in "phase B.2" has not been further developed in the prototyping experiments than what is indicated in figures 9.3 to 9.5. A great deal of the data asked for in forms like in figure 9.6 and 9.7 can be imported automatically from the data collected in earlier phases. In that way, the auditing process will be supported by case specific formats in which the underlying conditions will be stated.

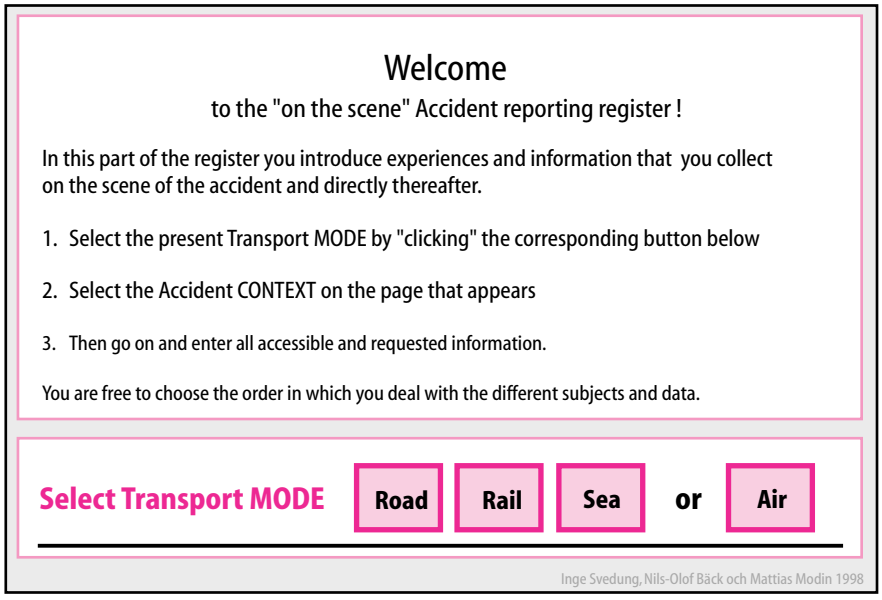


Figure 9.9. The opening page of a Transport Accident reporting and analysis Tool as it appears to the person supposed to make an "on the scene" data collection and report. Some instructions are given and the optional transport modes to select from are presented.

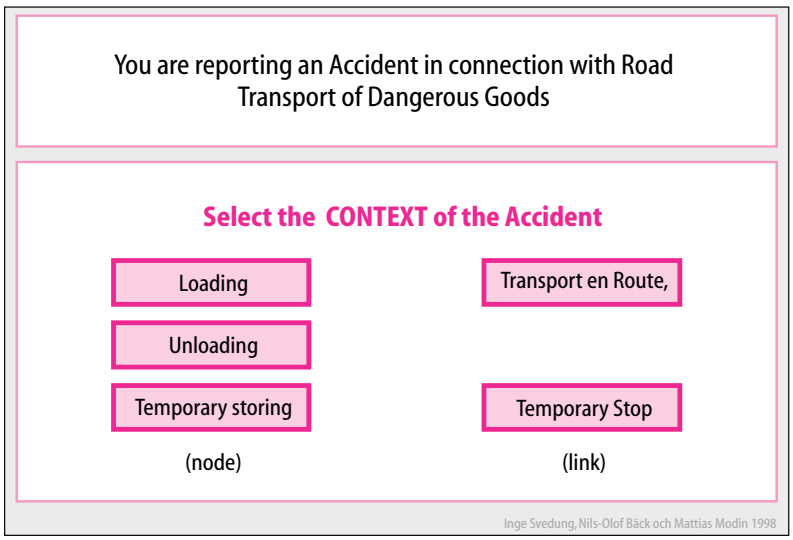


Figure 9.10. The page that comes up if one selects the Road Transport option on the previous page. This page gives a confirmation of the selection made to get there and the different options of Accident contexts to select from to get further, the "node" ore the "link" options.

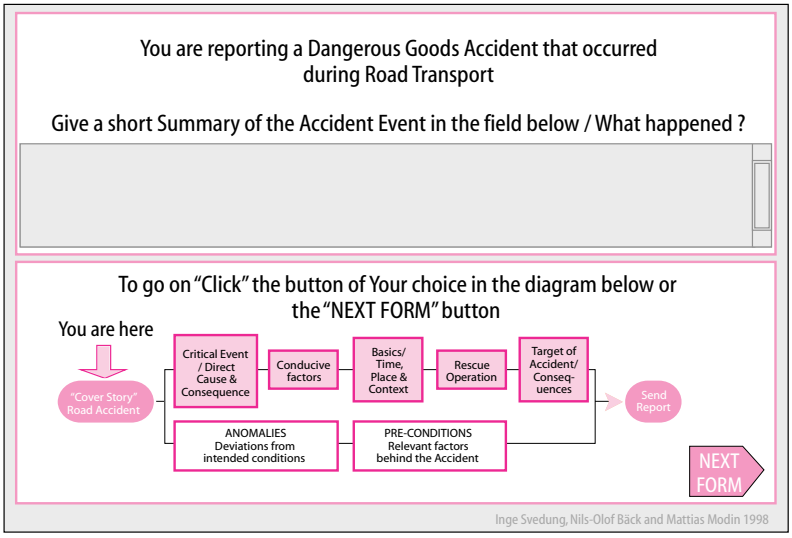


Figure 9.11. The page one arrives at if a "link" option was selected on the previous page. This selection is confirmed and the short "Cover Story" is asked for in a "free text field".

The structure of the Tool is described in a form that allows for calling up the pages for the corresponding data categories to report. "Clicking" the corresponding "buttons" does this.

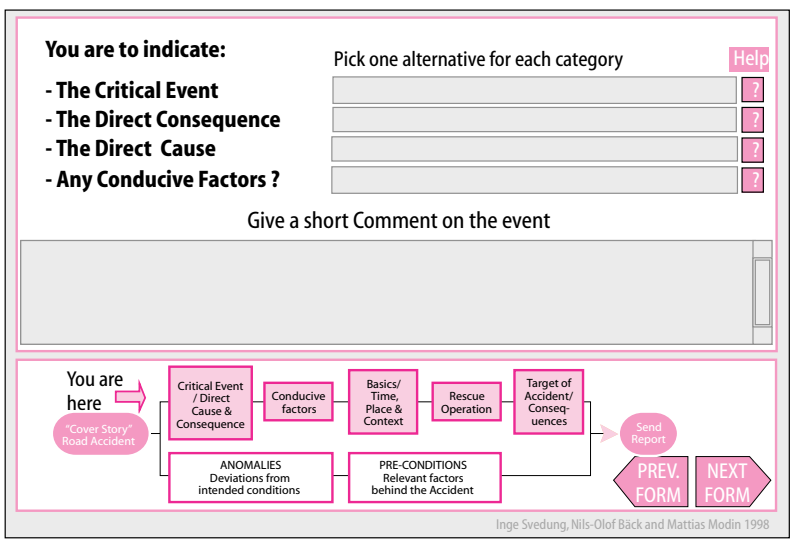


Figure 9.12. The page used to indicate the critical event, the direct consequence of it, the direct course and the contributing factors. The alternatives pop up when the different fields are clicked on and extra information regarding these alternatives can be reached by clicking the "? – buttons" In the "Free text field" the selections can be commented on. At the bottom the tool structure is shown together with the present position in it and the options when getting further in the reporting process.

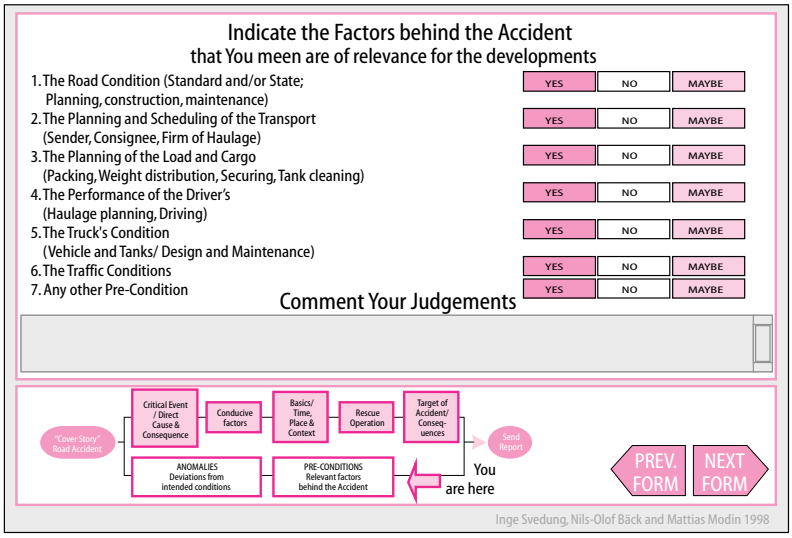


Figure 9.13. The page where the person making the "on the Scene" report is asked to indicate what the factors are that have, may have or not have influenced the development of the accident. The judgements are asked for to get an indication of what to analyse further in an eventual "face B audit" that will have the "face A report" as a basis.

10. Emergency Management and Rescue Services

When the ultimate risk cannot be managed by control of the flow of events after release by means of dedicated defenses integrated in the system configuration, society requires general services for emergency management after the fact, such as fire brigades, rescue services, civil defense brigades, etc.

Also for emergency services, a trend away from pre-planned command-and-control management strategies toward closed-loop, self-organizing strategies is found. The need for this change has in particular been voices by *Dynes*[1] from the Delaware Disaster Research Center. His arguments are reviewed in the following paragraphs and illustrate a shift in approach very much in line with the general Swedish argument for an objectives-and-result management strategy, see for example Rosenberg[2] (1998).

The usual emergency management approach is based on the military command-and-control model, which is extensively applied for the civil defense corps aiming at protection of the population during acts of war. The possibility of using it in civil context was institutionalized in a doctrine of "dual use" but the dual use was always framed in terms of the application of "military" planning to civil emergencies. For local authorities inexperienced in emergency planning, previous military experience became an obvious qualification for emergency planners.

10.1 Assumptions Embedded in the Planning Model

Dynes identifies several interrelated assumptions:

- The emergency period is characterized by a sharp distinction from the previous normal period. The situation shifts abruptly from some state of "normalcy" to a state of social chaos, signaled by considerable irrational social behavior and, therefore, traditional social control mechanisms have lost their effectiveness.
- Due to the weakness of individuals and social structure, it is necessary to establish some "command" over chaos and thereby to regain "control".
- Planning efforts have to relate to some social unit, and the focus of planning is the "community". Problems are found in planning related to isolated social units. Often planning for a unit (such as police and fire departments) is based on the assumption that such units have authority even in areas where no formal authority has been established.

10.2 Consequences of the Planning Model

The assumption of chaos stems from the enemy attack scenario, which imply that emergencies can be recognized. This is very often not the case, emergencies evolve gradually and often over considerable time. Very often, failure to announce an emergency only in hindsight can be attributed to lack of appreciation. The assumption justifies the supplement or replacement of local institutions by "outside" organizations of paramilitary structure. The assumption is, that emergencies disorganize individuals: they become traumatic, anti-social, they panic, etc. In consequence: pre-emergency planning normally has a number of features:

- When persons are disorganized, strong authority structures have to be created;
- Attention must be paid to controlling irrational and antisocial behavior;

1. Russell Dynes: Emergency Planning: False Assumptions and Inappropriate Analogies. Proceedings of World Bank Workshop on Risk Management and Safety Control, 1989. Karlstad: Rescue Services Board.
2. Rosenberg Tommy (1998) "Risk and Quality Management for Safety at a Local Level", Royal Institute of Technology, Stockholm, Sweden

– Significant resources must be spent on creating paramilitary organizations;
– Individuals cannot be expected to perform effectively in most occupational functions;
– Pre-emergency planning must be based on rigid rules, otherwise, people will not exhibit appropriate behavior.

The preoccupation with the command and control models has some immediate consequences:
– A great deal of effort is spent on documenting authority relationships;
– Organizations writing emergency plans give themselves greater authority than they have in the plans of others;
– They assume that authority in emergencies is uni-dimensional, even while recognizing the multi-dimensionality of pre-emergency structures.
– They assume that decision making and authority should be centralized;
– There is considerable tendency to "over-plan" and to continue to specify details. Thus a plan, by its very nature, is unfamiliar when it is implemented;
– There is the assumption that communication is 'downward'. Only those in the top of the structure "know" what must be done.

Dynes seriously questions the basic assumptions and he points to the lack of supporting evidence and to existing research results and empirical evidence which in fact contradict them on essential issues.

10.3 Toward a More Adequate Planning Model

On this background, Dynes suggests a fundamental revision of the planning model. He suggests a problem solving model based on more realistic assumptions about emergency behavior instead of a model implying top-down rigid control: Instead of chaos, the emphasis should be on continuity: instead of command emphasis should be on coordination; and instead of control, it should be on cooperation.

Continuity. The idea suggests that the best predictor of behavior in emergencies is the behavior prior to the emergency. The normal routines of people should be utilized for planning emergency actions, e.g., evacuation routes should be based on normal traffic patterns.

Coordination. The best predictor of emergency authority will not be to create an artificial authority structure, but, following the previous principle, the normal, "pre-emergency authority". Coordination can be enhanced through promoting inter organizational coordination and common decision making rather than hypothetically establishing the "proper" authority relationships. In fact, the continuity principle suggests reliance on the normal *competence* of people. The coordination principle appears to express the same solution at the higher planning levels: to plan for a structure in which to improvise for coordination rather than to rely on top-down control. Dynes argues that emergency management needs to include both improvisation and preparedness activities: "Without improvisation, emergency management loses its flexibility in the face of changing conditions. However, without preparedness, emergency management loses some degree of clarity and precision".

Cooperation should replace control. The fear implied in the command and control model that massive failures could be anticipated by the loss of personnel not fulfilling their obligations, simply has no empirical support. This means that the central planning problem is not 'control' but to find ways to effectively re-allocate human and material resources in the community. Many of those allocative decisions will be made without much planning attention because people do improvise and 'volunteer'.

Dynes concludes that "there is considerable irony in the fact that much of the recent increased interest in emergency planning has been channeled in directions which reinforce the military model". However, "there are glimpses of hope". A new generation of emergency planners is less burdened with the scenario of enemy attack, and more research is done in emergency behavior.

Dynes concludes the discussion by the statement that emergency plans shape emergencies to match the organization editing the plans and, generally, plans talk about organization, not emergencies. Being dependent on the military paradigm, the planning ideology is culture independent and universal.

Dynes' request that emergency responses should be based on peoples normal way of organizing behavior relates well the requirements for closed-loop performance. Preparedness ac-

tivities imply a preparation of the structure within which to improvise and creation of an awareness of the available options, i.e., the opportunities for actions. The problem in emergency situations in actually utilizing the available options in a way is analog to the difficulty of a company in realizing its options for changes in work practice and organization when new technology is introduced.

The question is; how can you support the necessary exploration of available action alternatives when conditions change during emergency, i.e., how to support the use of experiential knowledge during emergencies? *Dynes* answer to this question is that support should be given;

1. by collection and distribution of information and by realizing that changes in information flow is necessary during emergencies
2. by building-in *observers* in the emergency plan who check the newness of the situation, and *critics* who can react to behavior.

What Dynes actually suggests is to base emergency plans on guidance based on feed-back from observed behavior and to create an information environment which make it possible for people to adapt to the emergency by their normal learning mechanisms.

10.4 Information Systems for Emergency management[3]

The position of Russell Dynes with respect to emergency management planning has been discussed here in some detail because his requirements for a dynamic organization are closely related to the requirements for proactive risk management, as discussed in chapter 4.

The decision-making problem for emergency management has some very peculiar characteristics:

- The problem domain is poorly defined. Decision-making and planning are related to a large variety of emergencies, caused by very different physical processes. The resources to consider in emergency control may belong to different technical service fields.
- The decision-makers are difficult to identify in advance. They are activated, depending on the size and nature of the actual case.
- Several organizations and technical services are involved, and decision making will have the nature of a cooperative effort in a distributed system. Support of decision-making is required during dynamic emergency situations, as well as for planning purposes.
- Information needed as a basis for decisions may stem from a large variety of sources, such as engineering textbooks, laws and regulations, risk analysis, analysis of prior accidents, procedures, and instructions.

Key problems for decision support will therefore be to consider:

- Organization of large, inhomogeneous databases, information retrieval, requirements for analysis supplying data in order to have proper data attributes and formats compatible with user needs.
- Analysis of the organization of the cooperative decision making, and the structure of the communication network that evolves depending on the situation.
- The nature, in general terms (covering typical situation scenarios), of the control and decision task, and the related information needs.

As it is discussed in chapter 4, support of improvisation and problem solving in a dynamic society cannot be based on preplanned instructions and procedures. Instead it is important to make a faithful representation of the workspace available in terms of a kind of means-ends map.

The workspace of a rescue service commander is very different from the work domains normally considered for design of work support systems. In a normal productive organization, actors are operating within the same workspace during longer periods. Furthermore, means and ends belong to the same reasonably familiar workspace. The situation of a rescue services commander is very different. His workspace must be defined on occasion.

He will have to consider two separate domains, one describing the domain of the active hazard sources, and another representing the available resources for mitigation. In the particular situation, he will have to merge these two domains into a perception of his actual workspace. His information needs

3. This section is based on interviews reported in. Rasmussen, J., O. M. Pedersen and C. D. Grønberg (1987): Evaluation of the Use of Advanced Information Technology (Expert Systems) for Data Base System Development and Emergency Management in Non-Nuclear Industries. Risø-M-2639

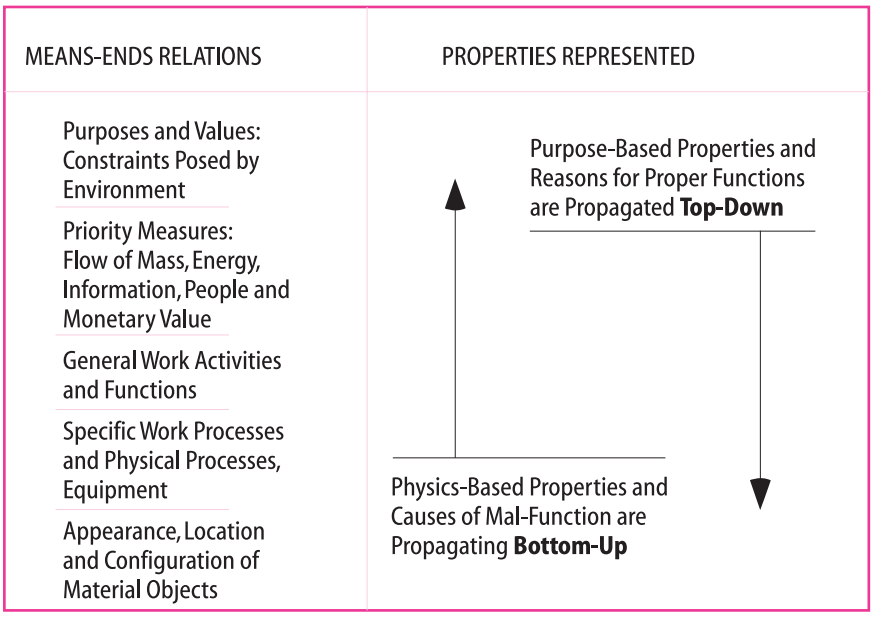


Figure 10.1. A means-ends abstraction hierarchy used for representation of the functional properties of a physical work environment.

vary widely with respect to content and relevant information sources. To be able to develop decision support for the great variety of decision situations, it is necessary to create separate representations for the potential risk domain and the mitigation resource domain.

A means-ends/part-whole map is very useful for representation of the workspace involved in resource management, and is discussed in some detail in the following paragraph because it gives a more detailed discussion of the work space representation discussed in section 7.8.1.

10.5 Workspace Representation

A representation of a workspace in terms of a means-end hierarchy has proved to be useful for planning decision support systems.[4] This representation is used to describe a workspace along the part-whole and the means-end dimensions in order to have a consistent framework for identification of the control requirements of a system and the content of the related decision task. Emergency management is a typical resource management task in a purpose-function-equipment hierarchy and the adequacy of a decision support system cannot be judged without an explicit description of the means-ends space.

Resource management task depends on navigation in a means-end hierarchy representing the functional properties of the workspace, see figure 10.1. In this hierarchy, the functional properties of the workspace are represented by concepts that belong to several levels of abstraction. The lowest level of abstraction represents only the physical form of the system, its material configuration. The next higher level represents the physical processes or functions of the various components and systems in a language related to their specific physical properties. Above this, the functional properties are represented in more general concepts without reference to the physical process or equipment by which the functions are implemented. Finally at the two top levels, the purpose and the constraints defining the coupling to the environment are represented, together with the priority measures guiding functional planning.

At the lower levels, elements in the process description match the component configuration of the physical imple-

4. Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.

	Domain of Potential Risk				
	National Overview and Patterns	Emergency Classes	Companies and Installations	Specific Production Plants and Systems	Processes, Substances, and Components
Goals, Purposes and Constraints	Risk pattern in terms of social and economic consequences with reference to features of established policies and public opinion				
	National pattern, geography and demography	Risk pattern as related to industrial branches	Risk pattern of individual installations and plants	Risk related to specific processes	Risk related to specific materials, substances and components.
Priority Criteria, Economy, Risk, Man Power Flow	Risk measures in terms of economy, probability and other abstract measures suitable for setting priorities				
	Accident potential in general terms: fire, explosion, flooding, toxication				
General Functions	Relation to geographical regions or population features	Relation to industrial activities or to population groups	Relation to specific process plants or installations	Functional and accidental mechanisms or specific processes	Risk classes related to categories of substances, and material
	Physical processes and mechanisms behind accidents, causation, propagation, potential for interaction with accident control measures				
Processes of specific Installations, Groups, and Equipment	National and geographical patterns, meteorological data, water streams, other propagation characteristics	General data on industrial practices, processes and accidental mechanisms. Safety measures	Functional information on specific plants, accident potential and mechanisms. Safety measures	Relation to specific manufacturing processes	Properties of substances and materials
	Locations, topography, physical design and appearance				
Material Locations, Configurations, Appearance	National pattern of potential sources and population, propagation routes, road and barrier topography	Distribution according to branches and risk categories	Location of specific plants and installation. Drawings of buildings and access routes, maps of likely propagation paths	Location of specific process equipment, identification data, transport and access information	Information for identification and location of material, substances, and components. Personal data

Figure 10.2. The figure illustrates a means-ends/part-whole representation of the domain of potential risk to be considered when planning rescue services and emergency management.

mentation. When moving from one level of abstraction to the next higher level, the change in system properties represented is not merely removal of details of information on the physical or material properties. More fundamentally, information is added on higher level principles governing the co-function of the various functions or elements at the lower level. These higher level principles are derived from the purpose of the system, i.e., from the reasons for the configurations used at the lower levels. Change of level of abstraction involves a shift in concepts and structure for representation, as well as a change in the information suitable to characterize the state of the function or operation at the various levels of abstraction

Within this hierarchy, causes of improper functions (disturbances) depend on changes in the physical or material world. Thus they are explained "bottom-up" in the levels of abstraction, whereas reasons for proper or acceptable function are derived "top-down" from the functional purpose.

Basically, decision making is a process of iteration between considerations at the various levels rather than an orderly transformation from a description of purpose to a description in terms of physical materialization of a solution. There exists a many-to-many mapping between the levels; a purpose can be served by many physical configurations, and a physical system can serve many purposes or have a variety of effects.

The framework therefore is useful in the present context, since emergency management includes the ad hoc design of a mitigating system, and its subsequent control. Figure 10.2 and 10.3 shows an overview of the domain of potential risk and the domain of mitigation resources.

Domain of Potential Risk. This part of the potential work space includes information identifying the potential risk sources, their functional physical properties making it possible to predict the accidental propagation of effects of accident releasing mechanisms, and the possible higher level consequences in relation to social norms and legal rules. The related part of the database will supply the basis for a situation analysis defining the emergency situation that should be subject to control. The information will be available from risk analysis, technical manuals, and analysis of the technical features of prior cases. Examples of the information at the various levels are shown in figure 10.2.

The Mitigation Resource Domain. This domain includes the information about functions, processes, and equipment/personnel that is available to form the counteracting and mitigating force. It represents the problem space for the planning the mitigation effort. The information included at the various is illustrated in figure 10.3.

10.6 The Use of the Workspace Representation

The representation of the problem space in figure 10.2 and 10.3 is a multi-level representation in terms of the governing objectives and the available/required equipment-process-function-purpose elements, and the information that should be available for decision making in a specific situation.

The functional elements represented at the various levels can be characterised in three different ways: 1. "what" it is, i.e. its defining characteristics, described in terms related to that particular level; 2. "why" it may be chosen, i.e., its role at the next higher level, and 3. "how" it may be implemented by resources at the next lower level. This means that the data element in a database should be characterised from all three different points of view. Decision making in a particular situation will be an iterative consideration of the resources at the various levels until a satisfactory relationship through the levels has been identified, connecting the various, possibly conflicting, goals and constraints with the available physical resources. This will involve the task of keeping track of a many-to-many mapping in a complex net. The use of information technology should be considered to give easy access to information by accepting a query language including all three what-why-how aspects. In addition alerting the user to consider other relevant means-end mappings than the one behind an actual information request. Figure 10.4 and 10.5 shows an overview over the information sources relevant for the two domains.

10.7 Decision Support

Databases derived from the means-ends representations are relevant for preplanning of emergency services and for support of a rescue commander in action.

The information retrieval problems are different in the two cases, and depend on the competence of the user and the means for interaction with the database. Who will be the typical users? ? Somebody in a command center with radio link to a data center? A rescue commander having direct access to the

Domain of Emergency Management Resources					
	National Overview and Patterns	Activity Categories Emergency Classes	Organizations and Institutions	Emergency Task Forces	Individual Agents and
Goals, Purposes and Constraints	National laws and government agency regulations	Goals and constraints for measures against; fires, floods, traffic accidents, etc.	Goals and targets for services and institutions; hospitals, fire brigades.	Goals and targets for groups and task forces	Exposure limits for individuals, regulation data
Priority Criteria, Economy, Risk, Man Power Flow	Criteria and measures for priority setting Flow, accumulation, turn-over of funding, man power, and material				
		Risk Categories	Services	Task forces	Individuals and equipment
	Available resources for general emergency control functions: Fire fighting, medical care, transportation and evacuation, etc.				
General Functions		General overview of resources. General rules and heuristics for counter measures.	Resources specified with reference to organizations, institutions. General institutional rules and practices.	Resources of identified task forces, groups, and operational units and institutions	Capabilities of equipped individuals and major tools
	Physical functioning, capabilities, and limitations of emergency control mechanisms; potential for interaction with accident control measures				
Processes of specific Installations, Groups, and Equipment				Physical functions and capabilities of tools as available to task forces and groups. Instructions and procedures, standing orders.	Physical Characteristics and limitations of tools. Information on possible, unacceptable interaction with media and installations (chemical, electrical, etc.) Procedures and practices.
	Locations,descriptions, identification of items, forces, groups.				
Material Locations, Configurations, Appearance	Road system with data on traffic and load capacity.	Geographical location of services and institutions, access routes.	Drawings of remises of individual institutions. Drawings of buildings. Inventory lists of service stations.	Inventory, locations, identifying characteristics of equipment, tools, and members of task forces	Drawings of equipment with size and weight data.

Figure 10.3 illustrates a means-ends/part-whole representation of the emergency management resources.

	Domain of Potential Risk: Information Sources				
	National Overview and Patterns	Emergency Classes	Companies and Installations	Specific Production Plants and Systems	Processes, Substances, and Components
Goals, Purposes and Constraints	Generalizations in terms of policies and goals				
Priority Criteria, Economy, Risk, Man Power Flow	Generalizations from accident and risk analysis and overviews; in terms of economic and risk level terms for settings priorities				
General Functions	Statistical reports and overviews	Overviews from branch organizations, safety authorities, journals, etc.	Company overviews and safety records. Risk analyses and consequence prognoses.	Risk analysis, consequence prediction. Incident and accident reports. Textbooks and journals.	Chemical, technical textbooks and journals. Risk and work safety handbooks.
Processes of specific Installations, Groups, and Equipment	National summaries and overviews	Summaries over branches and emergency classes.	Technical manuals, emergency and safety plans and procedures. Overall production, transport, and management manuals and reports.	Technical equipment manuals, process specific accident research and event reports. Inspection reports; maintenance logs.	Toxicological and pharmacological handbooks. Incident analysis reports and data banks. Hospital rules and data.
Material Locations, Configurations, Appearance	National summaries and overviews	Geographical overviews for emergency classes from branch organizations and authorities.	Drawings, maps, manuals on sites, buildings, and configuration of installations and supply/waste piping	Drawings, manuals, descriptions of plants and equipment. Installation and handling manuals. Inspection reports. Inventory lists.	Reports from companies, suppliers, inspection reports. Inventory lists.

Figure 10.4. The figure shows a means-ends/part-whole map of the information sources related to the potential risk domain.

Domain of Emergency Management: Information Sources					
	National Overview and Patterns	Activity Categories; Emergency Classes	Organizations and Institutions	Emergency Task Forces	Individual Agents
Goals, Purposes and Constraints	National laws and regulations		Statutory instruments. Authority regulations Institutional constitutions.	Istitutional derivation of laws and regulations	Worker protection regulations. Union agreement.
Priority Criteria, Economy, Risk, Man Power Flow	Accounting Systems				
General Functions	Resources and capabilities; reports from institutions and services				
		General strategies; textbooks, generalizations from incident, accident, and risk analysis. Generalizations from drills, exercises, and experiments.			
Processes of specific Installations, Groups, and Equipment		Functional information from accident and risk analysis, exercises and manuals for equipment. Derived procedural information and empirical know-how			Equipment manuals, data from research, textbooks, accident and risk analysis.
Material Locations, Configurations, Appearance	Road authorities, statistical institutions	Descriptions, architectural drawings and maps, equipment inventories, and staffing information			Equipment manuals and specifications.

Figure 10.5 shows the information sources describing elements of the mitigation resource domain.

database? Or advisers of varying competence supporting the commander on location?

Data types to consider together with their sources will be:
- Orders (in terms of goals), statements of objectives, etc. (from preplanning or from level above),
- Procedural information (from preplanning or from coordinators),
- State information in actual situation (from communication sources),
- Background information (structural, causal information, from textbooks, risk analysis, incident analysis).

The form in which the information should be stored in the database depends entirely upon the users' formulation of their problem and needs.[5] This, in turn, depends on the identity of the actual decision maker, and the boundaries of his information needs in terms of location in the work space map, as well as upon the hierarchical structure of the operating organization. Will, for instance, the organization be strictly hierarchi-

cal, as a military command organization in which each person is clearly related to a function in the hierarchy, and (ideally, at least) only communicates orders downwards in the form of goals to achieve, not the ways to do it. In this kind of system, the information to be communicated between actors, and the kind of information they will seek in the database can be identified. However, in normal, civil organizations, people do not stick to their roles, and the same individual will probably be moving between levels. This situation probably corresponds better with the dynamic organization suggested by Dynes. This may give ambiguity in the search phrases for items from the database. Communication between levels may be through a person moving between levels, rather than by person-to-person exchange, (i.e., will a person look after information at the level he at the moment cognitively will be at, or will he look from levels above and below?).

The perception of the task by the individual participants in a case should be carefully studied, together with the way the task and information need is expressed, in particular, the redundancy in the verbal terms with reference to the problem space characteristics should be considered. In the analysis it may be a help to compare situations or activities which were considered particularly successful or the opposite by the participants. Is there a difference in the distribution of these cases in the problem space? Considering the needed assistance, the support systems to consider may be different for different persons, and will consequently depend on the localization in the problem space. Another aspect of a strict hierarchical structure that should be considered in the analysis of cases is the possible lack of contact between groups at the same level. Does a problem appear if the rescue-company such as, e.g., "Falck", the public fire brigades, and the civil defense corps, cooperate in fire-fighting, and the hierarchical structure is respected? Again, this issue was discussed by Dynes.

For the effective use of information, it should be considered that the selection and formulation of information to present should reflect and distinguish the different alternatives of action. The number of action alternatives is increasing down through the levels. In this respect the information should be clearly operational, and the implications in terms of action alternatives, and in constraints on their choice, should be represented in a way that can be used in search terms. Frequent failures are related to not using an action alternative, rather than to doing something wrong.

It should be carefully considered that the amount of information and the complexity/diversity (in a specific, dynamic situation, at least) will increase downward through the hierarchy. This will probably be reflected in the organizational structure if it is assumed that the evolution will have aimed at equal complexity for the individual decision-makers.

The data base representing the problem domain in terms of risk potential and emergency management resources will include structural information about functional properties and causal relationships which must be transformed into procedural information in order to be operational in the actual accident situation. This transformation can be based on heuristics derived from prior experience or deductions based on state information from the case actually present. If procedural transformations are incorporated in the database, it will have to be rather general rules, or very specific retrieval attributes must be defined. If the procedural information have to be generated on-site, it will either have to be done by the commander himself. Being busy, it is more likely that he will pass information on the actual state of affairs to an advisor in possession of the necessary general background knowledge or to a person in the command center who has access to the relevant databases. See figs. 10.6. This advisor can be a human domain expert or an "expert system inference machine" attached to the database.

Very likely the advisor has access to factual and functional information in the database. To generate the necessary procedural information, he will have to interpret this basic information in the situational context that is known to the active commander. Experience from computer-based support systems indicate that this interactive process tend to make the use of databases difficult.

10.8 Rescue Commanders' point of View

Interviews[6] of rescue commanders have indicated the following general information needs:

5. See the discussion of information retrieval in libraries in: Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.
6. Source: Rasmussen, J., O. M. Pedersen and C. D. Grønberg (1987): Evaluation of the Use of Advanced Information Technology (Expert Systems) for Data Base System Development and Emergency Management in Non-Nuclear Industries. Risø-M-2639.

10.8.1 Route Information.

Which way is recommended leading from station to the scene of the accident? Such advice shall be an optimal suggestion considering actual traffic load, road repair, weather, sight, one-way restrictions, and the most recent traffic accidents are taken into consideration.

10.8.2 Access to the accident site

Today's plans for access to specific sites: theatres, sport grounds, factories, etc., are frequently out of date. There is a constant need for updated plans.

10.8.3 Capacity of hospitals

An information center keeping account of actual (hour by hour) capacities for receiving patients on hospitals in the region. Such information is urgent to the emergency officers and ambulance drivers.

10.8.4 Plant descriptions

Local geography, plant functions, materials and chemicals are the typical information one gets from local people, when these are available. Some of these data should already be contained in the chief fire officer files, because they are the basis for inspection. Ignition sources, fire potential, water supply are evaluated regularly, as well as emergency exits, fire extinguishing systems, also showing that the fire service may use technical means to draw information from their own files.

10.8.5 Sewers

Water and other substances used in the fire fighting will normally end up in the sewerage in many cases. The fire commander needs information on sewer systems, if explosive or polluting substances are drained into a sewer. He may warn sewer stations on the actual line, and warning may be given to residents and people on the roads.

Such information does not belong to the fire service, but resides in another branch of the local authority.

10.8.6 Chemical expertise

Normally, a very comprehensive knowledge system is made available to the fire commander, with chemical emergency cards, expert advisors, and information centers with links to foreign systems. Development trends for chemical knowledge systems should preferably aim at:

- Means for more expedient identification, as far as this key is a necessary first step
- More selective presentation of relevant information

Fire officers often feel burdened by too much information.

10.8.7 Medical expertise

Fire personnel traditionally follows simple and mostly rather efficient rules during rescue operations, concerning priorities, transport of injured persons, and first aid principles. In disaster cases there will be doctors and nurses mobilized to work on the scene of the accident and relieve the fire commander.

The chemical emergency cards give specific first aid information for each chemical. This information is formulated specifically for fire personnel, ambulance drivers, etc., who can administer first aid in the absence of experts.

It may constitute a large step forward, if the emergency manager can obtain the set of first aid rules specific for the actual case, i.e. the optimal procedure, based on the information presented. Under present conditions, this information is available in fixed sets and released only when specific keys are presented.

10.8.8 Technical expertise

Cases in the past show examples when electrical and mechanical expertise might be of great help: is it advisable under the circumstances to shut down the extraction plant, for instance by breaking the electrical power supply? And which procedure is suggested? In an actual case, an explosion happened at the moment, where one power line was broken in order to reduce the amount of potential ignition sources inside the explosive zone.

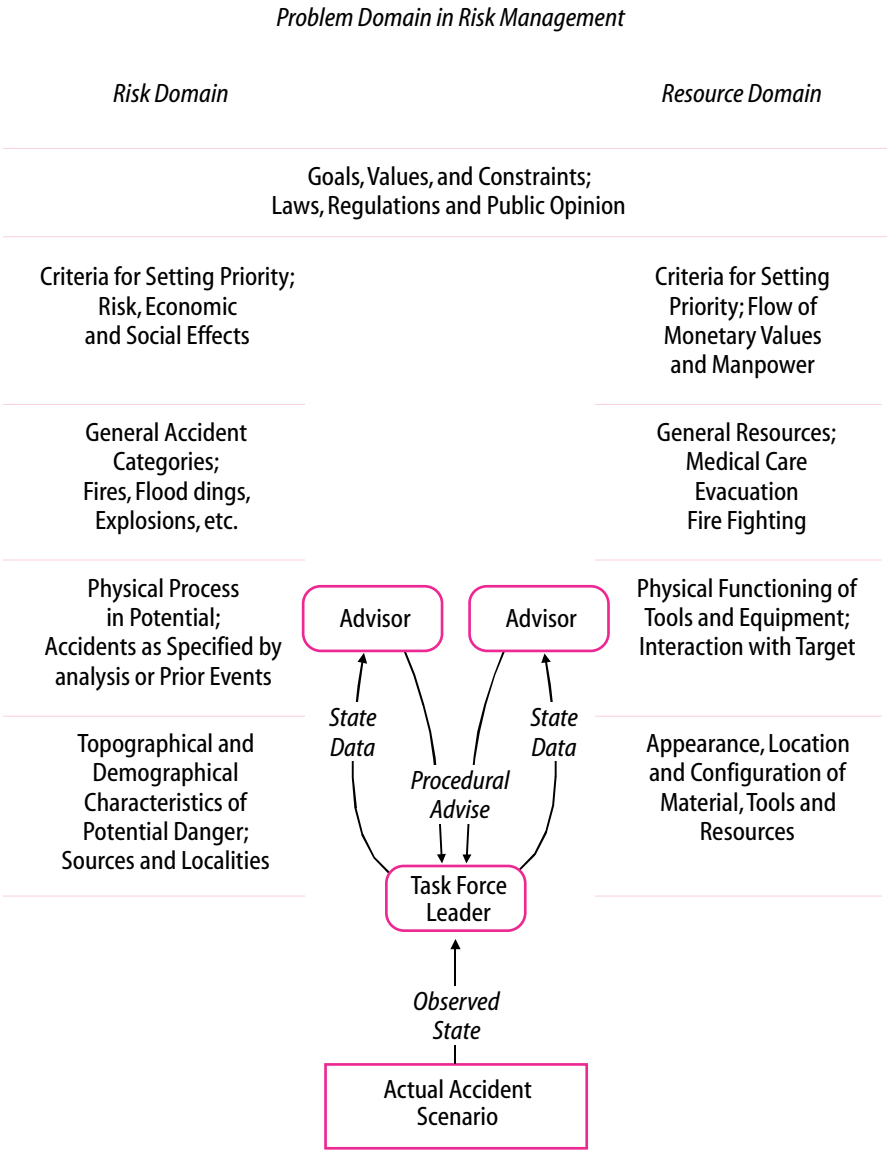


Figure 10.6 illustrates the iterative interaction necessary between a rescue commander or task force leader and advisors with access to databases. The commander must inform the advisor about the actual context to make it possible for him to generate procedural advice from basic database information.

11. Example of a detailed Field Study

This study exemplifies the approach to a study of the normal work conditions in a particular workspace, as described in chapter 7. It was performed in a company manufacturing chemo-technical products that are marketed and distributed to wholesalers and superstores. The warehousing and delivery function has been studied with focus on the quality of service performed by the warehouse staff and the effects of new routines for quality improvement. The functions in focus are those of the warehousemen, the "goods handlers".

The company investigated was selected for the study because it was fairly well known to us beforehand from previous investigations mainly on accidental risks and risk management in production departments. The warehouse department was selected since it has an important role to ply in the control of safety in transport. There was no coupling between the company and any of the accidents analysed in Appendix A.

The experiences used as basis for analyses have been gained over a period of about a year by direct work observations and interviews to identify functions within the department and in functional co-operation with it, to identify individual and groups of actors and to reveal there information network.

To get a general and updated idea of the organisation we surged for public information on web-sights and in newspapers. In the first contact we asked for copies of the latest issues of the in house magazine and of other documents used within the organisation to inform staff of goals, state of business and projects running on technical and organisational changes.

In an early stage of the study persons identified as planners and supervisors were interviewed to get a picture of the general functions performed, production-data, equipment used and methods and routines by which official information was distributed and called fore. Based on such data a thorough study was planed and performed with in depth interviews and by following individual actors in their work. When a specific behavior was recognised questions were raised about way, what alternatives there were and what it was that made them act as observed. Interviews were performed in a rather free form where people, individually or in group, were encouraged to tell about experiences made in their normal work. Notes were taken and supplemented soon after from own remembrances and by renewed contacts.

During analysis models or "maps" were created describing the system as understood from the information collected. These were presented to and discussed with the actors involved.

Rasmussen[1] et al has described in more detail the method of investigating work organisations.

Statistics about the "production process", gathered by the organization as a part of normal follow up, is another important source of information. The results of the investigation are presented mainly in a number of "maps" and diagrams describing:

- The Context;
  - warehouse layout and utilities used
  - "production-data"
  - functions performed within the warehouse
- The Actors involved in the warehouse functions and those in co-operation with them
- Information/co-operation structure around two types of actors (warehouseman and foreman)
- Goals and strategies of warehouse men
- Type and number of deficiencies in deliveries according to customer complaints
- The process of implementing a routine to report back to warehousemen periodically and individually about customer complaints

1. Rasmussen, J., Pejtersen, A. .M and Goodstein, L. P. (1994): Cognitive Systems Engineering. New York: Wiley.

- The effect over time on the number of complaints of implementing this routine
- Normal work of a warehouseman, an ActivityMap

11.1 The Context

11.1.1 Warehouse and utilities

The warehouse consists of two parts, one for inflammables and one for other goods. Layout and some designations used below are shown in figure 11.1.

Goods is handled on pallets or in containers designed to fit with the rack system for pallets. In the warehouse there are 11 000 pallet- or container places mainly in five-level racks. Computer-controlled pallet cranes serve two parallel ten-level racks.

Racks are numbered with signs on the short ends. To define and indicate a pallet place in the rack-system a digit combination is used stating the rack-number (XX-), the position along the rack (-YY-) and the rack-level (-ZZ) with –00 indicating the floor level.

The 1 700 pallet places on floor level can be reached manually by the "goods handler" who, with the aid of a small electric fork truck, picks up and gathers goods on pallets for delivery. These places are called "Pick-Up Places". The rest are for whole-pallets and consequently called "Whole-Pallet Places". They are served by counterbalanced fork-trucks.

11.1.2 Production

Yearly 20 warehouseman working two shifts are handling 40 000 ton of goods following the instructions in 38 000 orders comprising 390 000 order-lines. About 60 % of the total goods volume is collected manually and gathered on pallets

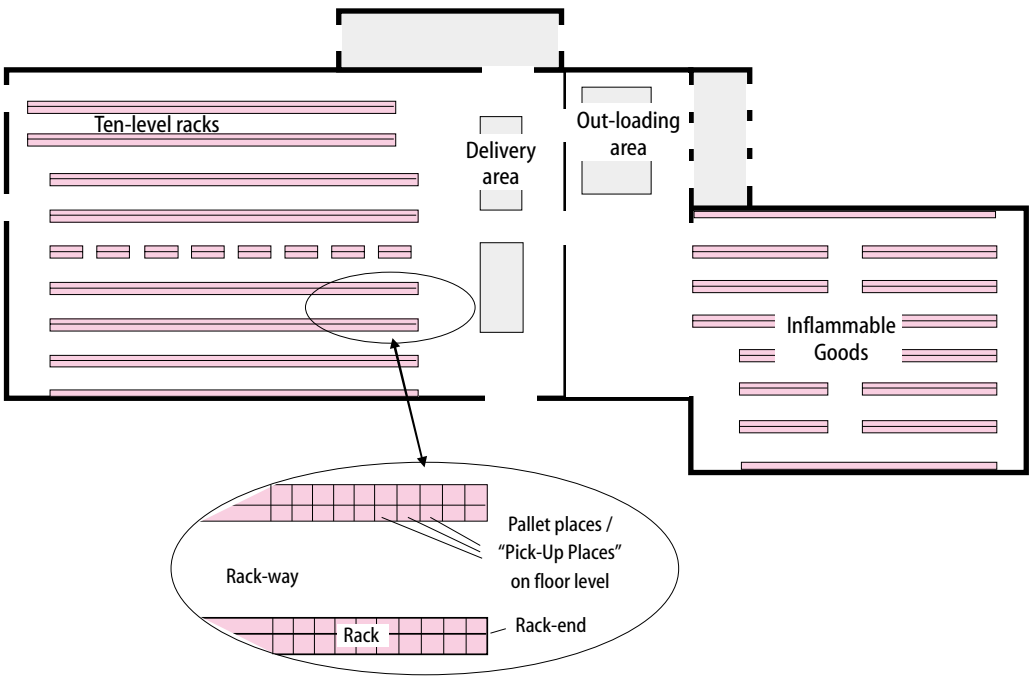


Figure 11.1. Warehouse layout and designations used

for delivery. The rest is handled as whole pallets. A single order can include both pick-up items and whole pallets. In total 1 400 000 packages are delivered.

11.1.3 Functions performed

In figure 11.2 the physical flow of goods and the functions performed to control this flow are indicated.

Bold arrows indicate the flow of goods as it is delivered to the warehouse and distributed to whole-pallet places and from there further on, either directly or via Pick-Up places in smaller lots, to the delivery areas where it is wrapped in a polymer foil, labeled and registered as delivered. From there the goods is transported to the out-loading areas and then loaded on trucks for transport to customers. Another physical flow is that of goods documents produced by the delivery function and handed to the truck drivers.

Fine arrows indicate the normal flow of information between the operative functions as they support and perform the every day "production process".

To keep the figure 11.2 easy to grasp the co-operating functions not directly involved in every day production in the warehouse are not included in figure 11.2.

11.2 Organization / Roles of actors

Actors within the warehouse function are indicated in the format of an ActorMap in figure 11.3, either as individuals or as groups with the same function to perform. Co-operating functions within the company are also indicated together with the most important external parts, customers and firms of

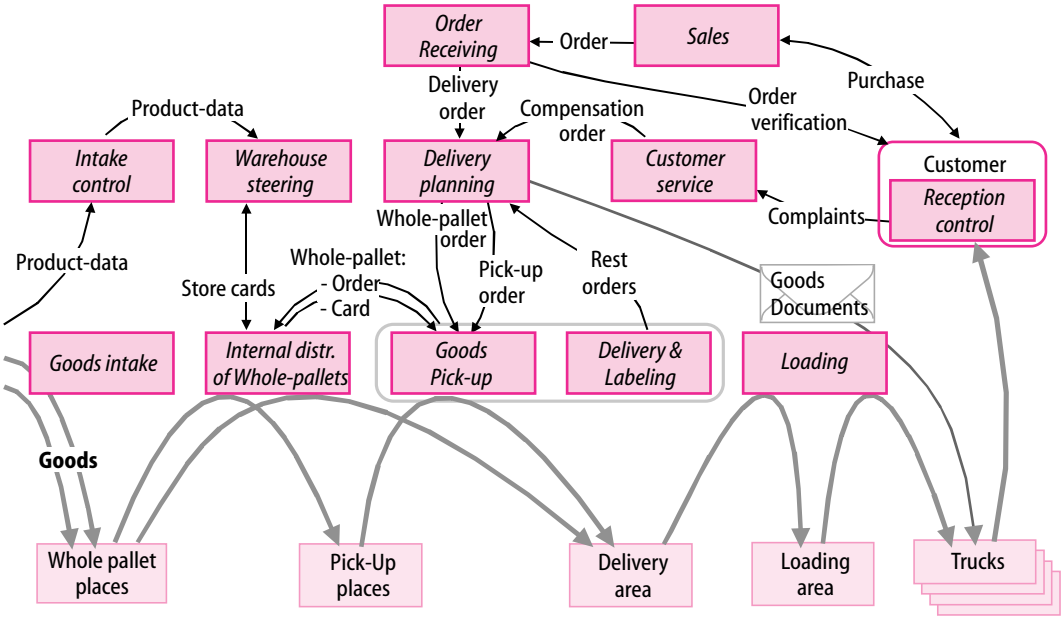


Figure 11.2. The physical process and the operational functions performed within the warehouse. The customer's goods reception control function is included to indicate the delivery complaint compensation function. The lower part of the figure constitutes the physical level and the upper part the operator level of the system

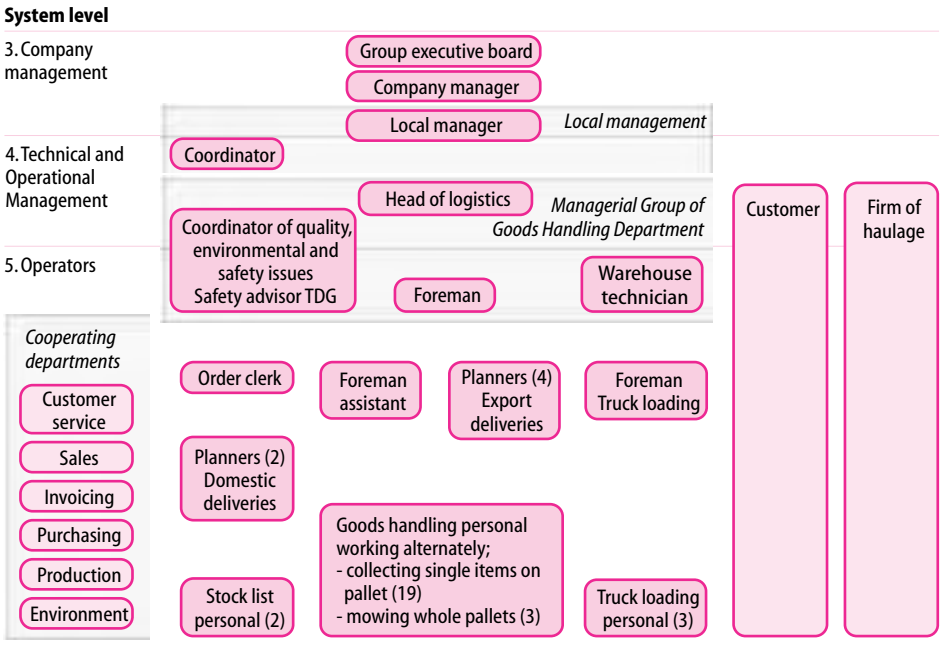


Figure 11.3. The actors, individuals, groups and departments on system levels 3 to 5, that cooperate to perform or support the warehouse function. The customers and firms of haulage are also indicated.

haulage. Below a number of statements about the actors and the functions they perform are presented to facilitate the comparison of figures 11.2 and 11.3.

Daily production

- The order clerk receives orders in electronic form from salesmen, checks if the orders are plausible, contacts the customers to verify and sends them to the delivery planners.
- The planners of domestic and export deliveries receive sales orders from the order clerk. They register them in the computerized system, adding data such as article- and pick-up place numbers and information about demands for goods separation during transport, data accessible from a product data bank. They estimate the number of pallets to carry the goods, decide time of delivery and the position in the delivery area were the goods is to be placed before further transfer. They produce the whole-pallet and pick-up orders lists (on paper) and place them for the goods handling personal to attend to. They also receive compensation-orders from the customer service and treat them alike. Based on order-lists returned by the goods handlers after being attended, they produce the transport documents (transport cards and delivery notes) that travel with the goods.
- The stock list personnel operates a card-system to control the inventory and it's location in the warehouse. For incoming goods they combine the goods document with a pallet place number card, mark the place number on the goods and store the document and the card. In the delivery process they exchange, with the goods handlers, the whole pallet orders for pallet place cards.
- The goods handling personnel performs one of the following three functions following a rotating schedule:

  - Internal distribution of whole-pallets of goods in accordance with pallet place notations on incoming goods and with whole-pallet orders for delivery or for internal distribution to pick-up places
  - Collection of goods following requests on pick-up order lists, palletizing it and labeling dangerous goods, making notes about not deliverable items on the lists, signing the list and handing it to the delivery planners ore entering the data directly into the computerized system for order- and delivery management. This process is described and analyzed in more detail in the following sections of this chapter
  - Checking inventory on pick-up places and requesting goods to be distributed from whole pallet places to eliminate shortages.
- The truck loading personnel identifies goods in the delivery areas with respect to its destinations according to its placing. They then transfer it to respective loading area and from there on to the trucks were they secure the goods in co-operation with the truck drivers, to prevent it from moving around during transport.
- The foreman of the truck loading function supervises the loading and forward the transport documents to the truck drivers.

Planning and support

- The foreman plans the working schedules for the goods handling personal and assists them in their work. He collects and organizes data on deliveries, warehouse inventory fluctuations, number of rest notations and delayed deliveries. These data are gathered from the computerized order- and delivery management system and from the inventory card system. He also gathers and analyses customer complaints and informs the goods handlers individually about number and type of faults in deliveries, see also figure 11.4.
- The Co-ordinator of quality, environment and safety issues also has the role of safety advisor as stated in the ADR regulations. He co-ordinates the implementation of work routines within the warehouse and when purchasing transport services. He documents local work instructions and supervises staff education and training.
- The Warehouse technician undertakes minor alterations and repair works on equipment and interior fittings. He purchases different services from the in-house repair shop and from firms outside and he organizes corresponding statistic.
- The head of logistics performs long-term planning of the transport functions and of the over al function performed within the warehouse. He supervises projects concerning organizational and technical changes, and he makes requests for funding and follows up budget.
- The purchasing department selects firm of haulage and purchase transport services for deliveries and for incoming goods from domestic in-company production sites. Transports from other companies and from abroad are organized by firms of delivery.

11.3 Flow of information

From figure 11.4 it can be seen that there are rather many actors that communicates with the foreman who performs a complex set of tasks. During his normal, daily work the goods handler on the other hand communicates only with a rather limited number of actors, see figure 11.5. The staff is very familiar with their tasks and the daily work is performed with a minimum of "shop-talk".

The Pick-up order-lists contain information about list- and page-number, date of ordering, customers name and address, date of delivery, transport mode, firm of haulage, order number, number and type of packages, free space for indicating estimated number of pallets and signing by delivery planer. The number of different product types on the list can vary from one to more then a hundred with an average of about ten. Each type of product is presented on one order line where the following information is given:

- Pick-up-place number, article number and article designation
- Weight or volume of article
- Number of articles ordered and a space for notation of number delivered
- Order line number
- ADR- and IMDG- class, UN-NR, Flash point and cold-resistance.

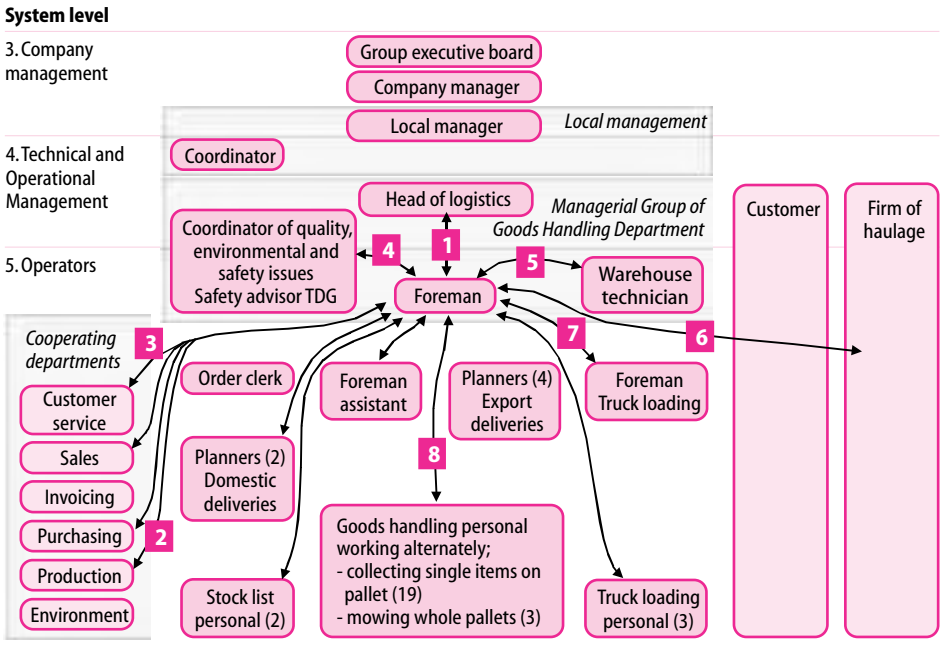


Figure 11.4. Information flow OUT from and IN to the Warehouse foreman:

1. *OUT: Statistics on production, stock, staffing maters, accident and incident reports, disturbances, quality of service performed*
   IN: Info on long term changes regarding warehouse function, organization, work and report routines, technical systems
2. *Consultation regarding transports of incoming goods and packaging items*
3. *Consultation regarding stock-keeping*
4. *OUT: Information about goods flows, goods in stock, routines in practice, accident and incident reports, disturbances and data regarding customer complaints.*
   IN: Advise and information regarding work routines with respect to safety maters
5. *OUT: Requests for necessities, service and maintenance,*
   IN: statistics

6 , 7. Consultations regarding loading and fixation of goods

8. *OUT: Working schedules and periodic individual information regarding customer complaints*
   IN: Consultations regarding work practice, Reports on work load, deficient equipment.

11.4 Goals and Strategies of Goods Handler

11.4.1 Goals

When picking up and palletizing goods in accordance with a pick-up order list the goods handler has a number of different goals. In general terms some of them may be formulated as doing ones share of the work to satisfy fellow goods handlers, superiors and customers. In the present case this can be formulated, in a way relating better to the functional requests, as follow.

To arrange on the right place in the delivery area:

- well built, stable and "proper" pallets
- with the right products
- in right condition
- in right number
- in right time
- checked, registered in the delivery system and
- labeled and marked with the right addressee.

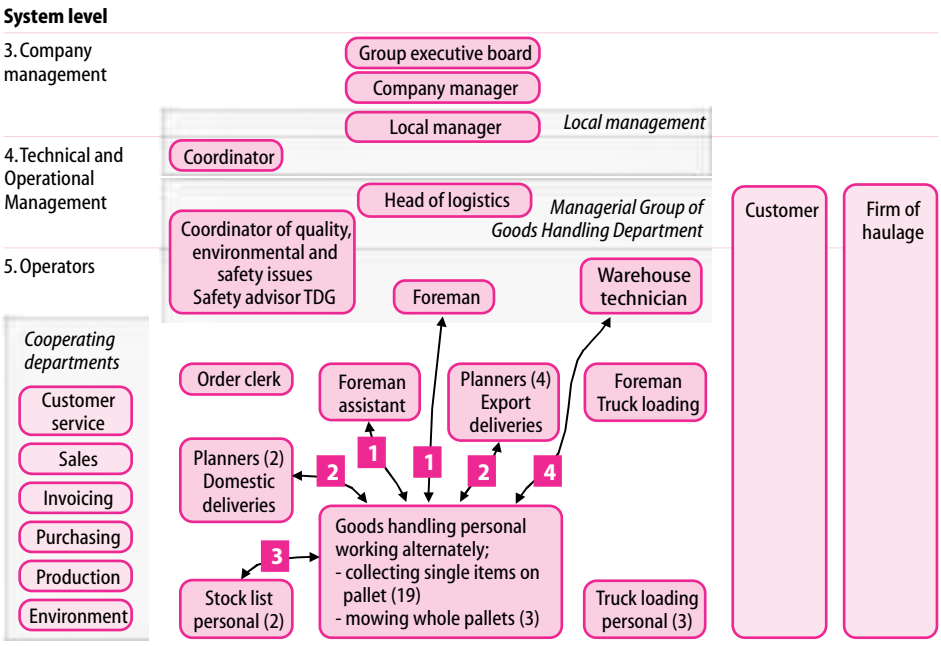


Figure 11.5 Information flow OUT from and IN to the goods handlers:

1. *OUT: Reports on work load, deficient equipment, incidents*
   IN: Working schedules, advise on work practice and periodic individual information regarding customer complaints.
2. *OUT: Signed pick-up order lists*
   IN: Pick-up order lists.
3. *OUT: Whole-pallet order*
   IN: Hole pallet cards
4. *OUT: Reports on state of equipment, requests for service*

11.4.2 Strategies

When the goods handler's task is to pick up goods and place it in the delivery area he does the following:

1. Collects a pick up order list in the order list stand.
2. Examines the list with respect to number, type, volume and weight of items.
3. Plans the picking sequence with respect to the information's considering his knowledge about form and strength of the packaging.

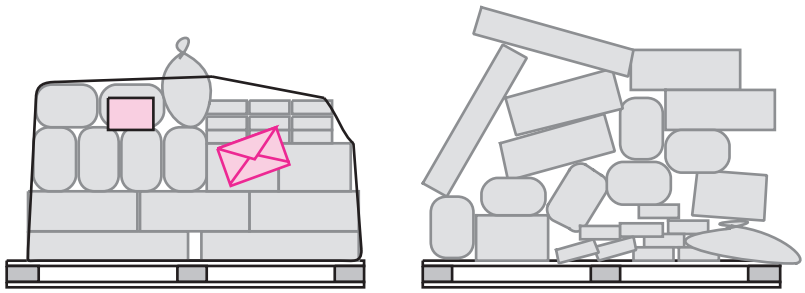


Figure 11.6. Stable piles of goods with fragile items on top, wrapped in foil and with proper labeling and receiver's address

The planning is normally restricted to what one pallet can hold. It results in a memorized plan, normally not marked on the order list. The computerized order management system does not give any assistance except by stating the number, volume and weight of the items.

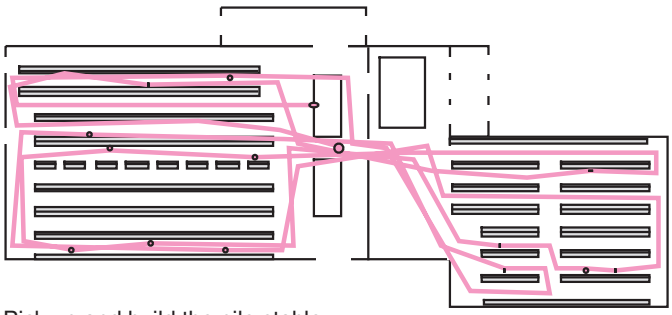
To get an idea of the goods handler's strategies, when they plan and accomplish the gathering of goods items on pallets the interviews were supplemented by an experiment. Ten identical pick-up order lists with about 30 different products were handed to ten goods handlers. The goods was to be placed on a single pallet and the goods handlers were asked to indicate on the list in what order they would pick up the goods. The results show that they plan their work with to different aims:

a. *Build stable pallets* – Place the goods on the pallet in such a way that a stable pile is formed and so that fragile goods is protected from physical impact during transport.

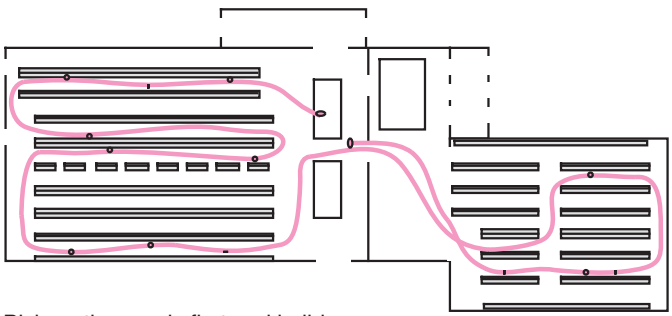
   Heavy goods and strong packages are placed in bottom layers and arranged such that the layers fixate each other. Small and fragile packages are placed on top and in cavities formed by arranging other goods around.

b. *Rational driving* – Reduce the total driving distance, the number of long movements and change of rack way during goods collection.

Both stable pallets and rational driving can be achieved by rearranging the goods when collected. The experiment indicates that individual goods handlers give different priorities to these aims and that no two suggest the same order of collecting the items. Two type strategies can however be recognized: pick and build or pick first and build afterwards, as indicated in figure 11.7 below.



Pick up and build the pile stable
with little attention to the driving distance



Pick up the goods first and build
the pile afterwards

Figure 11.7. Two strategies for collecting goods and building stable piles on the pallets. Goods handlers plan the pick up and build process by focusing on one or the other in an individual way.

11.5 Delivery Deficiencies

From data collected on a routine basis within the investigated warehouse function one can read the number and type of delivery deficiencies reported by customers, how they vary over time and who the goods handlers behind them are. By investigating these data and the circumstances behind them some experiences can be drawn that improve the understanding of how the work is carried out. This was done with data collected during a period of eight month.

11.5.1 Type of Deficiencies

There are tree types of deficiencies that can result from misses in the pick up process and in the concluding check-up routines:

a. *Wrong article* – This can be the result of picking goods without checking the identity after stopping at wrong pick-up place or if wrong product has been placed at the "right" place.
b. *Wrong number of* or *missing articles* – This can be the result if:
   - The article is picked up but later left behind when rearranging the goods
   - The article is missing or not present in adequate number at the pick up place and the necessary completion is missed after that the deficiency in the pick up place has been corrected.
   - The goods handler misses to "rest-note" not deliverable goods when dispatching the delivery.

Figure 11.8 indicates the possible direct causes of customers reporting deficiencies in deliveries applying for re-compensation and the goods handlers' part in these events.

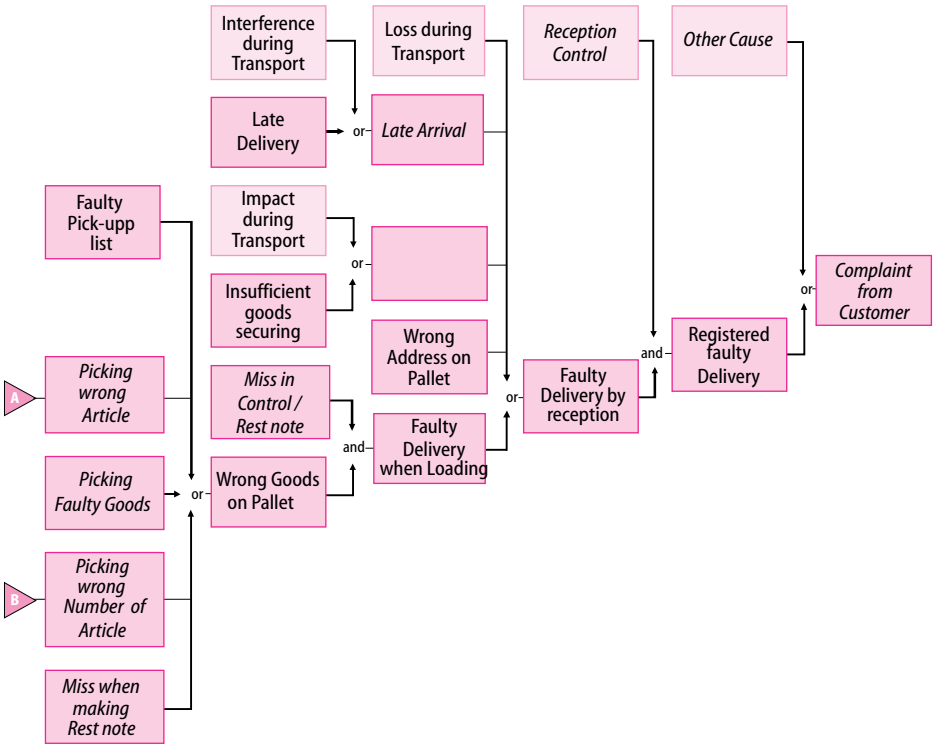


Figure 11.8. Possible direct causes behind customers reporting deficient deliveries and applying for re-compensation. Goods handlers perform activities that are indicated in the more deep coloured rectangles.

11.5.2 Number of deficiencies

Total number

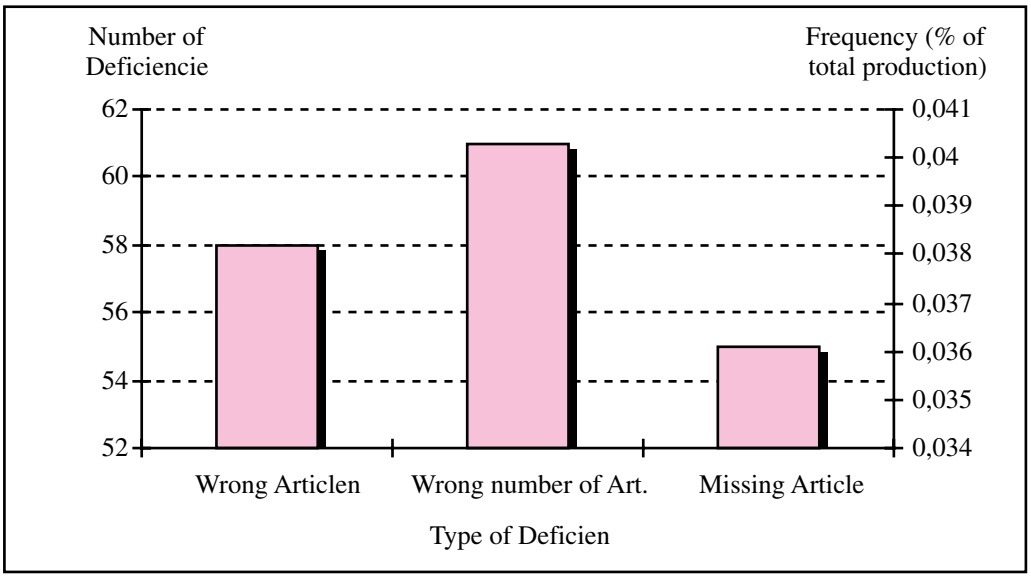


Figure 11.9 The total number of the tree different types of faults reported by customers as delivery deficiencies and the corresponding fault frequencies relative the total production in the warehouse during a period of eight month.

Performance variation among individuals

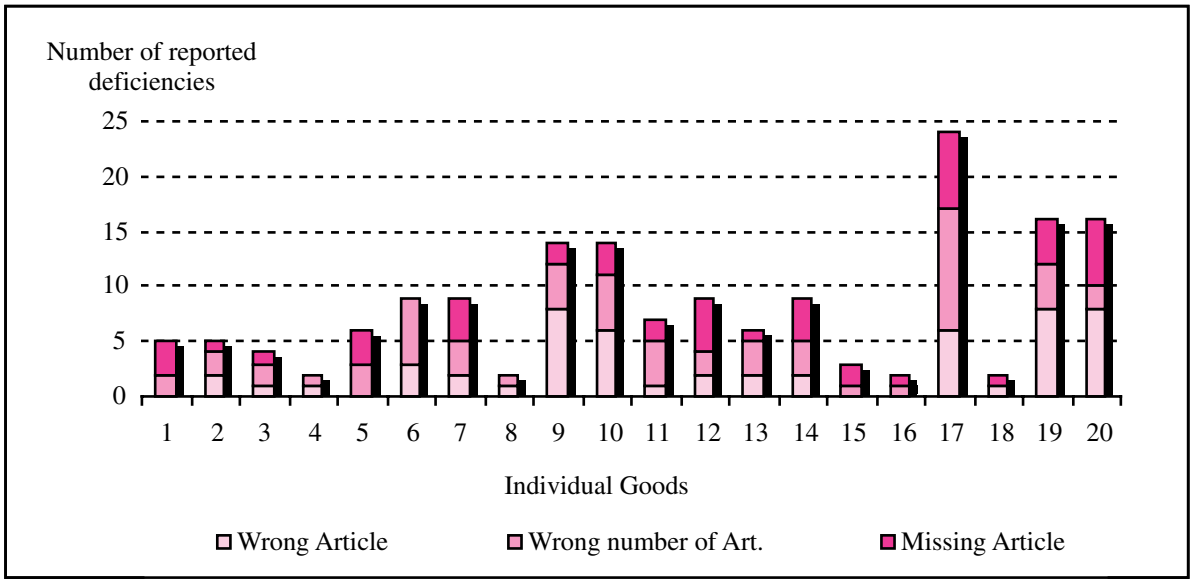


Figure 11.10. The number and type of reported deficiencies associated with individual goods handlers.

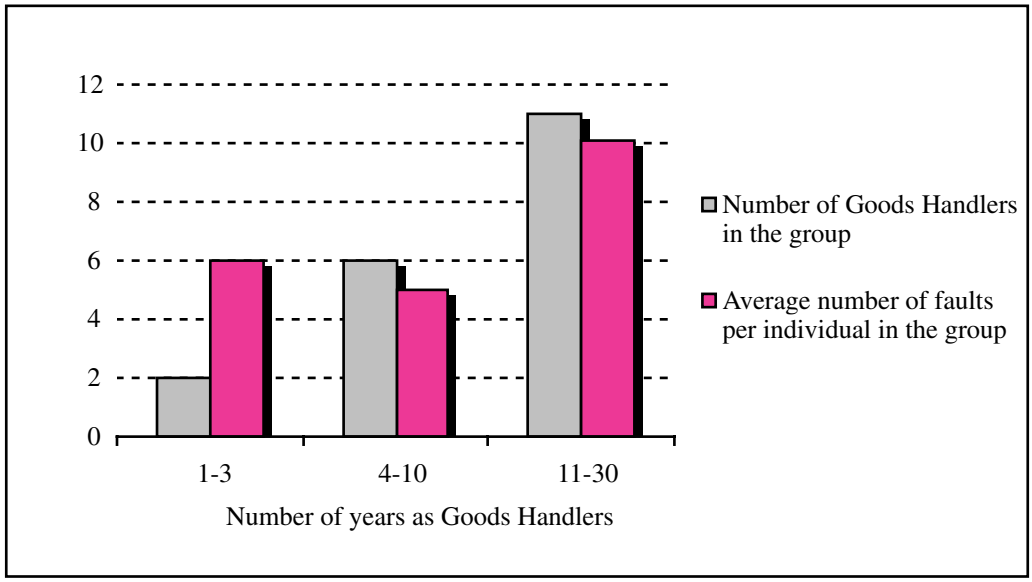


Figure 11.11. Numbers of deficiencies associated with goods handlers employed for different number of years.

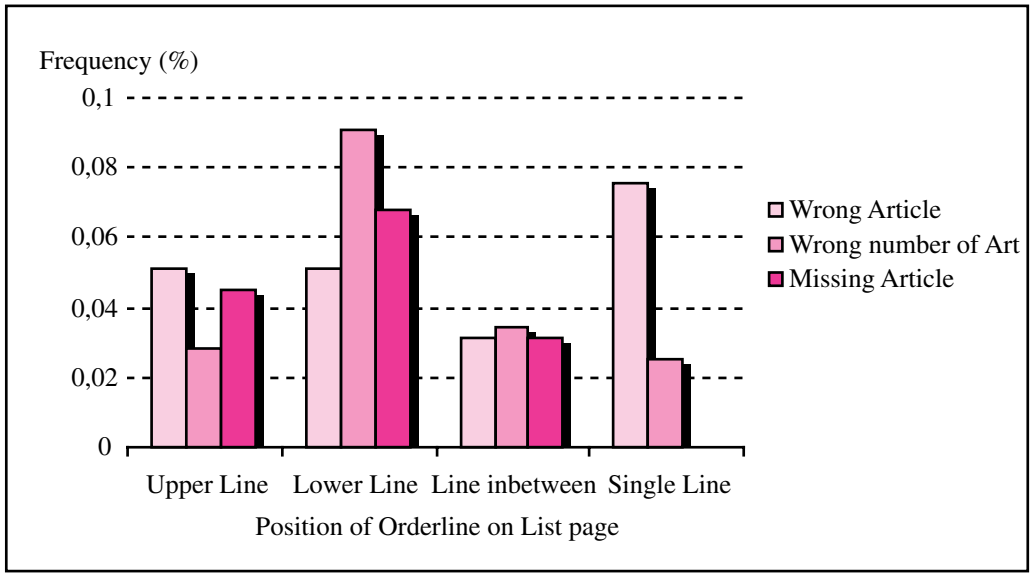


Figure 11.12. The effect of the items' position on the order list on fault frequency.

Effect of experience

Experts, when working in a well-known context, make more mistakes than novices occupied with the same task. This is an effect of a time-effort trade-off managed by experts when possibilities for self-control are prevailing since negative side effects then can be compensated for. Figure 11.11 indicates that experienced goods handlers also in the present context make more mistakes then those with less experience, as discussed in section 7.5.5 A more effective way of detecting misses would have allowed them to correct them.

Effect of position of order line on order list

From figure 11.12 it can bee seen that the probability of picking wrong number of articles is about twice as high if the items are indicated on the lower line of any list page and that this is the case also for "missing articles". The manual handling of the list and the possible confusions or lack in attention when turning page may be the reason for this. For single line order lists there is an over-representations of "wrong articles".

Direct causes for "Wrong Article faults"

When driving, the goods handler can, by mistake, end up in the wrong rack-way, on wrong side of it or in the wrong position along the rack. If the position and article numbers then are not verified when stopping, the pick-up and counting process will lead to a "wrong article fault". By analyzing where the goods handlers have picked the goods when such faults was identified, the following positioning errors were found:

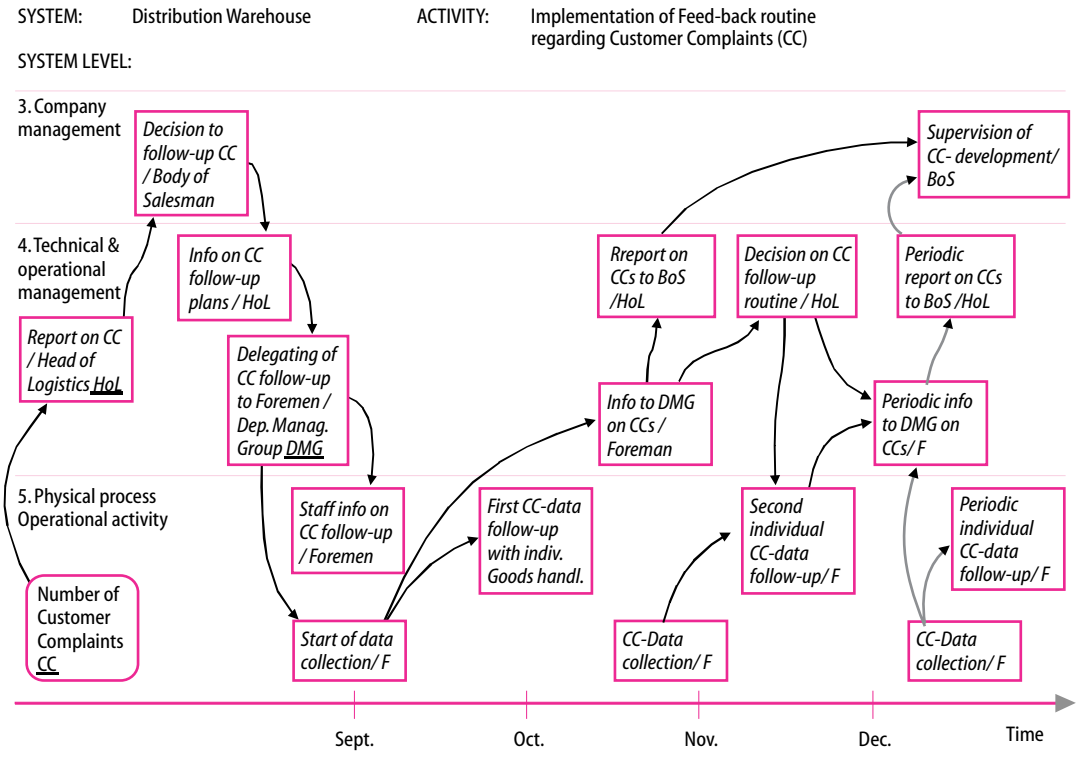


Figure 11.13. An ActivityMap indicating the implementation of a routine by which customers' complaints are analyzed and reported back to individual goods handlers.

	Percent of total
Right rack way and rack but *one* pick-up place away	46
Right rack way and rack but *two or more* pick-up places away	27
Right rack way but opposite rack	14
Adjacent rack way but "right" position along the rack	11
Wrong rack way and wrong position along the rack	3

11.6 Implementation of a feed back routine for complaints

Reports from customer service regarding complaints on deliveries had been collected during many years but not analyzed and reported back into the organization. In a general campaign to improve quality of service the statistics was recognized and a routine was implemented to secure a direct feedback to individual goods handlers of type and number of complaints in connection with deliveries attended by them. This process, which was introduced and evaluated by the warehouse organization, is described in the ActivityMap of figure 11.13.

11.7 Effect over time of the feed-back routine

The process of informing individual goods handlers on the type and number of reported deficiencies in connection with deliveries performed by them started in September according to figure 11.13. The effect of this process under a period of eight month is described in figure 11.14.A, were the monthly number of deficiencies reported is indicated together with the number of order lines administrated.

The positive effect of the feedback process seems to be quite pronounced for the first five month and then vanish. During the month of March the production is however quite higher than during previous month. By calculating the deficiency fre-

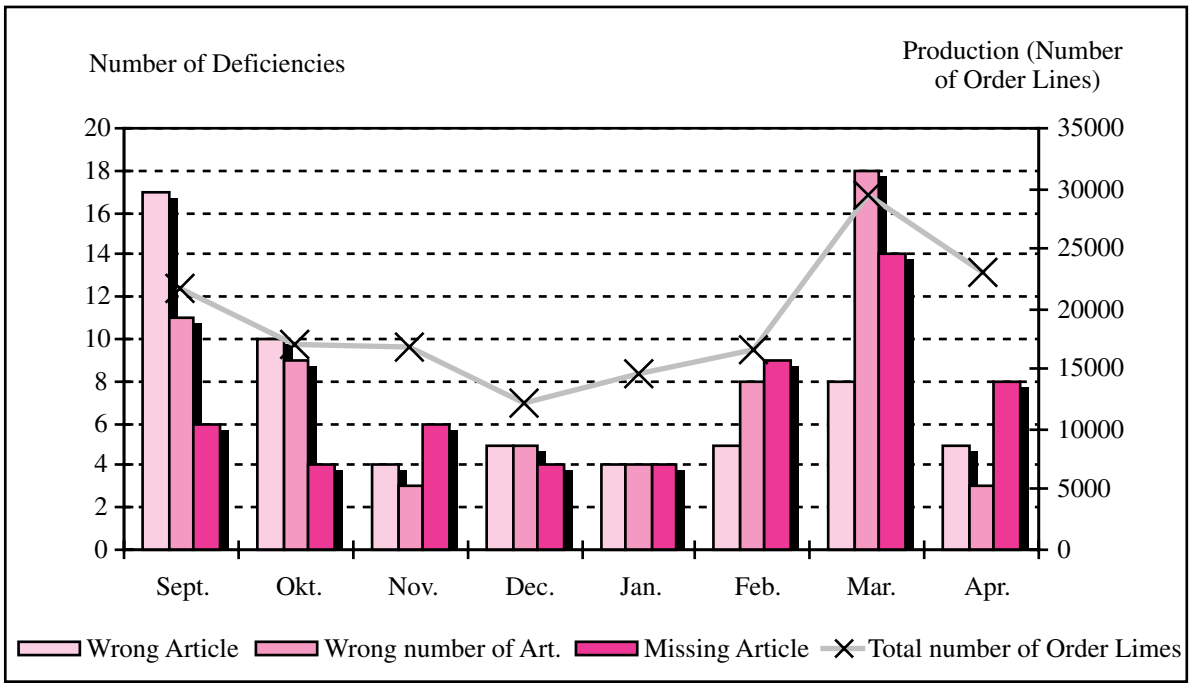


Figure 11.14.A. The variation in reported deficiencies and production with time during the first eight month after that the feed back process was implemented.

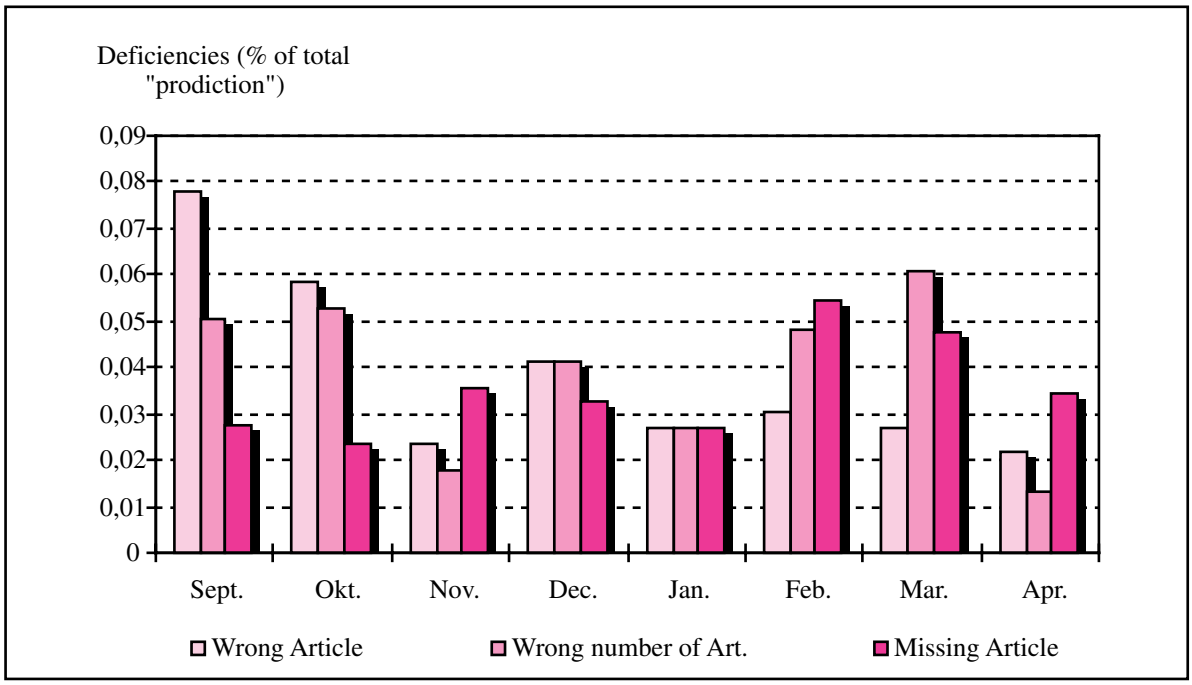


Figure 11.14.B. The variation in frequency of reported deficiencies during the first eight-month with personal feed back to individual goods handlers in the warehouse.

quency one ends up with the data in figure 11.14.B that show a steady decrease in the frequency of wrong product deliveries while that of wrong number of articles and missing articles increase during periods with high production rate. This may be explained by the fact that the probability of finding an inadequate number of goods items in the pick-up area is higher in periods with high goods flow. The process of requesting whole pallets of goods, to be transported to the pick up place, then has to be activated. This opens for mistakes.

11.8 Normal work of a warehouseman / an ActivityMap

The process of collecting goods as requested in a pick up order list and building a stable pile has been discussed in the paragraphs above. From the maps and data presented and from other experiences gained through interviews with most of the goods handlers in the warehouse, a picture of the pick-up process has been formed an shown in figure 11.15. In addition to the set of sequential activity steps indicated, the possible outcome of these steps is indicated and so is a number of factors that influence them. The self-control activities indicated are those that are influenced by the feedback process.

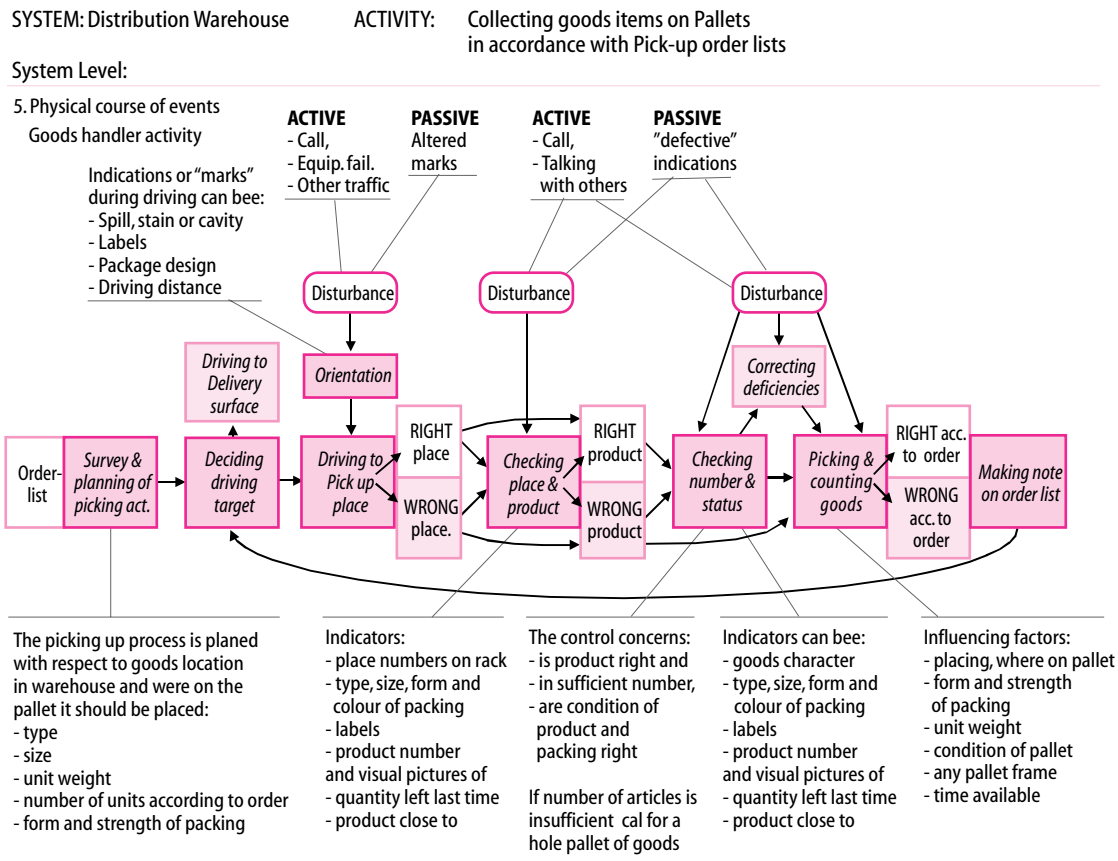


Figure 11.15 An ActivityMap of the Pick-up process performed by the warehousemen.

Appendix A: Accident Scenarios

Table of Contents

A.1. The Zeebrügge Accident,[1] Annotations

A.1.1 General

The Zebrügge accident happened on the 6th of March 1987. The Roll on/Roll off ferry Herald of Free Enterprise carried approximately 459 passengers, embarked for Dover, 81 cars and 47 freight vehicles. A crew of 80 hands manned the ferry all told.

The weather was good, with a light easterly breeze and very little sea. The ferry left and past the outer mole at 18.24 and capsized 4 minutes later.

(1): The ferry was built for the Dover-Calais connection and both of these harbors have two level berths capable of loading both car decks of the ferry. Zeebrügge has only a berth for one level ferries and, consequently, it was necessary to raise the

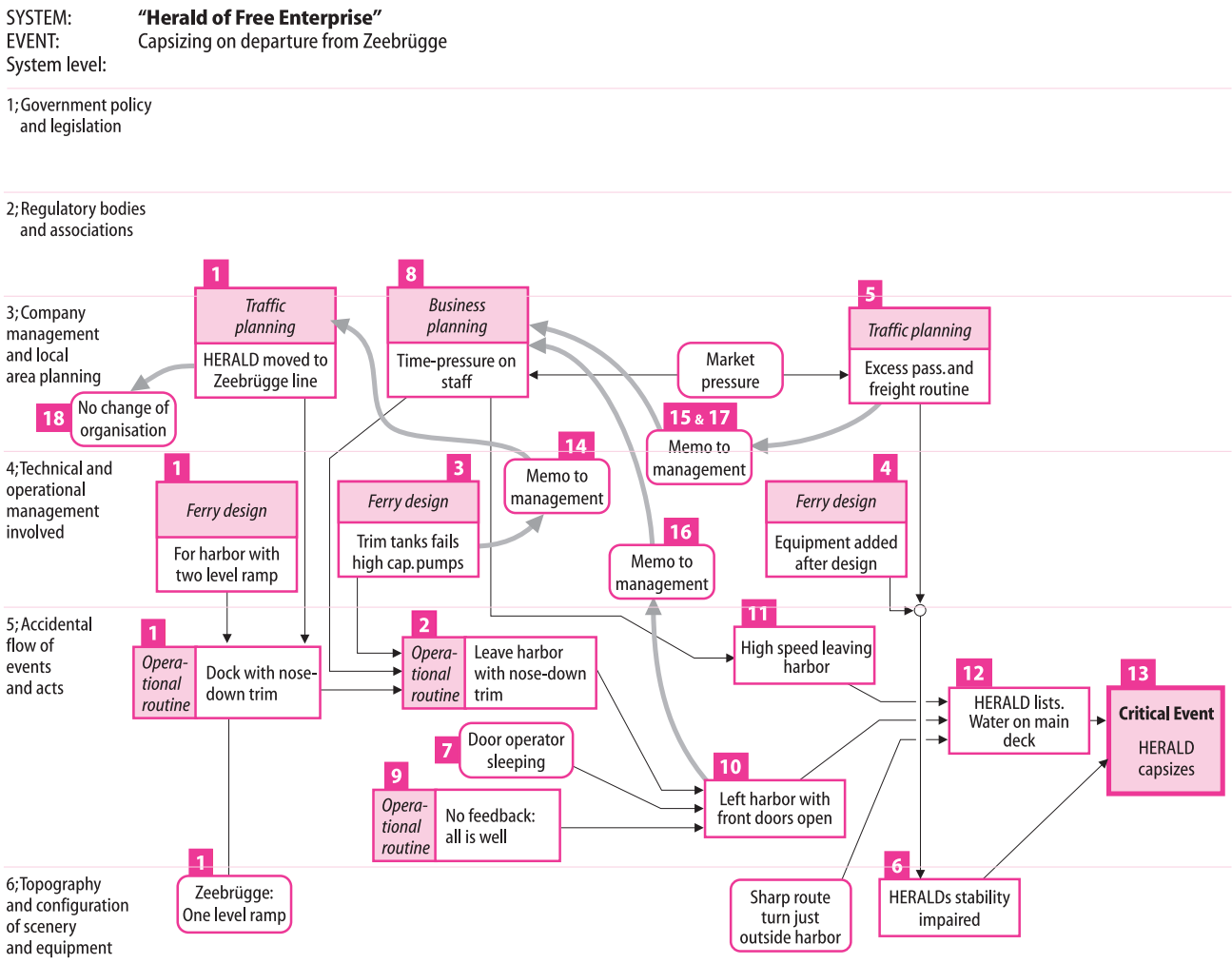


Figure A.1.1
An AcciMap representing the Zeebrügge accident. Numbers refer to the bold bracket-numbers below.

1. Notes to: M.V. Herald of Free Enterprise. Report of Court No. 8074, ISBN. 011 550828 7, Department of Transport, November 1987. London: Her Majesty's Stationary Office. *Numbers in brackets refer to sections in this report.*

ramp so that it reaches upwards to the upper deck also. When loading during high tide, it was necessary also to trim the ship by ballast to allow the ramp to reach the upper deck.

(2): The general practice was to start flooding the ballast tank two hours before arrival in order to berth with the appropriate trim by the head.

(3): The forward tanks were on the main ballast line but were not connected to the high capacity pumps.

(4): The Herald was, due to modifications, about 250 tons heavier than the Builders' original estimate.

(5): The average excess load of the freight vehicles was about 13 %. This was the case for all the Free Enterprise ferries (8.4). At departure, the ship had "a mean draught of between 5,68 and 5,85m with a trim by the head of about 0,8m."

(6): "A probability is that the draught and trim approached the upper limit condition and that the ship was in fact overloaded significantly at departure." This was not in any way causative, but "the real significance is in the lessons to be learned from it," in the present context, about the boundary seeking adaptation (8.5).

(7): It was the duty of Mr. S. to close the bow doors. He opened the doors on arrival and was then busy supervising maintenance and cleaning. Following this, he fell asleep in his quarters and he did not wake up on the "Harbor Stations" call on the public address system. He remained asleep until he was thrown out of his bunk by the capsize (10–1).

(8): Why could the responsible loading officer not just wait the three minutes on the G deck to see the doors close? In fact, there was significant pressure to leave port and, consequently, the officers normally went to the bridge to make sure they could leave port immediately after loading was finished. Frequently, the "Harbor Stations" call was given before the loading was finished. (11–1).

Considerable pressure by company memoranda was on leaving Zeebrügge at the earliest possible moment, due to very tight time schedules at Dover which caused delayed arrivals at Zeebrügge: "Let's put the record straight, sailing late out of Zeebrügge isn't on. It's 15 minutes early for us." On this day, they were running late and Herald left harbors 5 minutes late (11–3).

(9): The ready-for-sea instruction states: "Heads of departments are to report to the Master immediately they are aware of any deficiency which are likely to cause their departments to be unready for sea in any respect at the due sailing time. In the absence of any such report the Master will assume at the due sailing time that the vessel is ready in all respects." On the day of the accident, the captain saw the chief officer come to the bridge. The chief officer did not make a report and the Captain did not ask for one. (12.4).

Standing orders "1. made no reference to closing the bow and stern doors, and 2. they appear to have led Captain L. to assume that his ship was ready for sea in all respects merely because he had no report on the contrary." (15.3). (Note: Interestingly, the management had several memoranda saying that the ship was not 'ready for sea'). (15.3).

The company's ship standing order makes no reference to the closing of the watertight doors. Before the disaster, there had been no less than five occasions when one of the company's ships had proceeded to sea with bow or stern door open. Some of these were known to the management who had not drawn them to the attention of the other masters. (12.5).

Capt. K. adopted the general instruction issued by Capt.. M.: "The officer loading the main vehicle deck, G deck, to ensure that the water tight doors are secured when leaving port." He was content that there had been sufficient compliance with that instruction if the loading officer ensured that the assistant bosun was actually at the control position.

(10): The bosun, Mr. A., was working at the G deck and was the last man to leave it. He was working close to the bow doors and saw nobody there to close them. Asked whether there was any reason why he did not close them, he stated "It has never been part of my duty to close the doors or make sure anybody is there to close the doors." (10–2)

A general instruction prescribed that it was the duty of the officer loading the main vehicle deck to ensure that the bow doors were "secure when leaving port." That instruction was regularly flouted, taken to imply that is was the duty to see that somebody was at the controls. (Context governed cue utilization) (10–4).

Mr. M., the second officer went to the G deck to relieve the chief officer who later left Mr. M. in charge of loading. When there were still 20–25 cars to load, Mr. M. on his radio overheard the chief officer issuing orders. He assumed then that he was no longer to exercise his responsibility as the loading officer was: "He took over as loading officer, so I assumed he took the responsibilities that go with the job." (10–5).

The chief officer, Mr. S., did not dispute that he took over and that it was his responsibility to make sure the bow doors were closed but he, also, interpreted it as merely the duty to ensure the controls were manned. (10–6).

(11): The Master and deck officers testified that when entering or leaving Zeebrügge with the ship trimmed by the head care was taken to restrict speed to a level which would avoid water coming over the bow spade. However, on passing the outer mole, Capt. L. sets the machine controllers at 6 on all three engines, and Herald accelerated rapidly to 18 knots. Model tests and experiments with a sister ship show that this caused a bow wave 2m above the level of the top of the spade (9–2,3). The captain did not follow stated practice.

(12): A large quantity of water entered G deck and caused an initial lurch to port due to free surface instability which was extremely rapid and reached perhaps 30 degrees and

(13): the Herald capsized (9–3).

A.1.2 Memos to management

(14): *Need For High Capacity Ballast Pumps:* In a memorandum, Mr. C., a Chief Engineer, he listed a number of problems and proposed high capacity ballast pumps: "Pumping time amounts to approximate half the normal passage time." Mr. D. "appeared to think that the chief engineer was grossly exaggerating the problem." – Mr. D. appeared to think that the HERALD was designed to proceed to at sea trimmed by the head, despite the fact that he had no stability information for the ship in that trim." (20).

(15): *Excessive Passenger Numbers:* Captain B. and Captain P. sent several memoranda to the management complaining about excessive passenger numbers (40–250 in excess), due to unreliable ticket and head counting on shore. Captain D.S. stated in a memorandum after complaining over excessive passenger count that: "This total is way over the life saving capacity of the vessel. The fine on the Master for this offense is L50.000 and probably confiscation of certificate. May I please know what steps the company intend to take to protect my career from mistakes of this nature." (17.7).

And so on, but the company in responses only discussed possible reasons for the miscount. The court "reluctantly concluded that Mr. Y. (the director) made no proper effort to solve the problem." (17.14).

(16): *Indicator Lights:* Memorandum by Captain B.: "Mimic panel- there is no indication on the bridge as to whether the most important water tight doors are closed or not. That is the bow and stern doors. With the very short distance between the berth and the open sea on both sides of the channel this can be a problem if the operator is delayed or having problems in closing the doors. Indicator lights on the very excellent mimic panel could enable the bridge team to monitor the situation in such circumstances." (18.4).

Mr. D. circulated the memo and got comments back like: "Do they need indicator lights to tell them whether the deck storekeeper is awake and sober?" – "Assume the guy who shuts the doors tells the bridge if there is a problem." (18.5).

In the memorandum the management states: "In short, if the bow or stern doors are left open, then the person responsible for closing should be disciplined." – – – "So in conclusion, the Bridge indicator is a 'no go.' " (18.7).

(17): *Ascertaining Draughts:* "It is a legal requirement that the Master should know the draughts of his ship and that these be entered in the official log book before putting to sea." (19.1). "Capt. L. told the Court quite frankly that no attempts had been made to read the draughts of his ship on a regular basis or indeed at all in routine service. Fictitious figures were entered in the Official Log that took no account of the trimming of the water ballast" (19.2).

A memorandum from Capt. M.: "For good order I feel I should acquaint you with some of the problems associated with one of the Spirit class ships operating to Zeebrügge using the single deck berths". – – – "As you probably appreciate we never know how much cargo we are carrying, so that a situation could arise that not only are we overloaded by 400 tons but also trimmed by the head by 1,4m. I have not been able to see how that would affect our damage stability." The response

of the director: "Initially I was not happy." Later he said: "I think that if he had been unhappy with the problem he would have come in and banged my desk." – – – "If he was that concerned he would not have sailed. I do not believe there is anything wrong sailing with the vessel trimmed by the head." (19.3).

Memorandum to Mr. A., a naval architect who was a director of the company at the relevant time, by Capt. B.: "With all our ships it is very difficult to read the draught with the result that for record purposes it is often as not guestimated. Suggest fitting automatic draught recorders with read-out in the wheel house." Mr. A. did not answer that memorandum. (19.4).

A.1.3 Organizational Issues

(18): *Lack of Organizational Update:* The staffing on the Zebrügge route was different. The passage took 4,5 hours, which is substantially longer than Dower-Calais and, therefore, the officers have more time to relax. The company therefore employed a Master and two deck officers instead of Master, two chief officers and a second officer. This was according to regulations, but the company *did not consider* that this required a change of the organization. Company standing orders were issued for the ferry covering the use in the Dower-Calais passage but were not extended to the Zebrügge passage. This raises the question concerning the effect of management issuing operating instructions signaling that the staff should obey rules and, at the same time, expect them to modify rules when circumstances are changed.

Capt. K. had repeatedly sent memoranda to management to have more permanent staff on the Herald. 30 deck officers served from 29 Sep. 86 to 5 Jan. 87. "To make matters worse, the vessel has had an unprecedented seven changes in sailing schedule. The result has been a serious loss in continuity. Shipboard maintenance, safety gear checks, crew training and the overall smooth running of the vessel have all suffered." (13.1).

"The board of directors did not appreciate their responsibility for safe management of their ships. They did not apply their minds to the question: What orders should be given for the safety of our ships? – – – There appears to have been a lack of thought about the way in which the HERALD ought to have been organized for the Dover/Zeebrügge run."

The failure on part of the shore management to give proper and clear directions was a contributing cause of the disaster."

A director, Mr. D., said "he felt 'it was more profitable not to define the roles but to allow them to evolve.' " – – – "It demonstrates an inability or unwillingness to give clear orders. *Clear instructions are the foundation of a safe system of operation.*" (Emphasis in original). (14.2).

Court discussing standing orders: "*Any set of orders must be so drafted that every expression therein has only one meaning throughout the order.*" (Emphasis original) (15.2).

A.2. The Clapham Junction Railway Accident[1] Annotations

A.2.1 The Event

During November 1988, the signal system of Clapham Junction was being modified. On 10 Dec. the weekly operating notice instructed that "signal WA25 has been abolished and a new 4 aspect automatic signal WF138 has been approved." (1.1). (Numbers in brackets refer to the section numbers in the court report):

"It was that new signal, WF138, which two days later in the morning rush hour of Monday, 12 December failed to prevent a second train from occupying the same track as an earlier one and failed to stop the front of the second from running into the back of the first." (1.1). 29 trains had passed the cutting in the two hours prior to the 8:10 train, driven by Mr. McC. He experienced an unexpected set-back when the signal WF138 had changed from green to red when he was almost on top of it, so that he had no chance of coming to halt before passing it. The reason for signal WF138 suddenly turning red was because the preceding train had moved from the faulty track circuit where it was invisible. He had, unwillingly committed a "signal passed at danger" for which the rulebook requires immediate stop and report to signalman. He stopped to use the signal post telephone (2.44). *The next train from Pool could not see the train due to a curve and runs straight into the back-end of the holding train* (3.11).

The cause of the faulty signal indication was a sneak path in the signaling system due to inappropriate modification of its wiring:

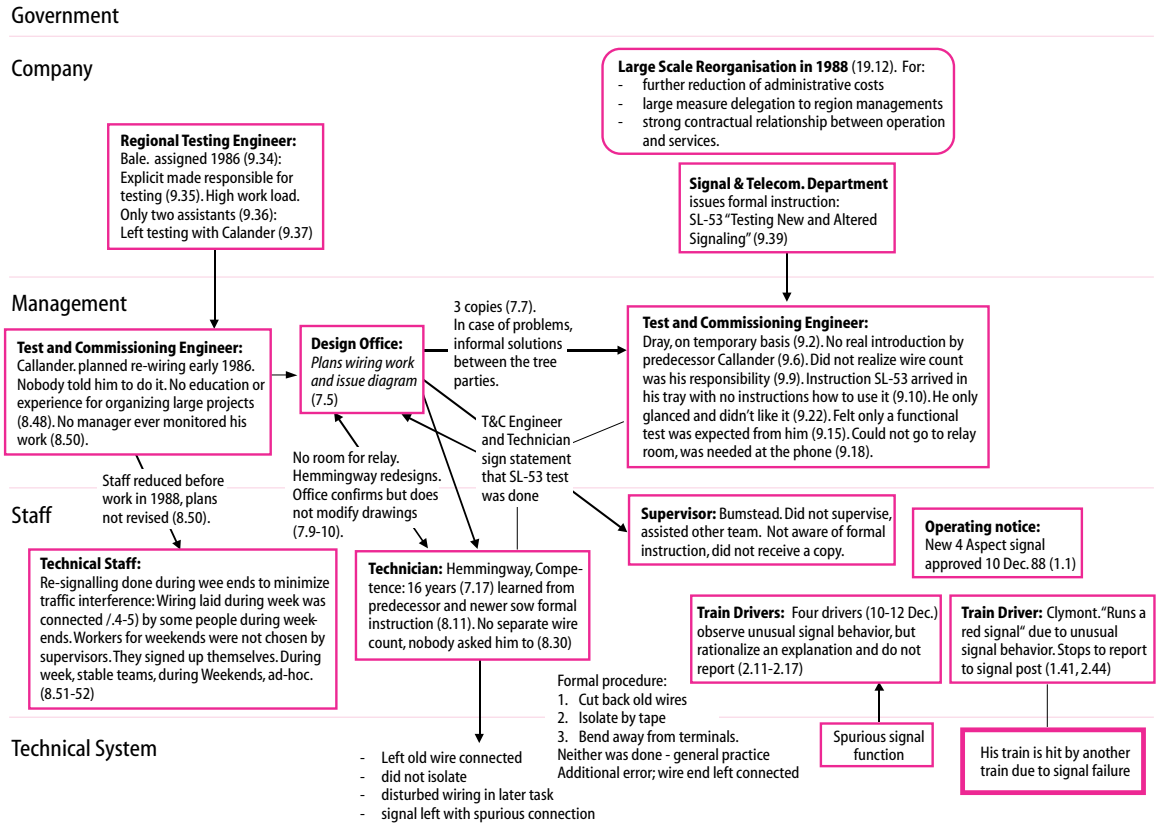


Figure A.2.1

1. HMSO (1989): *Investigation into the Clapham Junction Railway Accident.* The Department of Transport. London: Her Majesty's Stationary Office, 1989. *Numbers in brackets refer to sections in this report.*

On Sunday, 27 November 1988, Mr. H. was to transfer the signal function from the old WA25 to the new WF138 (1.33) by connecting the new wires and disconnecting the old wiring. Since the signal wiring was old an brittle, the WA25 wires should not be removed, but the formal procedure included safety precautions against sneak paths in the old wires by 1) disconnecting wires in both ends, 2) cutting back wire ends, and 3) isolating ends by tape. This was not done, and the old wires were just pushed aside and left connected in one end (1.35).

On 11 December 1988, Mr. H. is working on another modification in the same relay rack. This involves replacement of a relay in the same rack. The relay is heavy and during manipulation of the relay, Mr. H. disturbed the wiring left over from the previous modification and creates a sneak connection in the signal WF138 circuit (1.37).

There would be no disaster as long as there were trains kept running through the cutting with enough gap between one train and the train ahead of it (1.40). "However, when driver Mr. McC. stopped the 07:18 Basingstroke-to-Waterloo train at signal WF47 to telephone the signal man, in the utter faith of a railway man that the signal behind him, WF138, HAD to be red, it was not (1.41) and the accident happened.

A.2.2 Task Performance

Mr.H. had been with BR for 16 years, was held in high regards of colleagues and supervisors, had experienced no critique, thought he did a good job (7.17). He is both meticulous and consistent in his work. However, he learned the job from watching predecessors, he never saw a job description nor had formal instruction (8.11).

The only explanation is that he was interrupted by some event. (8.20). The morning of 27 November was a bit unusual, work did not go as smoothly as expected (7.20).

As mentioned, due to the danger in disturbing brittle wiring from removing old wires, a safe alternative had evolved based on 1) cutting back old wires, 2) insulating by tape, 3) bending back from terminals. However, this was not done (7. 26). It was standard practice not to cut back wires, or by tying back (8.3). In addition to the errors of normal practice, one wire end was left connected, which would have been found by wire count (8.18). However, Mr. H. never did a separate wire count at the end of his work. He did as he got along. Nobody taught him to do the separate one. Nobody ever checked his work (8.30).

A.2.3 Work Planning

The 4-aspect signal had been in use since 1920, there was nothing new or unusual in the design (1.29). However, the modification leading to the accident was part of a massive re-signaling operation had taken many years to plan initially and many years in obtaining the financial approval (1.31). The report states that it is "important to look at the disturbing length of time which the resignation project took from its first seeds in the year 1978 to its imminent completion in the near future (1.32).

Mr. C. was planning the rewiring very early in 1986. Nobody told him to do it; he had no education or experience in organizing such an extensive work. Furthermore, for the planning "he was using staffing levels from 86 which were to deteriorate significantly over the next two years." (8.48).

The re-signaling work was done during weekends to minimize traffic interruption (7.4). The weekends workers were not chosen by supervisors, they signed up themselves 8.51). During the week, people were working in stable teams, during weekends teaks were assembled ad-hoc (8.52).

The new wiring was laid during the week and usually connected during weekends by the same people, working according to diagrams prepared by the Design Office some time in advance (7.5).

Three copies of such diagrams would be issued to the Signal Works Assistant, one copy for Testing and Commissioning Engineer, one for the work supervisor, one for the senior technician doing the work (7.7).

In case of problems, they were worked out informally between technician, supervisor, and design office (7.8). That was the case here, too little room was found for an extra relay. Mr. H. redesigns (7.9) and gets confirmation from design office, which does not issue a modified wiring diagram (7.10).

A.2.4 Work Supervision

As mentioned, Mr. H. did not do a separate wire count to verify his work. And, as it turns out, nobody ever did visual inspection or wire count to test his work (7.22):

The *supervisor*, Mr. B., did not actually supervise. As a result of the limited numbers available to work and his confidence in Mr. H., the supervisor spent his time working with another team (8.36). Due to heavy workload for this other team, he was working long and hard and carrying out manual work himself (7.31).

Another safety net should have been the presence of the *test and commissioning engineer*, Mr. Dray, on the scene. Mr. D. did not test or wire count (8.43). Neither did he do a visual inspection (7.34). If he inspected the relay racks he only looked at eye height (8.42).

A.2.5 Staff and Work Management

British Rail underwent a large scale reorganization 1988 with a three fold aim: 1) reduction of administrative costs, 2) large measure delegation to new tier of management at regional level, and 3) ensure strong contractual relationship between operations and services (10.12).

This had a number of consequences: People were leaving due to the extensive weekend work (8.49). One tester in each area (10.15) replaced regional testing teams composed by three men.

A.2.5.1 THE SUPERVISOR

The management of instructions in the organization was ineffective: 11 May 1987 S&T Department issued a Departmental Instruction SL-53: "Testing New and Altered Signaling" specifying wire count. The supervisor, Mr. B., did not receive a copy (9.39). He was neither aware of the work instruction, nor of the good testing practice (8.41). No adjustments were ever made for this and no manager above Mr. C. ever monitored his work (8.50).

A.2.5.2 THE TEST AND COMMISSIONING ENGINEER

There was no permanent test and commissioning engineer for the region. MR. D. took a vacancy on a temporary basis (9.2). He lived at Ashford and due to reorganization his position as resident site engineer at Washford had disappeared. He was "displaced" and had been unsuccessful in 4–5 applications for other jobs. He did not want the job at Wimbledon for reason of the travel involved, but accepted it without enthusiasm for 6 weeks until the replacement of Mr. C. could be found (9.3).

Mr. D. had no real introduction training by Mr. C., during the overlap, the worked at different times, met only in the morning and Mr. C. did not realize that Mr. D. "would be in his shoes" (9.6). Mr. D. had not done wire count for 10 or eleven years. He knew the "Provisional SL instruction" from 1985 as a discussion document, he commented on it, but was never formally informed of its actual authorization (9.7).

The test and commissioning engineer, Mr. D., did not realize that wire count was his responsibility, neither did the supervisor nor Mr. H. (9.9). 11 May 1987 the Departmental Instruction SL-53 was issued and arrived in Mr. D.'s in-tray with no instruction how to apply it, it was just another document (9.10). Mr. D. made no attempt to put SL-53 into practice and nobody senior to him told him to. Mr. D. said a practice had developed where he felt a functional test was what was required from him (9.15). Mr. D. said that if he were responsible for an independent wire count, he would have had to ask an assistant to do it. He was on the signaling floor and could not leave for the relay room, because he was needed at the phone (9.18).

The former Test and Commissioning Engineer (T&C-E), Mr. C., never read the work departmental instruction SL-53 which dropped into his basket. He realized it was a Departmental Instruction and he had to read it carefully. However, he only glanced it (he perceived no problems). He did not like it (9.22). He did not believe he would be able to do all the things that were stated by the instructions (9.23). "The entire responsibility for the testing of new installations on the WARS scheme was placed in the hands of a man who never read SL-53 and had never worked to it. At no stage, the superiors inquired whether he was doing so and never discovered he was not." (9.26).

The technicians and the T&C-E had to sign a certificate stating that the test was done in agreement with SL-53 (9.27).

A.2.5.3 REGIONAL TESTING ENGINEER

4 August 1986 Mr. B. took up the role of Regional Testing Engineer (9.34). At a construction group meeting, he was explicitly instructed that he was responsible for the standard of testing (9.35). But nobody informed him, how he should raise the standard of testing. He had a very high workload and only two assistants. (9.36). The testing of WARS was left to Mr. C. because the workload did not allow the Regional Testing Team to cope with WARS (9.37).

A.2.6 Operational Feedback

Four drivers before the accident had noticed that the signal, in an unusual way, shifted from green to a more restrictive signal (double yellow). They all, however, rationalized an explanation (such as interference by a signalman) and did not report the event. Which was judged to be not in conflict with the intention of the rule system (2.11–2.17).

A.2.7 Previous Incidents

A.2.7.1 OXTED INCIDENTS, 1985:

Three incidents from unreliable commissioning of modifications: Wrong-side signal failures from wiring faults that would have been detected by wire-counts. These were not made (9.48). Only effect of the investigation: brief flurry of paper work, the assignment under Mr. B. of a regional testing team to raise the standard of testing, but adequate resources were not given (9.53).

A.2.7.2 QUEENSTOWN ROAD INCIDENT, 1988:

Re-signaling had been approved (9.62). Wrong-side signal error appeared which was detected because the driver could see the previous train at a straight section of the railway line (9.64). The design department issued an erroneous drawing, lacking a signal circuit, and the fault was not detected in test (9.65).

A.2.8 Lesson Learned

The report realizes the presence of systemic factors: "There were other factors causative of the Clapham Junction accident which are not so much faults which can be attributed to any individual as faults of the system and the way in which it was run" (16.74).

A.3. Road Transport of Diesel oil / Accident along Stream Mieån, Annotations[1]

System: Truck and trailer with full cargo of diesel oil running on main road NR 29 along stream "Mieån" in the county of Blekinge, Sweden.

Event: Loss of containment of diesel oil. The cargo tank, mounted on the trailer, cracked when ditching, tipping over and running into a bolder in the roadside. The roadway was slippery due to snowfall; the narrow and curved road was blocked by another truck and the speed of driving to high for the circumstances to allow for a controlled stop.

Date: 940118

Numbers given in figures A.3.1.A and A.3.1.B correspond to the numbers and annotations below:

A.3.1 Preconditions

1 The section of the road NR 29 that is running along the stream "Mieån" is winding and narrow (breadth 7m). Maximum driving speed is 90 km/h, 70 km/h in parts, and the connecting roads out are numerous. Roadsides are not cleared from boulders.

2 Traffic intensity; 1 800 vehicles per day (over the year average) of which 300 are heavy and 200 carrying dangerous goods.

3 Two fish farms are located along the stream Mieån and 25

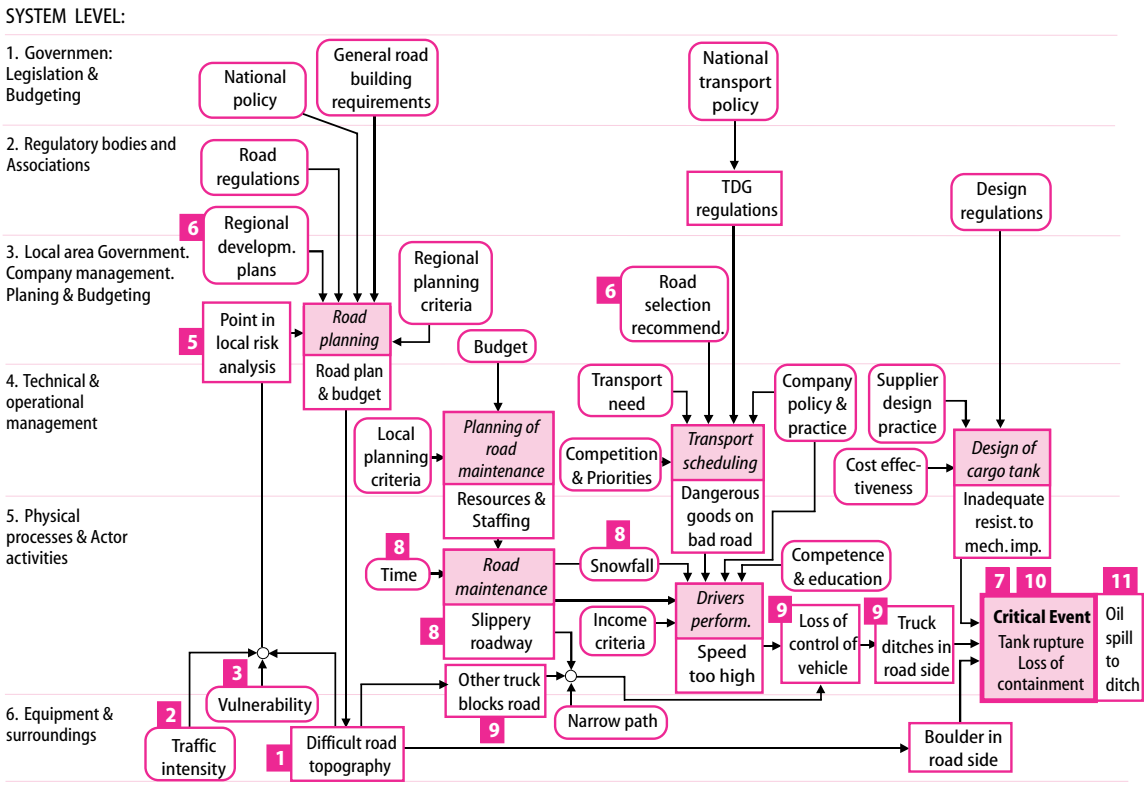


Figure A.3.1.A
The AcciMap describing conditions and development before the critical event. Numbers refers to notation numbers below.

1. The annotations refer, if no other reference is indicated, to the report by the county administrative board of Blekinge, Sweden. The report, which is in Swedish, is entitled: Trafikolycka med farligt gods på riksväg 29 den 18 januari 1994, Länsstyrelsen i Blekinge, Rapport, 4 mars, 1994.

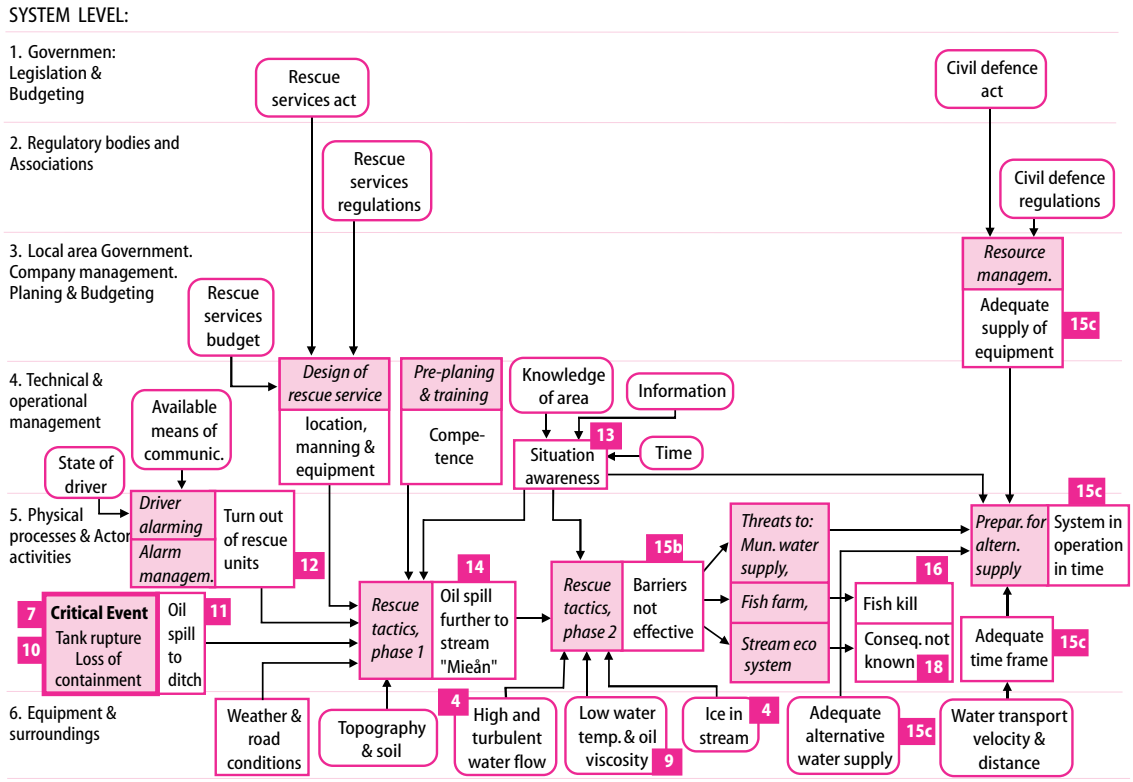


Figure A.3.1.B
The AcciMap describing conditions and development after the critical event. Numbers refers to notation numbers below.

km downstream of the place of accident is located the row water intake of the municipal Karlshamn with 28 000 inhabitants. The stream was holding a number of rare species and considered as an environment particularly worthy of preservation

4 The stream was partly cowered with ice and the water flow strong and turbulent for the period.

5 Risks concerning dangerous goods accidents along the road in question attracted much attention for a long time before the event and the problem was dealt with in land use plans, in rescue plans and in the municipal risk analysis.

6 Demands for prompt measures to increase safety on main road 29 on the section along "Mieån" had bean risen by the regional government (Road selection recommendation for transports of dangerous goods in the county of Blekinge, Report; County of Blekinge, Dec. 1993)

A.3.2 The Accident

7 Time of accident 10,30 a.m. January 18 1994.

8 There was a heavy snowfall from 09.00. Dray salt was spread on the roadway at 09.15. At the time of accident the roadway was coated with snow and slippery.

9 The driver of the truck and trailer in question, carrying in total 30 tons of light fuel oil ("green" diesel oil), discovered an other truck at still blocking the roadway and tried to stop. The trailer ditched, tipped over and collided with a bolder in the roadside.

10 *Critical event*; 3 of 4 sections in the cargo tank of the trailer were penetrated and about 15 m^3 of the oil flew into the ditch.
11 The flew of oil followed the ditch about 20 m and into a marshy area in direct contact with the stream Mieån.
12 Alarm; The truck driver alarmed the SOS-central at 11.09 a.m. and the alarm was passed on at 11.15 a.m. to the rescue service station of Karlshamn and the police force in Tingsryd.

A.3.3 Rescue phase 1

13 The rescue force from Karlshamn arrived at 11.50 a.m. The rescue leader promptly informed the political leader of the municipal, its technical and environmental management, a decontamination firm and the rescue force of Tingsryd. Also the owners of the two fish farms were informed.
14 The aim of the first face of the operation was to prevent the stream Mieån from inflow of oil. When this work was finalised, at 12.00 a.m. day 2, most but not al of the spill had been captured in the marshy area along the ditch from the place of oil spill to the stream.

A.3.4 Rescue phase 2

15 The second face of the operation aimed at:
   a. Decontamination of the marshy area. (Successful but costly and time consuming)
   b. Supervision and prevention of further dispersion of oil along the stream. (The prevention was not successful due to turbulence and the presence of ice in the stream, Oil was detected at the row water intake 4 days after the accident)
   c. Preparation for an alternative row water supply for the municipal of Karlshamn. This operation was successful. Reasons for this was that:
      – an effective organisation was formed,
      – an adequate alternative water supply (Stora Koksjön) 2,4 km from the waterworks was available,
      – an adequate supply of equipment for 10 pipes in parallel (60 km in total) with motor pumps, thermal isolation and a total capacity of 115 l/sec was available,
      – there was adequate time for its installation.

A.3.5 Consequences

16 The two fish farms reduced there water intake from the river but oil exposure killed 500–600 fishes and caused taste of oil to all 30 tons of fish.
17 The alternative water supply was in use for two months
18 The effects on the environment is not known
19 The total cost of the accident was estimated to be close to 10 mil. SKr (1,1 mil. EURO).

A.4. Road Transport of chemical oxidant and fuel / Accident in Köping Annotations[1]

System: Road Transport of Dangerous Goods (Sodium chlorate and fuel)

Event: Collision between two trucks, loss of containment, fire, deflagration, demolishing and fatal injury.

Time and place: 881205, E18, Municipal of Köping.

Numbers given in figures A.4.1.A and A.4.1.B correspond to the numbers and annotations below:

A.4.1 Preconditions

A.4.1.1 ROAD STANDARD AND CONDITIONS

1 Section of highway (E 18) between the cities of Västerås and Köping. Roadway without central refuge, covered with asphalt, total breadth including verges; 14 m. On the place of accident the road descended in the direction towards Köping.

Due to winter conditions and unsatisfactory road keeping the road was in a slippery state. (9, appendix 3)

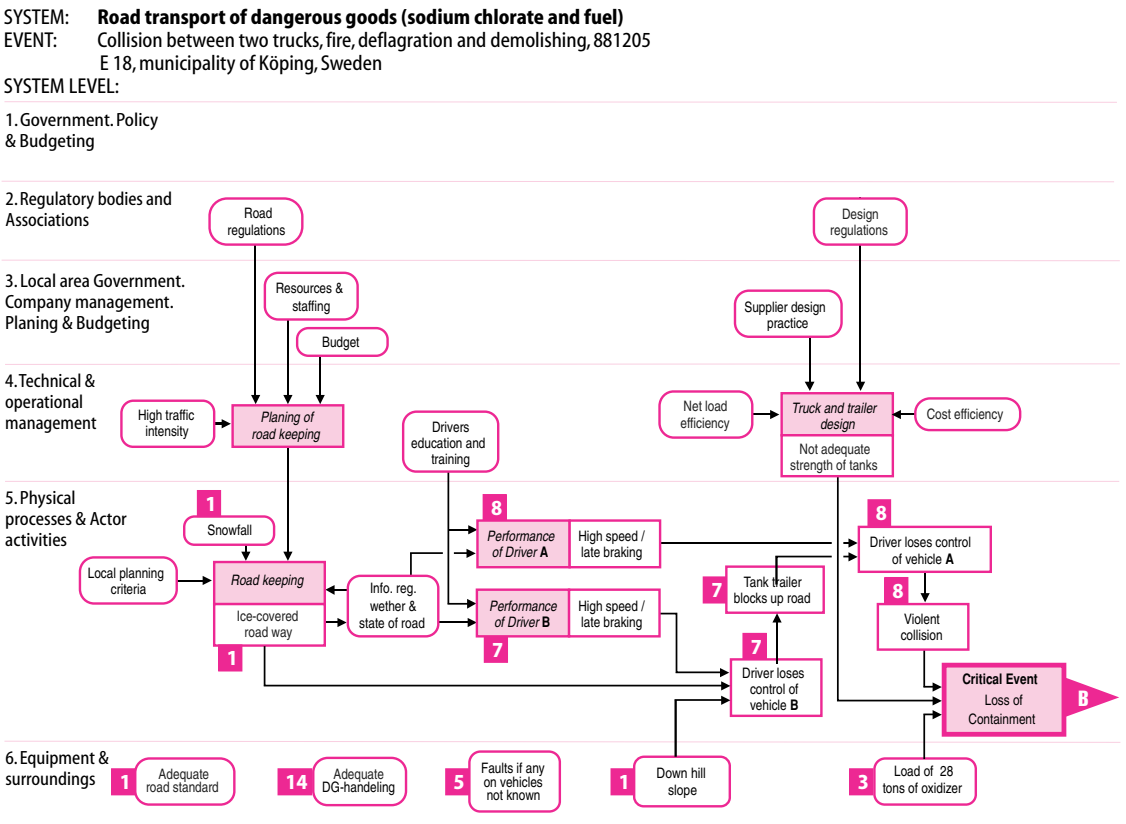


Figure A.4.1.A
The AcciMap describing conditions and development before the critical event. Numbers refers to annotation numbers below.

1. Where no other reference is given numbers within brackets in the annotation text refer to pages in the official report (Nr 2:1989) of the Swedish Commission, Kn 1981:2, of investigation of serious accidents, The Explosion Accident on E 18 within the Municipal of Köping, December 5 1988.

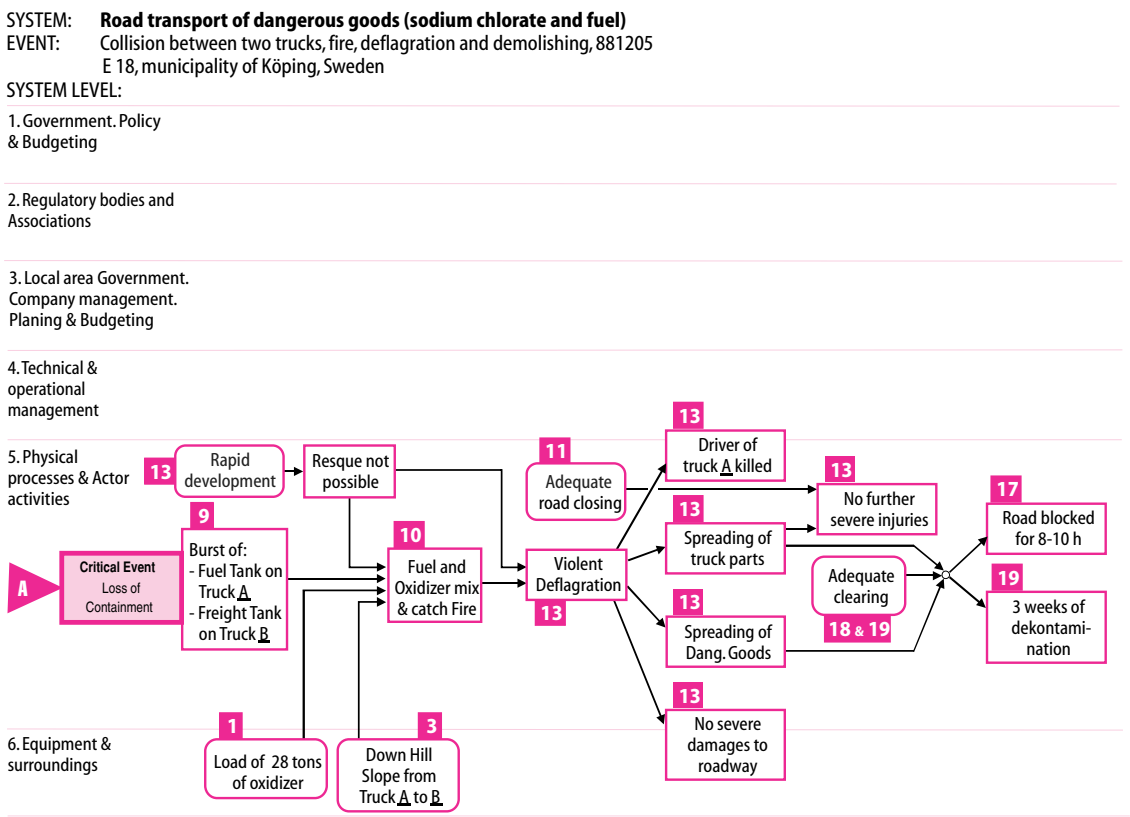


Figure A.4.1.B
The AcciMap describing conditions and development after the critical event. Numbers refers to annotation numbers below.

A.4.1.2 VEHICLES

2 Vehicle A, Heavy-duty freight truck with trailer. Cargo; on truck 19 pallets with general cargo (fruit, juice, purée, jam, marmalade, nuts), on trailer, in the front end, the same type of general cargo and 9 cartons with in total 1 600 explosive capsules, in the rear end a number of package baskets with general cargo. (9, appendix 1)

3 Vehicle B, Tank truck, Semitrailer with a tank for bulk gods containing 28 tons of sodium chlorate (a chemical oxidiser) (9)

4 Both vehicles were equipped with the necessary sign regarding dangerous gods. (9)

5 The status regarding technical standard and up keeping of the vehicles is not mentioned in the report (9)

A.4.2 The accident

6 It's about 23.00 hours (9)

7 The driver of vehicle B, the tank truck, when driving downhill in the direction towards Köping, realise that the vehicles ahead of him are breaking. In an attempt to stoop his

vehicle he looses control over it on the slippery roadway, slides and comes to a halt on the opposite side of the road with the truck in the ditch and the tank trailer right across the roadway. (9)

8 The driver of vehicle A, the freight truck, can not bring this to a safe stoop but runs into the tank trailer filled with sodium chlorate. The collision is violent. (10)

A.4.3 The critical event

9 Truck A creates a rupture in the tank on the trailer of truck B and sodium chlorate flows out on the roadway. Simultaneously also the fuel tanks or the fuel piping of truck A is damaged and in total 500 litres of diesel oil flows out on the roadway. The serious mechanical damages in the front of truck A indicates that also lubricating oil from engine and gear box together with antifreeze mixture flows out on the roadway. Since truck A stands in an up hill slope the sodium chlorate from truck B runs underneath truck A. (10)

A.4.4 Consequences

10 An accelerating fire starts under truck A. Mechanically or electrically formed sparks and hoot engine parts are possible igniting sources. Another is that the lead battery of truck A may have been damaged and sulphuric aside may have flown out and mixed with the fuel and the sodium chlorate forming a mixture that ignites spontaneously. (10, 15)

11 Police, present near the collision due to previous traffic disturbances, observes the fire call for rescue services (23,08 hours) and close the road to traffic. (11)

12 People witnessing the fire observe an intensive yellow light, a hissing sound and a dense white smoke. (10, 15)

13 After a few minutes the fire turns into a very violent explosion (deflagration) centred under the driver's cab of truck A.

The driver of truck A is killed. Were he was situated at the time of explosion is not known

Truck A is almost completely destroyed. Main parts of it are thrown up to 200 m away from the centre of explosion. The trailer of truck A had just minor damages.

The rear bogie of the tank trailer of truck B is thrown 100 m away. Of the 28 tons of sodium chlorate, originally in the tank, about 20 tons remains in it and about 5,5 tons is collected from the place of accident.

The explosion created no crater or other severe damages on the roadway. (10, 11)

A.4.5 Rescue activities / damage confinement

14 The first call about the accident reached the "SOS-centre" in Västerås at 23.08 from the police in Köping ho had personal in the vicinity of the accident due to earlier car rescuing. This call was about the early stage of the traffic accident and the fire.

At 23.09 the "SOS-centre" made "a large call" to the rescue services in Köping and to the rescue officer on duty that received it on his bleeper. (11)

15 When after about a minute there was an explosion the "SOS-centre" received several telephone calls about the accident. Therefore the operator at the centre did not notice until about 5 minutes later that the rescue services in Köping had not reported back to confirm the call. They were then called for again. (11)

16 A rescue forces from Köping arrived to the place of accident and started to fight the fire. The road was blocked by the tank trailer of truck B so, to be able to reach the fire from both sides, reinforcement was called fore from the rescue services in Västerås. (11)

17 The road (E 18) was blocked to the morning the following day. (11)

18 Clearing operations were performed during the night. The tank with the remaining sodium chlorate was transported to a dump tip for intermediate storage while awaiting final treatment. (11)

19 The day after the accident a firm was commissioned to decontaminate the place of accident and the surrounding piece of woodland.

The operation was extensive and took about 3 weeks. (12)

A.5. Capsizing and wrecking of RoRo Ship Vinca Gorthon, Annotations[1]

System: Ro/Ro Ship VINCA GORTHON
Event: Capsizing and wrecking in the North Sea,
Date: 880228

Numbers given in figures A.5.1. correspond to the numbers and annotations below:

A.5.1 Preconditions

A.5.1.1 THE SHIP

1 Lengths o.a.; 166 m, breadth; 22,6 m, depth to top deck; 18,45 m, draught; 7,00 m (summer), 6,85 m (winter), gross register tonnage; 18 773, main engine power; 4 900 kW (father), 3 300 kW (son), one propeller (C.P.P.); 145 rev./min., service speed; 16,5 knots.

Date of ordering; 851202, date of delivery; 870501. VINCA represented together with it's sister VIOLA the latest in a development process were a sea transport system

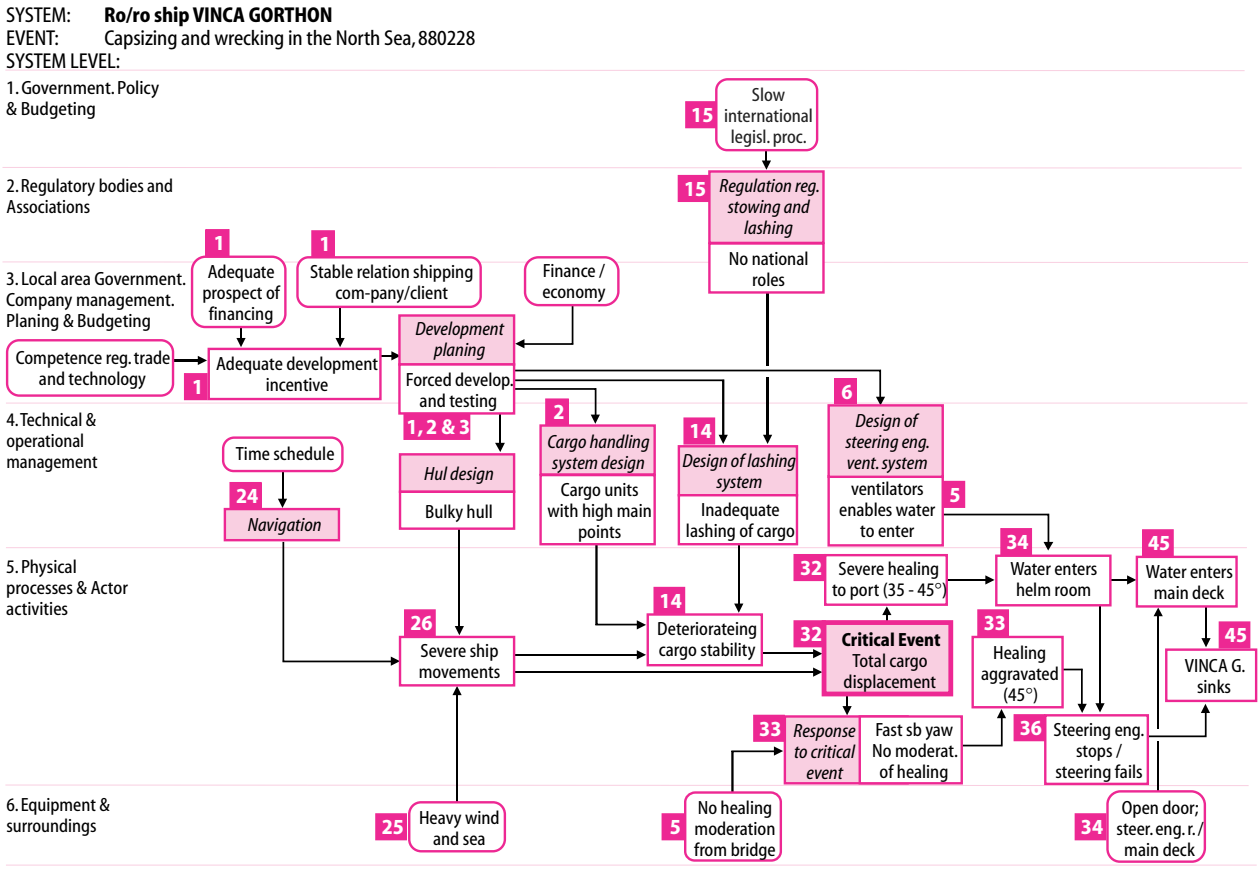


Figure A.5.1
The AcciMap describing conditions and development before and after the critical event. Numbers refers to annotation numbers below.

1. Where no other reference is given numbers within brackets in the annotation text refer to sections in the official report of The Swedish shipping commission of inquiry, dated 890607 regarding the capsizing and wrecking of the Ro/Ro ship VINCA GORTHON.

was tailored to the needs of forest industry MoDo, it's installations in Sweden and ports in Europe.

Ro/Ro handling and transports of paper, pulp and timber on roll trailers (40 feet, tare 5,7 ton, Safe Working Load 50 ton, designed to withstand 10 % overload). VINCA could carry 160 roll trailers distributed on 3 decks (tank top, main and upper deck). The top or weather deck could carry 100 private cars or 24 containers and tank-units (20 feet).

Priorities: Capacity, operability and reliability.

Goals: Efficiency.

Conflict: A rapid development and a significant technical step up resulted in; lack of time during construction and building and systems in operation not fully tested. (1.2.2)

2 During design the shipping company realised from a preliminary stability book that the shipyard had done a mistake. As a pre-requisite they had used to low a value for the height of the loaded roll trailer corresponding to a height of the centre of gravity of 1,95 m instead of the correct value 2,45 m.

During ship model testing the shipyard decided to alter the shape of the stern to reach a satisfactory ship stability (1.2.3)

3 During construction a decision was taken to increase the draft from 6,83 m to 7,0 m which brought about alterations in the hull. Also certain elements placed high up in the ship were removed or reduced in weight.

The ship had to carry ballast also with a full cargo.

Priorities: Safety.

Goals: Stability, cost effectiveness

Conflict: Increased costs of construction and operation. (1.2.3)

4 Results from the official stability test stated that the actual stability values were well within the frames of the calculated values. (1.2.3, 1.10.4)

5 The ship was equipped with:

- Computer aided cargo management system. From calculated cargo cases one could read; gross tonnage, draft, trim, heeling, bending moment and tensile forces, ballast, bunker, fresh water and supply.
  Conflict: The trim of the ship did not effect the calculation of its stability.
- System for roll moderation at sea: Heeling compensation during cargo handling in port and assistance during operation in ice. Three sets of pair of pressure/vacuum operated water tanks with electronic level measurement and regulation for dynamic stabilisation and compensation.
  Conflict: The system could only be operated from the cargo control room on the main deck, not from the bridge.
- Electric power generating system: Two auxiliary engines (870 kW), each operating one generator (1 050 kVA). One shaft generator (1 500 kVA), one emergency generator (250 kVA).
- Ballast system
  Conflict: The system could be operated from the cargo control room on the main deck and from the engine control room, not from the bridge. (1.2.5)
- Steering engine: Two electric powered hydraulic pumps placed in a separate room on main deck (stern on port side). The room was ventilated via two ventilators along the shipsides on the open part of the upper deck.
  Conflict: Due to cooling demands the ventilation could not be closed. With a heavy list and ruff sea the ventilators offered a way for water to enter the steering engine room and on to the cargo decks (if door not closed).

  The steering engine could be operated with one pump in operation. For rapid rudder movements both pumps were used.
- Steering propellers: Electric, one stem (736 kW) and one stern (368 kW). (2.5)

A.5.1.2 THE CREW

6 In total 16 regular members; Captain, 3 mates, chief engineer, 2 engineers, boatswain, 3 seaman, repairman, engine man, cock steward, 2 messmate. Extra on the last voyage one service engineer.

On duty on the bridge were normally one mate and one seaman. The engine room was periodically unattended. One engineer was on duty.

Numbers and combination etc. complied with the regulations. (1.3.1)

7 Al officers had the proper education and training in the type of ship in question. (1.3.2, 2.3.1)

8 Al officers except the second mate had former experience with VINCA. (1.3.3)

9 The captain, mates and the rest of the crew were educated in the functioning and operation of the computerised car-

go planing and handling system by the officer who had developed it and who served on board as a super cargo for the first 3 weeks VINCA was in operation. (1.3.4, 2.3.2)

A.5.1.3 CARGO HANDLING

10 The main type of cargo was paper rolls, pulp, board and wood. (1.4.1)

11 The cargo was handled on roll trailers and was loaded, lashed and secured to these trailers in storehouses in the loading ports (Husum and Oskarshamn) by staff from MoDo.

The cargo plan was based on information on every roll trailer, its number, weight, height and destination. Cargo planing in the storehouses must correspond with the cargo planing on board in order not to have to rearrange the roll trailers on board or in the unloading ports. The cargo plan was supposed to bee accessible to the ship officers 24 hours before loading started. (1.4.1)

Priorities: Effectiveness, reliability and punctuality.

Goals: Full cargo, easy to unload, extra heavy trailers placed on lower decks.

Conflict: Loading plans were made up late and altered during loading, which made the process difficult. (appendix 6)

12 Proper methods and routines when loading and lashing cargo on roll trailers were given in documented instructions that were used during training of MoDo personal.

To secure the cargo on the trailer 9 lashes (terylen belts, designed for 4 tons load) were used together with "corners" made of aluminium or plastic. (1.4.2)

Conflict: Some corners of aluminium had small damages and sharp edges. On the same roll trailer the height of the cargo piles could vary.

Tightening of the lashes was made with pneumatic tools. The roll trailers were than sent to one of three storehouses were kept in registered places. From the storehouses they were transferred to a special station on the quay were the lashes were tightened a second time by MoDo personal. (2.4)

13 From the quay the roll trailers were transported on board by stevedores in a listed order and placed in accordance with a cargo plan. In place the roll trailers were secured to the ships deck by 8 lashes (terylen ribbons) designed for 12 tons load. This operation was performed by stevedores and supervised by a mate. The lashing of the cargo to the roll trailers and the roll trailers to de ships decks was checked visually and by hand.

Conflict: Since every lash hold in the deck were used for 4 lashes these could not be conveniently re tightened due to lack of space. (1.4.2)

14 According to calculations the lashing arrangements used to secure the cargo (rolls to trailers and trailers to ship) had a very limited supporting effect even if they were properly applied and tightened. Thus the intrinsic stability of the cargo units towards tipping was increased by only 30 % i.e. from 15° to max 20°. (1.10.2, 2.4)

15 The International Maritime Organisation (IMO) 811119 adopted a resolution (A 489 XII) concerning safe stowing and lashing of cargo units in ships. It contains a recommendation that the governments in the assisting countries would adopt regulations regarding lashing instructions.

An IMO sub committee has 871026 presented a document (BC 29/4) with a stowing and lashing code. This was planned to be incorporated in the SOLAS-74 and then formulated and implemented as national rules in the assisting countries.

Conflict: In the Swedish regulations there were no general roles concerning stowing and lashing of roll trailers at the time of the capsizing and wrecking of VINCA. (1.4.6)

16 The superior mate was supervising the loading process from the cargo control room. He had special control of the heel reducing system. (1.4.2)

A.5.2 Loading in connection with VINCA's last voyage

17 VINCA arrived to the port of Husum 880221. The air temperature was –10 °C and fell to –20 °C during the time in port. Loading started in the afternoon 880221 and went on until the afternoon 880123. At the end of that period, when the last roll trailers were placed in position on the main deck, the ship suddenly heeled over.

The incident was, according to the superior mate, due to a fault signal from a frozen water level indicator in an empty tank in the heeling compensation system. The signal indicated full tank, which blocked the system, which in turn could not compensate for the lack of balance. (1.4.3, 2.2.3)

18 The lack of balance was instead compensated for with the ballast system and the heating was increased in the frozen

tank, the effect of which was registered manually. The signal than turned OK and the heeling compensating system became operative. This happened short after departure. (1.4.3)

19 The cargo from Husum consisted of 175 roll trailers (21 were 20 feet and 152 were 40 feet). Further more there were 7 containers (20 feet), 5 MoDo tank units and a private car on top deck. (1.4.3)

20 After loading and unloading in Oskarshamn the cargo consisted of 170 roll trailers (21 were 20 feet and 149 were 40 feet) and on top deck, the same cargo as indicated above.

Most roll trailers were new with steel frames and load surfaces made of plywood board. The cargo consisted mainly of paper rolls of varying height and diameters. The distances between the rows of roll trailers were 40–45 cm. (1.4.3)

Based on the cargo plan and information from MoDo the following conditions have been calculated; Total DW 9 890 ton (cargo 8 493 ton), deplacement 17 224 ton, draft 6,47 m. (1.4.4)

The centre of gravity of the cargo was 0,169 m to port. (1.10.1)

A.5.3 The day of the event

21 VINCA enters the North Sea at 01.15 (Elbe 1), 880228, after passage of the Kiel channel, heading for Antwerpen. (1.6)

22 Number two engine (the son) and one of the two hydraulic pumps of the steering engine were running, The weather was getting worse and VINCA was leaning 3° to port due to strong wind pressure. (1.6)

23 The anti rolling system was not sat in operation.
The effectiveness of the system was questioned under the conditions with ruff sea and irregular waves. (1.6)

24 At ca 13.00 the course was set at 245°. (1.6)

25 Wind (16–24 m/s) and waves (sign. wave height 4–5 m, max. 6–7 m) abeam to starboard or somewhat fore. Temperature, air ca 0 °C, sea +5 °C. (1.5, 2.1, 2.1)

26 The ship was rolling from starboard 4° to port 10°. (1.6)

27 Calculations indicate that during the last 5 hours before the event the accelerations due to ship motions reached levels that caused the stability point of the cargo and roll trailers to be exceeded and the cargo to slide.

Conflict: The stability was undermined. (1.10.2, 2.4)

28 No abnormalities concerning ship movement or otherwise were registered. (2.1)

A.5.4 The event

29 At ca 15.35 Superior mate and mate on duty (on the bridge) and boatswain (in his cabin) heard a thud. This is believed to be due to a roll trailer tipping over towards a bulkhead. Due to dynamic forces this was so hard that the lashing did not coop. (1.6, 2.1)

30 Boatswain checked the cargo on the upper deck. (1.6)

A.5.4.1 CRITICAL EVENT

31 One trailer (A580) was rocking in its lashings, leaning ca 20° to port and hitting against a bulkhead. Suddenly the boatswain sees how rolls start to fall down from one trailer. VINCA starts to heel over to port and "every thing starts to tip at the same time" (1.6)

32 According to the mate on duty VINCA heels over 20 to 25° to port, heals back to 5 to 10° to port and than slowly over again towards an angle between 35 and 45°. This was due to an almost total displacement of the cargo. (1.6, 2.1)

33 The superior mate gives full starboard rudder and starts hydraulic pump number two of the steering engine.

VINCA yaws to starboard, the shortest way towards the wind and waves.

Priorities: Safety.

Goals: To decrease healing and rolling.

Conflict: The manoeuvre increased the healing to 45° due to dynamic forces. (1.6)

34 Sea water enters the decks via the ventilators to the steering engine room *due to an open door* between this room and the main deck. (2.1)

35 At 15.50 the mate on duty transmits "May Day".
Several ships including the oil tanker m/s STRIDE receive the call.

36 Shortly after the yaw has been started one of the hydraulic pumps of the steering engine stops and after another 40 minutes the second pump stops, the rudder gets stuck in the starboard position. VINCA now has the stem against the wind. (1.6)

37 The crew is gathered on the bridge provided with lifebelts. In the preparation to abandon the ship the launching of the lifeboats are not considered possible. Instead an attempt to launch two life rafts from starboard side of A-

deck is performed. This mission fails. (1.7.2)

38 At 16.37 helicopter transport is asked for to rescue two injured crewmembers. (1.6)

39 Preparations to abandon the ship

The main engines are stopped

Priorities: Safety of personal

Goals: Reduce the risks caused by the propeller

Conflict: (The manoeuvrability was already very much reduced) (1.6, 1.7.2)

40 VINCA raked to starboard got the wind and waves abeam to port and the healing increased to 50–55°. (1.6)

41 Wind and waves abeam to port, healing 50–55°.

The use of the ballast water system (BWS) was considered.

The manoeuvring of the BWS could only bee done from the main deck.

Priorities: Safety of personal.

Goals: Reduce the healing.

Conflict: Risks in connection with reaching and staying on main deck. (1.6)

A.5.4.2 RESCUE

42 Between 18.00 and 18.45 VINCA was abandoned The crew was transferred by helicopters to STRIDE. (1.6, 1.7.2)

43 The ship was drifting in the dark before strong wind and heavy sea, listing severely to port, slowly sinking and unlit.

Conflict: In the area are oil and gas fields with manned platforms. (1.6)

44 The Dutch Coastguard followed VINCA on radar and by observations from the rescue ship SMIT LLOYD. They were prepared to have the ship sunk by the Dutch Naval Forces. (1.6)

45 At 06.12, 880229 SMIT LLOYD reports that VINCA has a list of 90° and starts to sink slowly. At 07.30 VINCA disappears. (1.6)

46 Divers established, short after the shipwreck, that VINCA lied broken on the bottom with a list of 130°. (1.9)

A.6. Grounding of Gas Tanker Balina in Lake Mälaren, Annotations[1]

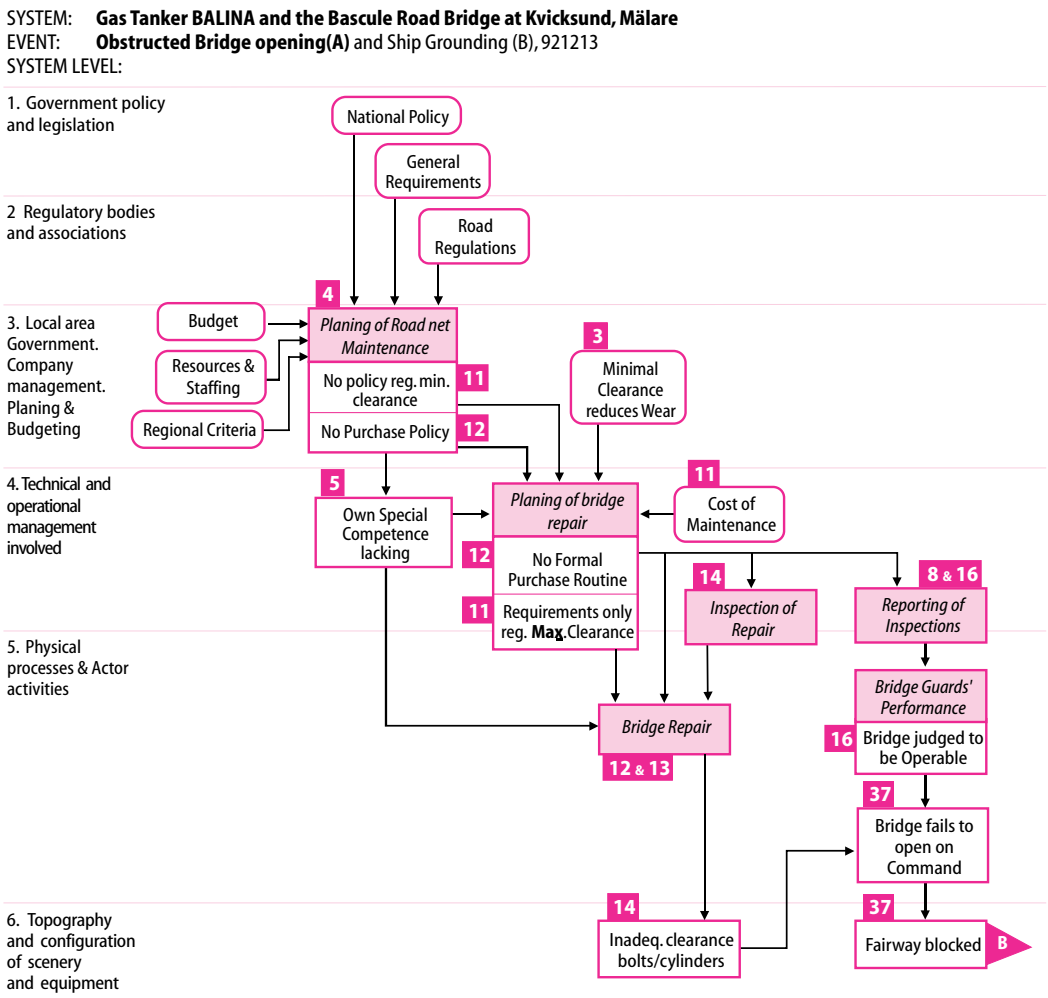


Figure A.6.1.A
An AcciMap describing conditions and development leading to the obstruction of the bascule bridge and a blocking of the fairway at Kvicksund. Numbers refers to notation numbers below.

1. Where no other reference is given numbers within brackets in the annotation text refer to pages in the repport; Passage of the Kvicksunds bridge in Mälaren, Incident – BALINA (LALZ4), 1992-12-13, Swedish National Maritime Administration, Bengt Erik Stenmark, report, November 1993.

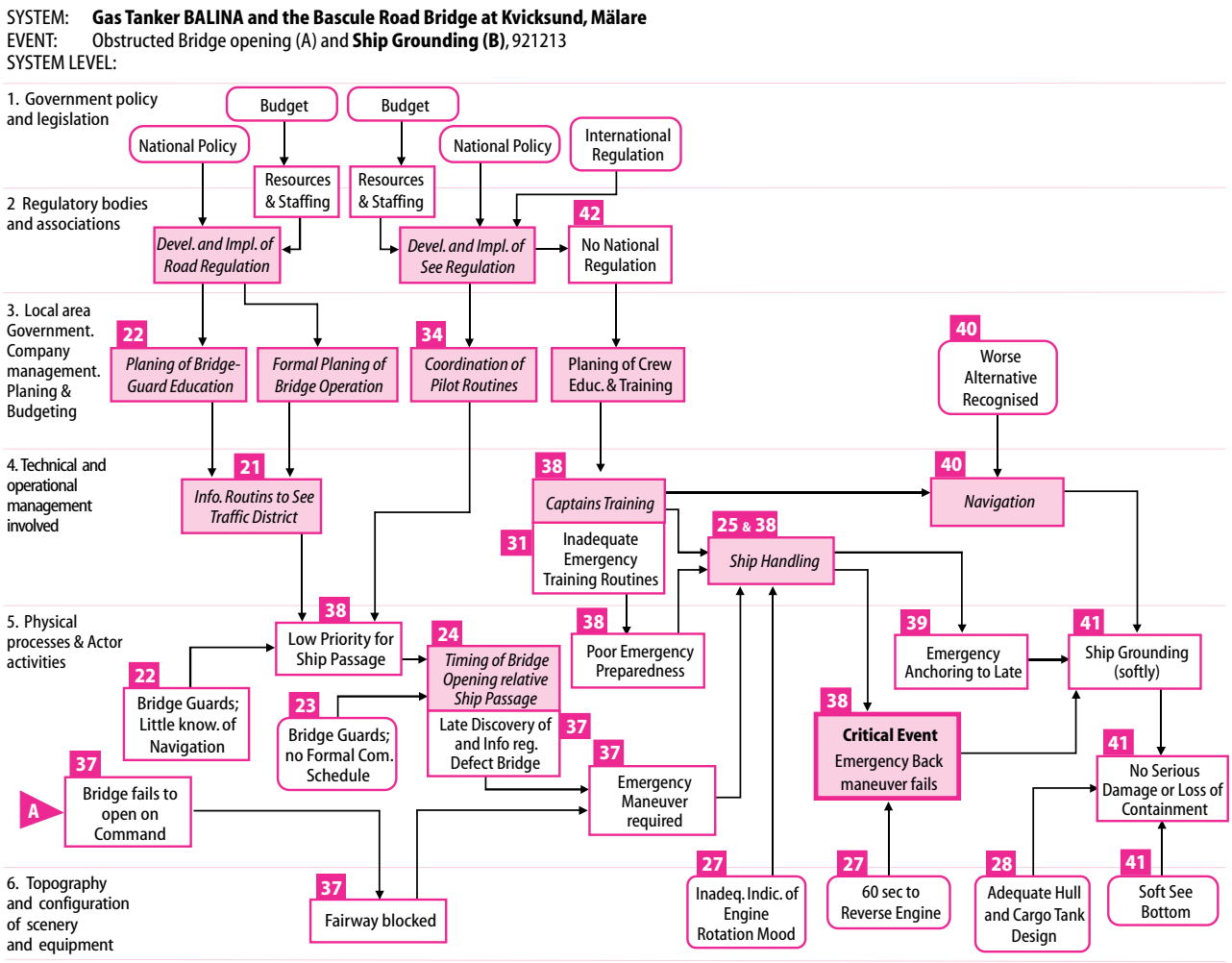


Figure A.6.1.B
An AcciMap describing conditions and developments effecting the event after that the bascule bridge failed in a closed position when ordered to open and further to the phase when the gas tanker was forced to ground aside the fare way. Numbers refers to notation numbers below.

System: A bascule rood bridge crossing a fairway and a passing tanker carrying condensed ammonia.

Event: Obstructed bridge opening forces the ship to make an emergency maneuver that results in a "gentle" grounding

Time: 921213.

A.6.1 Summary

1 921213, at approx. 07.00 hours, a gas tanker, BALINA, with a full cargo of liquefied ammonia should pass the "Kvicksund bridge in lake Mälaren. A technical defect in the bascule-bridge caused the bridge not to open as expected. At the time when this was realised the ship was in a position were a back manoeuvre was necessary to bring the ship to a standstill in order to avoid a collision with the closed

bridge. Due to another defect, this time aboard the ship, the back manoeuvre did not come of. The ship was still outside the ship conveying rails along the fairway under the bridge. It could therefore be steered aside of these rails and put aground on the side of the fairway. The grounding, which took place at low speed and against relatively soft sea bottom, stroke the bottom of the hull in the fore end. The hull had double bottoms. If it had been damaged a release of bunker oil could have occurred, There was no risk of an ammonia release in connection with the grounding as it took place. (1)

A.6.2 Preconditions

A.6.2.1 THE BRIDGE /PHYSICAL AND ORGANISATIONAL SYSTEM

2 The bridge is a part of road 53 connecting the northern and the southern sides of lake Mälaren. The road traffic is rather intensive. It's a bascule bridge that can be opened to allow for ships to pass to and from the inner, western part of the lake and the municipal of Köping. The bridge is built together with a parallel bascule railroad bridge in 1975.

On opening the bridge the two flaps are risen to a vertical position. This is achieved by electric machinery operated by a bridge guardian from a manoeuvre tower directly connected to the bridge. In the lowered position the bridge is blocked and fixed by bolts that are inserted from one of the flaps into cylinders in the other. When the bridge is about to be opened the bolts are moved out of the cylinders by electric machinery.

The bolts had been under maintenance repair 2 weeks before the event when they got stuck in the cylinders. This was the immediate cause for that the bridge could not be opened. (5)

3 *Conflict:* It is essential to keep the clearance between the bolts and the cylinders at a minimum in order to reduce dynamic forces and wear in the bridge due to mechanical vibrations induced by passing vehicles. A reduced clearance however also increases the risk of the bolts getting stuck in the cylinders.

4 The bridge comes under the Road Administration, Region Mälardalen in Eskilstuna and the main responsibility lies with the road director of the region. (5)

5 Under the road director there is a department for purchasing of operation and maintenance. The bridge at Kvicksund comes under this department together with 10 other bascule bridges in the region.

The department takes care of purchasing, deliveries control and permit matters.

The production division in Borlänge inspects the bascule bridges. This is done in a regular manor.

Conflict: There is no competence regarding hydraulics, mechanics or electricity within the Region Mälardalen. Such competency is exceptionally purchased from Region Stockholm. (5)

6 For practical reasons the Rail Administration is operating both the bridges. The main responsibility for the operation lies with the Rail Administration, Region East. (5)

7 Under the Rail Administration, Region East the management of the Västerås district is responsible for the operation of the bridge activity at Kvicksund.

The Rail Administration is thus responsible for the operation of both the bridges while the responsibility for the maintenance is shared between the Rail Administration (the rail bridge) and the Road Administration (the road bridge)

Via inspection protocols the Rail Administration is informed of results from inspections of the road bridge, performed by the Road Administration. (5)

8 Reparation performed by an outside workshop is followed by a not formalised reporting procedure.

Conflict: There is normally no inspection after such reparation and there is no formal routine stating that such an inspection should take place. (6)

9 There was a period of 2 weeks between the reparation performed and the time wen the defect appeared. (6)

A.6.2.2 THE BRIDGE / THE REPAIR WORK BEFORE THE INCIDENT

10 During the annual inspection of the bridge in 1991 it was established that the clearance was to large between the bolts and the cylinders used to fix the bridge in the closed position.

There was a claim for appropriate measures from the inspector of The Road Administration, Production division, Borlänge. (6)

11 *Conflict:* No explicit rule or policy is followed when appropriate clearance between bolts an cylinders is appointed and no such rules based on technical analysis are used. In

stead "old drawings" are followed together with experiences from the bascule bridges in use.

To keep at a minimum the costs of maintenance due to wear of the bridge.

A maximum value of the clearance between the bolts and the cylinders are given.

Conflict: Tight clearances minimise the dynamic forces and wear in the bridge. What might bee a proper minimum clearance value, regarding the risk of the bolts getting stuck in the cylinders, has not been analysed to any depth. (7, 8)

12 The Road Administration, Division Mälardalen gave Motala Works the commission to make proper repairs. This was done in verbal form during a visit, at the Road Administration in Eskilstuna.

Conflict: There was no written contract, no formal ordering procedure and no technical specification.

During the visit a proposal for a minor construction alteration prepared by the inspector from the Road Administration in Borlänge and the Motala Works is presented. This proposal, which was accepted by the Road Administration in Eskilstuna, implied a longitudinal enlargement of bolts and cylinders by 100 mm.

Conflict: The fact that the surface of contact between the bolts and the cylinders had been enlarged did not cause any alarm and no second opinion was asked for.

During the visit the inspector from the Road Administration in Borlänge was offered and assumed the task of inspection in connection with the reparation.

The Motala Works was engaged because the number of experts in bascule bridges is diminishing and the company is since long familiar with the bascule bridges of the Road Administration.

It was also the apprehension of the Road Administration that the Motala Works was classified according to ISO 9000 and therefore their competence was not questioned. At the time The Motala Works was under examination in this respect but some deficiencies in the quality system had been pointed out. (6, 8, 9)

13 Proposals for improvements regarding the technical capacity of the bridges are often presented by personal from Motala Works and the expertise from the Road Administration in Borlänge. When a competitor to Motala Works has been used the results haw not been satisfactory and hidden faults haw turned up after delivery.

Normally contracts are drawn up with both entrepreneurs and control functions but no real ordering procedure is in use. The Motala Works and The Road Administration in Borlänge have monopoly when it comes to bascule bridges since competency is rare in these maters.

Conflict: This phenomenon is not uncommon. (6, 9)

14 The inspector of the Road Administration 921123 in connection with the delivery inspection checked the bolts and the corresponding cylinders. Notes and spot checks showed that the bolts during the hardening had been somewhat crooked. Measures were taken after which the equipment passed through.

There was no notification of any deviations from approved clearances as a result of this control. The tolerance standard (max. 0,176 mm) marked on the drawing was meet (0,14 mm). A trial run of the bolt that later got stuck was performed 921126. There was no documentation regarding any trial run of the other bolt.

Conflict: After the event with BALINA the clearance between the bolts and cylinders was measured (921215) and found to bee smaller (0,08 mm) than the privies found (0,14 mm). The explanation was that "something must have happened during mounting of the cylinder" and that "the bridge was known to bee crooked". The inspector from the Road Administration in Borlänge, performing the inspection after the event, states in his report that the clearance shall be 1/1000 of the bolt diameter, which corresponds to aprox. 0,3 mm.

It had not been mentioned or documented earlier that the bridge was crooked. Neither, as it seems, has there been any measurements performed before or after the event to test that the bolts and the cylinders were in line. (6, 8, 9)

15 Relatively soon after the repair works electric currents higher than normal were indicated by the instruments on the manoeuvring panel when the bolts were operated. (6)

16 These abnormalities were not documented but only orally reported to the superiors. (7)

17 The Motala Works was contacted by phone by the Road Administration in Eskilstuna (Region Mälardalen) to get the problems solved. A representative of Motala Works performed not documented inspections but no careful analysis of the observations was performed and no sug-

gestions were given. Different types of grease for lubrication of bolts and cylinders were tested during this period. How this was done and the results of it are not documented.

Conflict: There are no routines for reporting divergence's and The Road Administration in Borlänge, who was appointed as inspectors, was not informed. (7)

18 After the incident with BALINA the chef inspector of the Road Administration gave order of increased clearance between the bolts and the cylinders. (7)

19 After this adjustment the troubles with bolts and cylinders stopped. (7)

A.6.2.3 THE BRIDGE / OPERATION

20 Well worked through accident plans are accessible to the bridge guardian and to persons at the central management level.

Conflict: The up keeping of these plans are done by unconfirmed corrections introduced by hand. (7)

21 In connection with bridge maintenance sea pilots only receive informal information from the Road Administration. Staff involved would like to see a formalised type of information six weeks before.

The staff involved would also like to see a yearly information event were for example accidents and near accidents could bee penetrated and personal network could bee established. (7)

22 The bridge is operated by a bridge guardian on duty.

The guardians have been recruited from railway personal in technical service and with a background that gives proper knowledge in the technical and operational conditions regarding the bridge. Knowledge regarding road and railroad traffic is also satisfactory.

Conflict: The bridge guardians had not been given any formal education in navigational matters in connection with bridge passage. (10)

23 The bridge guardians have no formalised routine for reporting any deviations in the conditions regarding bridge opening and either is there any information about the conditions when such reporting would bee justified.

There is no precise schedule for radio communication between the bridge guard and the captain or the pilot onboard ships. (10)

A.6.2.4 SHIPS PASSAGE OF THE BRIDGE / NORMAL PROCEDURE

24 According to chart 1131 the ship by means of a sound signal requests passage of the bridge at Kvicksund. After that the ship has to follow a number of marked light signals.

In practice the bridge guard was contacted via radio in good time before passage to request opening of the bridge. After that one "talks ones way" to the bridge.

The rail traffic has priority over the ships traffic, which in turn has priority over road traffic. In practice however the bridge is kept down for as long as possible as a service to the road traffic.

Conflict: The actual priorities, which are accepted by the pilots, have lad to late bridge openings from the ships manoeuvring point of view.

In reality the signal picture according to the chart is therefore of no importance. (9, 10, 15)

25 As a routine the opening of the bridge had to bee started before the ship begun *the final approach* of the bridge.

The event demonstrates that this routine gave only small, and as it came out, insufficient margins for corrective measures if not the bridge could bee opened. (10)

A.6.2.5 THE SHIP / MT BALINA

26 Manager; Norsk Hydro. Flag; Norwegian (NIS). Build; 1975, Pappenburg, Germany. Class; Germanischer Lloyd, +100 A4 E2 +MCE2 16/24 Liq gas tanker. Gross tonnage; 4286,56. DW; max 6187 ton. Lpp; 98,60 m. Bmld; 15,50 m. Draft; max. 7,56 m, with full cargo of ammonia 6,60 m. (Appendix 2, p2)

27 Main engine; Deutz RBV 12m 540 (reversible), max. Power 4000 kW.

Engine manoeuvring from bridge or engine room. The lever on the bridge is a combined regulator with functions for start, stop and speed (rev.) forward and backward.

Conflict: It takes 60 sec to reverse engine from full ahead to full back. There is no indication on the bridge of the status regarding engine operation during such manoeuvres. (Appendix 2, p3)

28 Hull with double bottom and with 3 cargo tanks for liquefied ammonia, cylindrical in shape and separated from the hull structure. Distance from tanks to hull is minimum 0,8 m. Bunker oil and ballast in tanks between hull bottoms

Ammonia is shipped in liquid form at –33 °C and atmospheric pressure. (Appendix 2, p3)

29 Manning; 19 in total, of them 4 Norwegians (captain, superior mate, chief engineer and first engineer) and 15 from the Philippines. All personnel are trained in the operation of gas tankers

The captain had been in gas tankers for many years.

Conflict: It was the captain's second voyage to Köping in BALINA, the first as captain.

At the time of the event the chief engineer, the third engineer and one engine man attended the engine room. (Appendix 2, p2–4)

30 The shipping company has a well documented and implemented Safe Management System in accordance with relevant principals. This system is well described in manuals and other documents. The company has long experience in gas tankers. (10)

31 *Conflict:* The short comings in connection with the passage of the bridge are due to organisational conditions, that is little practise with the emergency stop manoeuvre and the lack of knowledge and practise of and routines for rush anchoring. (11)

A.6.2.6 THE SEA TRAFFIC DISTRICT /PILOTS

32 Mälarens sea traffic district is under a district manager with two "stand by pilots" next in order. The district has approx. 100 employees. Of them 42 are pilots. (11)

33 The sea traffic district operates a traffic information system, which is based on ships self-reporting to a Traffic Information Central in the region (Södertälje) when at certain reporting points. The task of the central is to receive, compile and send information forward about ship movements and other conditions in the fairways of significance to the safety. (11)

34 The sea traffic district have not worked out a manual over its routines. (12)

35 The pilots have extensive freedom to draw up there own work. (12)

A.6.3 The Event

36 The manoeuvring was performed by the captain (lever) and the pilot (helm and radio)

The pilot reported to the Traffic Information Central when passing the reporting points and to the bridge guardian at the Kvicksund bridge in accordance with normal routines. When the speed had been reduced to half (10 knots) and the bridge could bee seen, this was still closed and the bridge guardian reported that it could not be opened. (16, Appendix 2, p7)

37 The bridge guardian is informed of the passage of BALINA. The rail-bridge is opened.

During the attempt to open the road bridge the bolts are found to bee stacked in the cylinders and the situation is reported to the pilot onboard BALINA. This is done in such a late stage that an emergency manoeuvre is required to avoid a collision. (Appendix 2, p5)

38 The captain was relatively new on board and he was not prepared for emergency manoeuvre of the machinery. No preparations were done for emergency anchoring

Wen performing emergency manoeuvre of the machinery the lever was operated to rapidly and the backward restart did not occur until it was carried out locally by staff in the engine room.

The captain then ordered the third mate and the watchman to hurry to the prow and droop the anchors. (16, Appendix 2, p7)

39 The starboard anchor was dropped but at such a late states that it probably had no effect. (Appendix 2, p5)

40 When the ship came closer to the bridge the pilot and the captain agreed to yaw south and ground the ship. (Appendix 2, p5)

41 The ship grounded at a speed of about 3 knots on relatively soft see bottom. No serious damage occurred. Cargo, bunker oil and ballast water were contained and the ship could be towed off and escorted to it's original destination (Köping). (Appendix 2, p7)

A.6.5 Regulations / National Maritime Administration

42 At the time of the incident there were no national regulations concerning:

- "Safe Management and Control (inspection) on Shipping Companies" and
- "Special Manoeuvring Controls on Ships Operating in Mälaren".

Proposals for such regulations were referred in the following year. (14)

Appendix B: Structure of Accident Data Collection

The types of data presented here are suggested to be collected, retrieved, and analysed in connection with investigations of accident that have occurred during road transport of dangerous goods. The complexity of the database has turned out to invite a structuring of the tool into several phases and levels of detail matching the requirements of different users. The process proposed for reporting and analysis is therefore divided in the following four steps that may be performed by different persons:

A. "*On the scene*" *data collection and analysis:*
   - A.1 *Direct observations.* This level includes observation of the circumstances of the specific accident, the critical event the preceding causal flow of events, the immediate consequences, thereafter and the rescue actions taken. This phase includes information from interviews on location.
   - A.2 *Judgements.* A more penetrating phase considers the pre-conditions judged to have shaped the course of development events, such as decisions and activities of work planners and equipment designers. This phase may involve other specialists in interviews of planners.

B '*Follow-up*' *data collection and analysis:*
   - B.1 *Observations;* Supplementary basic information, circumstances, developments and rescue actions as under point A.1 and information on activities such as rest value securing, decontamination of land and property and estimates of long term effects and costs.
   - B.2 *Information retrieval and analysis;* An audit of the organisations and agencies shaping the pre-conditions that are judged in the previous steps as relevant for the occurrence and development of the event.

The tool to support the collection and analysis process should be structured in such a way that when transport mode, i.e. Road transport, and accident context, i.e. loading/unloading, has been indicated, all requests for data concerning other modes and contexts should not appear in the "forms" that follows.

Data supposed to be collected in early steps of the process is in the "forms" of the later steps indicated in *italic* to mark that they, if previously introduced, should be filled in automatically.

A On the scene collection

A.1 Observations

1. Transport Mode		Mark
1.1 Road		
1.2 Rail		(not developed)
1.3 Sea		(not developed)
1.4 Air		(not developed)

2. Context of Accident		Mark
2.1 Transfer en Route	(link)	
2.2 Temporary stop	(link)	(not developed)
2.3 Loading / Unloading	(node)	
2.4 Temporary storing	(node)	(not developed)

2.5 Short "cover story" of the event in "free-text".

BASIC INFORMATION

3. Firm of Haulage	Indicate
3.1 Name	
3.5 Phone number	
3.7 Contact person	

4. Driver of Dangerous Goods Vehicle

4.5 Hours of driving before Accident

4.6 Condition

5. Transport Documents		
5.1 Dangerous Goods Declaration	Yes/No	
5.2 Transport Card	Yes/No	
5.3 Certificate of DG-vehicle valid:	Yes/No	
5.4 Cleanness certificate:	Yes/No	

6. Signs & Labels		
6.1 DG-Signs on Vehicle:	Yes/No	Correct: Yes/No
6.2 DG-Signs on Tanks/Containers:	Yes/No	Correct: Yes/No
6.3 DG-Labels on Packages:	Yes/No	Correct: Yes/No

7. DG-Vehicle

7.1 Type

Truck	Weight of vehicle
Trailer	Weight of vehicle
Lorry	Weight of vehicle

8. Transport type

8.1 Tank (tank or tank container with volume > 1 m^3.	Yes/No
8.2 Tank container	Yes/No
8.3 Bulk (solid not packed material)	Yes/No
8.4 Paced Goods	Yes/No

TIME, PLACE AND CONTEXT OF ACCIDENT

9. Time of Accident **Indicate**

9.1 Year Month Day

9.2 Time of day

10. Place of Accident **Indicate**

10.1 On Road or Temporary stop

10.1.3 Street, Street number

10.1.4 Road number

10.1.5 Sector; (between place 1 and place 2)

10.2 Loading / Unloading / Temporary Storing (node)

10.2.1 County

10.2.2 District

10.2.3 Enterprise where the Accident occurred

Name

Visiting address

Phone number

Fax number

Contact person

11. Context of Accident

11.0 Where the conditions to be considered as normal	Yes/No
If No describe in what respect	(free text)
11.1 On Road	Indicate

11.1.1 Type of Accident

Single

Meting

Catching up

Overtaking

Wild animals

Turn off to the left to the right

Turn into…

Crossing traffic

11.1.2 Involved in Accident

Wild animal

Private car

Other Truck / Lorry

Powered equipment

Unprotected road user or pedestrian

11.1.3 Surroundings

11.1.3.1 Countryside (Agricultural land, Forest land, Wet land, Groundwater reservoir)

11.1.3.2 Densely built-up area (Communication junction, Industrial area, Stores area, School, Day-care centre, Hospitals, Home for aged people, Residence area)

11.1.4 External conditions

11.1.4.1 Weather conditions:

Clear, fog, mist		
Rainfall;	Yes/No	Heavy; Yes/No
Snowfall;	Yes/No	Heavy; Yes/No
Wind;	Strong	Yes/No
Temperature		

11.1.4.2 State of road (Dray / Wet /Slippery / Cleared from snow)

11.1.4.3 Visibility (Open / Reduced)

11.1.4.4 Lightening: Existing; Yes/No, Turned on; Yes/No, Satisfactory; Yes/No

11.1.4.5 Road standard;

Type, width, slope, pavement, condition

Security arrangement; ditches, embankments, separations

11.1.4.6 Temporary obstacles; road-works, blocking up vehicles, wild animals, object; tree, branches, boulders, landslide

11.1.4.7 Hazardous objects; railings, posts poles, boulders, rock-side

11.1.5 Traffic conditions

10.1.5.1 Traffic intensity (Low, high, traffic jam)

10.1.5.2 Speed limit (30 / 50 / 70 / 90 / 110 km/h)

11.1.5.3 Normal traffic intensity (according to last measuring)

11.2 Temporary stop (not developed)

11.3 Loading / Unloading Indicate

11.3.1 Conditions:

Clear, fog, mist		
Rainfall;	Yes/No	Heavy; Yes/No
Snowfall;	Yes/No	Heavy; Yes/No
Wind;	Strong	Yes/No
Temperature		

11.3.2 Premises

Lightening: Existing; Yes/No, Turned on; Yes/No, Satisfactory; Yes/No

Signs, Traffic guidance display, separation: Existing; Yes/No, Satisfactory; Yes/No

Safety separation distances between place for goods handling and;

Warehouse, tanks: Satisfactory; Yes/No

Source of ignition: Satisfactory; Yes/No

Embankment: Satisfactory; Yes/No

Protective railing: Satisfactory; Yes/No

11.3.3 Equipment for goods handling

11.3.3.1 Bulk goods

Conveyer, crane, and excavator: Satisfactory; Yes/No

Pipes, hose, coupling, valve, pump: Satisfactory; Yes/No

Regulator: Satisfactory; Yes/No

Controls: Satisfactory; Yes/No

11.3.3.2 Packed goods
Conveyer, crane: Satisfactory; Yes/No
Fork truck: Satisfactory; Yes/No
Goods securing equipment
Pallets, collars: Satisfactory; Yes/No
Baskets: Satisfactory; Yes/No
Straps, belts: Satisfactory; Yes/No
11.3.4 Supply systems
Electricity
Steam
Compressed air

11.4 Temporary Storing (not developed)

12. Critical Event **Mark** **Direct consequence** **Mark**

12.1 Loss of containment of dangerous goods
12.1.1 Uncontrolled energy release
12.1.2 Fire / Explosion

12.2 Uncontrolled energy release
12.2.1 Loss of containment of dangerous goods
12.2.2 Fire / Explosion

12.3 Fire / Explosion
12.3.1 Loss of containment of dangerous goods
12.3.2 Uncontrolled energy release

13. Direct Cause **Mark if adequate**

13.1 External damage, wear on;
13.1.1 Tank
13.1.2 Equipment
13.1.3 Container
13.1.4 Package
13.2 Internal damage / wear, corrosion on;
13.2.1 Tank
13.2.2 Equipment
13.2.3 Container
13.2.4 Package
13.3 Over filling
13.4 Unintentional mixing of goods
13.5 Faulty heating of goods
13.5.1 external heating
13.5.2 Faulty equipment
13.5.3 Faulty handling
13.6 Sabotage
13.7 Extra ordinary conditions (Free text)

14. Conducive factors **Mark if adequate**

14.1 Transfer en Route
14.1.1 External force on; tank, armature, container,
14.1.1.1 Impact on stationary surrounding object
Road standard and state
DG-drivers driving and control of DG vehicle

14.1.1.2 Collision with other vehicle
DG-drivers driving and control of DG vehicle
Other drivers driving and control of vehicle
14.1.1.3 Goods containers and/or Packages in motion
14.1.1.4 Wrong handling of equipment
14.1.1.5 Sabotage
14.1.2 Internal damage to; Cargo tanks, Container, Equipment
14.1.2.1 High- or under-pressure
14.1.2.2 Corrosion; Control, Maintenance
14.1.2.3 Wear; Control, Maintenance
14.1.3 Over-filling/ Tight-filling
14.1.4 Unplanned mixing of goods
14.1.5 Faulty heating of goods

14.2 Temporary stop (not developed)

14.3 Loading / Unloading

14.3.0 Discharge during manual handling of equipment
14.3.1 External force on; tank, armature, container, package
Run into by vehicle
Handling of; tank, armature, container, package
Pressure / missiles; from explosion in surroundings
14.3.2 Internal damage to: Tank, Cargo tanks, Container, Equipment
14.3.2.1 High- or under-pressure
14.3.2.2 Corrosion
14.3.2.3 Wear
14.3.3 Over-filling
14.3.4 Unintentional mixing of goods
14.3.5 Erroneous heating of goods
Extreme Weather conditions
Fire in surroundings

14.4 Temporary storing (not developed)

15. Protective systems functioning

15.1 Transfer en Route

15.1.1 What precautionary measures had been taken on the place of accident to:
– Reduce probability of accident; (free text)
Observed effect (free text)
– Reduce effect s of accident; (free text)
Observed effect (free text)

15.2 Temporary stop (not developed)

15.3 Loading / Unloading

15.3.1 What precautionary measures had been taken on the place of accident to:
– Reduce probability of accident; (free text)
Observed effect (free text)
– Reduce effect s of accident; (free text)
Observed effect (free text)

15.4 Temporary storing (not developed)

16. Rescue operation / Rest-Value Securing

16.1 Fire-Brigade Turn-out Report — (Data not dealt with above)

- Call out time
- Time of arrival
- Number of units

16.2 Actions taken to reduce consequences

Evacuation	(Free text)
Fire fighting	(Free text)
Clearing	(Free text)
Decontamination	(Free text)

17. Target of Accident/Consequences — **Indicate**

17.1 Directly involved actor (driver, operator)

17.1.1 Dead		
17.1.2 Injured	Degree of disability	Lost Time Injury

17.2 Staff of involved enterprises

17.2.1 Number of dead		
17.2.2 Number of injured	Degree of disability	Lost Time Injury

17.3 Environment

17.3.1 Contaminated Land	Area
17.3.2 Contaminated Stream, lake, sea	
17.3.3 Rare species	Free text
17.3.4 Cultural values	Free text

17.4 General Public

17.4.1 Number of dead		
17.4.2 Number of injured	Degree of disability	Lost time injuries

17.5 Investments

17.5.1 Goods	Estimated value
17.5.2 Vehicles	Estimated value
17.5.3 Equipment	Estimated value
17.5.4 Loss of production	Estimated value
17.5.5 Buildings	Estimated value

17.6 Societal functions

17.6.1 Communications	Free text
17.6.2 Municipal water source	Free text
17.6.3 Sewer works	Free text
17.6.4 Electricity	Free text
17.6.5 Institutions	Free text

FACTORS OF RELEVANCE FOR THE OCCURRENCE OF THE ACCIDENT

14.1 Transfer en Route Indicate

- 14.1.1 Road Condition; Standard, state (Planning, construction, maintenance)
- 14.1.2 Transport Planning & Scheduling
- 14.1.3 Cargo Planning (Packing, wrapping, distribution in vehicle, securing, tank cleaning)
- 14.1.4 Driver's Performance (haulage planning, driving)
- 14.1.5 Truck Condition (Vehicle and tanks/ design and maintenance)
- 14.1.6 Traffic Condition

14.2 Temporary stop (not developed)

14.3 Loading / Unloading Indicate

- 14.3.1 Site condition (Planning, construction, maintenance)
- 14.3.2 Equipment on site (design and maintenance)
- 14.3.3 Equipment on vehicle (design and maintenance)
- 14.3.4 Planning of goods transfer
- 14.3.5 Operators performance

14.4 Temporary storing (not developed)

B Supplementary collection of data

B.1 Observations

BASIC INFORMATION

3. Firm of Haulage — **Indicate**

- ***3.1 Name***
- 3.2 Organisational number
- 3.3 Postal address
- 3.4 Visiting address
- ***3.5 Phone number***
- 3.6 Fax number
- ***3.7 Contact person***

4. Driver of Dangerous Goods Vehicle — **Indicate**

- 4.1 Age
- 4.2 Years as DG Driver
- 4.3 Formal Education
- 4.4 Licence as DG Driver
- ***4.5 Hours of driving before Accident***
- ***4.6 Condition***

5. Transport Documents

- 5.1 Dangerous Goods Declaration — Indicate when relevant
  - 5.1.1 Sender; Name, Address
  - 5.1.2 Receiver; Name, Address
  - 5.1.3 Goods: type, designation
  - 5.1.4 Quantity of Goods; Volume, Gross weight, Net weight (explosives)
  - 5.1.5 UN-number
  - 5.1.6 DG class
    - ***1.*** Explosive materials and objects
    - ***2.*** Gases: A. Suffocating; O. Oxidising; F, T, TF. TC, TO, TFC, TOC
    - ***3.*** Flammable liquids
    - ***4.1***, 2, 3
    - ***5.1***, 2
    - ***6.1***, 2
    - ***7.***
    - ***8.***
    - ***9.***
  - 5.1.7 Substance number
  - 5.1.8 Hazard category
    - a) Very hazardous substance
    - b) Hazardous substance
    - c) Less hazardous substance
  - 5.1.9 Exceptions from conditions in ADR due to: Free quantity. Restricted quantity

5.1.10 Restrictions regarding collective loading
5.1.11 Other information; Contract, Exemptions
5.1.12 Senders certificate: Yes/No

5.2 Transport Card ***Yes/No***

5.2-1 Proposed measure in the event of an accident

5.3 Certificate of DG-vehicle valid: ***Yes/No***

5.4 Cleanness certificate: ***Yes/No***

6. Signs & Labels

6.1 DG-Signs on Vehicle: ***Yes/No*** ***Correct: Yes/No***

6.2 DG-Signs on Tanks/Containers: ***Yes/No*** ***Correct: Yes/No***

6.3 DG-Labels on Packages: ***Yes/No*** ***Correct: Yes/No***

7. DG-Vehicle **Indicate**

7.1 Type

Truck	***Weight of vehicle***
Trailer	***Weight of vehicle***
Lorry	***Weight of vehicle***

7.2 Cargo capacity

Volume	Truck	Trailer
Net weight	Truck	Trailer

7.3 Year of manufacture

Truck
Trailer
Lorry

7.4 Time of last Vehicle Inspection

Truck
Trailer
Lorry

8. Transport type **Indicate when relevant**

8.1 Tank (tank or tank-container with volume > 1 m^3. ***Yes/No***

8.1.1 Total tank volume m^3
8.1.2 Number of sections
8.1.3 Approved for;
DG type, DG class
According to (Code)
8.1.4 Year of manufacture
8.1.5 Time of last Inspection by official organisation for testing and inspection

8.2 Tank container ***Yes/No***

8.2.1 Type
8.2.2 Volume
8.2.3 Approved for;
DG type, DG class
According to (Code)
8.2.4 Time of last Inspection
8.2.5 Anchoring

8.3 Bulk (solid not packed material) — *Yes/No*

8.3.1 Type

8.4 Paced Goods — *Yes/No*

8.4.1 Packages; Type, Volume, Type approved

8.4.2 Cargo Fixation

Gods to Gods-carrier; Over-pack

Gods-carrier to vehicle; Stretch straps, wedges, cushions

TIME, PLACE AND CONTEXT OF ACCIDENT

9. Time of Accident

9.1 Year — *Month* — *Day*

9.2 Time of day

10. Place of Accident — **Indicate**

10.1 On Road or Temporary stop

10.1.1 County

10.1.2 District

10.1.3 Street, Street number

10.1.4 Road number

10.1.5 Sector; (between place 1 and place 2)

10.1.6 Position

Road Data Bank

GIB

Country net

10.2 Loading / Unloading / Temporary Storing

10.2.1 County

10.2.2 District

10.2.3 Enterprise where the Accident occurred

Name

Organisation number

Place number

Estate code

Postal address

Visiting address

Phone number

Fax number

Contact person

11. Context of Accident — **Indicate**

11.0 Were the conditions to be considered as normal — *Yes/No*

If No describe in what respect — (free text)

11.1 On Road — Indicate

11.1.1 Type of Accident

Single

Meting

Catching up

Overtaking
Wild animals
Turn off *to the left* *to the right*
Turn into …
Crossing traffic

11.1.2 Involved in Accident
Wild animal
Private car
Other Truck / Lorry
Powered equipment
Unprotected road user or pedestrian

11.1.3 Surroundings
11.1.3.1 Countryside (Agricultural land, Forest land, Wet land, Groundwater reservoir)
11.1.3.2 Densely built-up area (Communication junction, Industrial area, Stores area, School, Day-care centre, Hospitals, Home for aged people, Residence area)

11.1.4 External conditions
11.1.4.1 Weather conditions:
Clear, fog, mist

Rainfall;	*Yes/No*	*Heavy;*	*Yes/No*
Snowfall;	*Yes/No*	*Heavy;*	*Yes/No*
Wind;	*Strong*	*Yes/No*	

Temperature
11.1.4.2 State of road (Dray / Wet /Slippery / Cleared from snow)
11.1.4.3 Visibility (Open / Reduced)
11.1.4.4 Lightening: Existing; Yes/No, Turned on; Yes/No, Satisfactory; Yes/No
11.1.4.5 Road standard;
Type, width, slope, pavement, condition
Security arrangement; ditches, embankments, separations
11.1.4.6 Temporary obstacles; road-works, blocking up vehicles, wild animals, object; tree, branches, boulders, landslide
11.1.4.7 Hazardous objects; railings, posts poles, boulders, rock-side

11.1.5 Traffic conditions
10.1.5.1 Traffic intensity (Low, high, traffic jam)
10.1.5.2 Speed limit (30 / 50 / 70 / 90 / 110 km/h)
11.1.5.3 Normal traffic intensity (according to last measuring)

11.2 Temporary stop *(not developed)*

11.3 Loading / Unloading

11.3.1 Conditions:
Clear, fog, mist

Rainfall;	*Yes/No*	*Heavy;*	*Yes/No*
Snowfall;	*Yes/No*	*Heavy;*	*Yes/No*
Wind;	*Strong*	*Yes/No*	

Temperature

11.3.2 Premises
Lightening: Existing; Yes/No, Turned on; Yes/No, Satisfactory; Yes/No
Signs, Traffic guidance display, and separation: Existing; Yes/No, Satisfactory; Yes/No
Safety separation distances between place for goods handling and;

Warehouse, tanks: Satisfactory; Yes/No
Source of ignition: Satisfactory; Yes/No
Embankment: Satisfactory; Yes/No
Protective railing: Satisfactory; Yes/No
11.3.3 Equipment for goods handling
11.3.3.1 Bulk goods
Conveyer, crane, and excavator: Satisfactory; Yes/No
Pipes, hose, coupling, valve, pump: Satisfactory; Yes/No
Regulator: Satisfactory; Yes/No
Controls: Satisfactory; Yes/No
11.3.3.2 Packed goods
Conveyer, crane: Satisfactory; Yes/No
Fork truck: Satisfactory; Yes/No
Goods securing equipment
Pallets, collars: Satisfactory; Yes/No
Baskets: Satisfactory; Yes/No
Straps, belts: Satisfactory; Yes/No
11.3.4 Supply systems
Electricity
Steam
Compressed air

11.4 Temporary storing (not developed)

THE ACCIDENT

12. Critical Event ***Mark***	***Direct consequence*** ***Mark***
12.1 Loss of containment of dangerous goods	***12.1.2 Uncontrolled energy release***
	12.1.3 Fire / Explosion
12.2 Uncontrolled energy release	***12.2.1 Loss of containment of dangerous goods***
	12.2.3 Fire / Explosion
12.3 Fire / Explosion	***12.3.1 Loss of containment of dangerous goods***
	12.3.2 Uncontrolled energy release

13. Direct Cause **Mark if adequate**

13.1 External damage, wear on;
13.1.1 Tank
13.1.2 Equipment
13.1.3 Container
13.1.4 Package
13.2 Internal damage / wear, corrosion on;
13.2.1 Tank
13.2.2 Equipment
13.2.3 Container
13.2.4 Package

13.3 Over filling
13.4 Unintentional mixing of goods
13.5 Faulty heating of goods
13.5.1 external heating
13.5.2 Faulty equipment
13.5.3 Faulty handling
13.6 Sabotage
13.7 Extra ordinary conditions (Free text)

14. Conducive factors **Mark if adequate**

14.1 Transfer en Route
14.1.1 External force on; tank, armature, container,
14.1.1.1 Impact on stationary surrounding object
Road standard and state
DG-drivers driving and control of DG vehicle
Timing:
Haulage planning,
Unplanned delay,
Promised time of delivery,
Dead lines at terminals
Choice of road
DG-drivers:
Competence; education, experience, training,
Condition
Information to DG-driver:
Goods documentation, Transport cards)
Traffic conditions, weather, state of road
Signs, traffic lights, temporary warning signs -lights
Functioning of vehicle
Vehicle: Design, Equipment, Condition
Cargo: Tonnage, Weight distribution, Securing
14.1.1.2 Collision with other vehicle
DG-drivers driving and control of DG vehicle
(See applicable parts of 14.1.1.1)
Other drivers driving and control of vehicle
(See applicable parts of 14.1.1.1)
14.1.1.3 Goods containers and/or Packages in motion
Distribution within and securing to the vehicle
Container, package
Design: Construction, Compatibility (material – goods), Test
Condition: Control, Maintenance / Cleaning
Cargo securing system
Design, Construction, Material, Test
Condition; Control, Maintenance
14.1.1.4 Wrong handling of equipment
14.1.1.5 Sabotage

14.1.2 Internal damage to; Cargo tanks, Container, Equipment
14.1.2.1 High- or under-pressure
14.1.2.2 Corrosion; Control, Maintenance
14.1.2.3 Wear; Control, Maintenance
14.1.3 Over-filling
(See 14.3.3)
14.1.4 Unplanned mixing of goods
(See 14.3.4)
14.1.5 Erroneous heating of goods
(See 14.3.5)

14.2 Temporary stop (not developed)

14.3 Loading / Unloading

14.3.0 Discharge during manual handling of equipment
14.3.1 External force on; tank, armature, container, package
Run into by vehicle
Traffic separation
Blockade
Handling of; tank, armature, container, package
Lifting devise, conveyer, securing
Wear; Control, Maintenance
Pressure / missiles; from explosion in surroundings
14.3.2 Internal damage to: Tank, Cargo tanks, Container, Equipment
14.3.2.1 High- or under-pressure
Operator's competence and preparedness
Marking and labelling of goods and equipment
Equipment
Design, Construction, Material, Test
Function, Control, Maintenance
Alarm; test
14.3.2.2 Corrosion
Operator's competence and preparedness
Marking and labelling of goods and equipment
Instructions
Equipment
Design, Construction, Compatibility (material – goods), Test
Handling, Control, Cleaning, Maintenance
14.3.2.3 Wear
(See 14.3.2)
14.3.3 Over-filling
Operator's competence and preparedness
Marking and labelling of goods and equipment
Instructions
Misunderstanding / faulty identification of goods container, equipment, vehicle
Equipment
Design, Construction, Material, Test
Function, Control, Cleaning, Maintenance
Alarm; test
Handling

14.3.4 Unintentional mixing of goods

Operator's competence and preparedness
Marking and labelling of goods and equipment
Instructions
Misunderstanding / faulty identification of goods container, equipment, vehicle
Equipment
Design, Construction, Material, Test
Function, Control, Cleaning, Maintenance
Alarm; test
Handling

14.3.5 Erroneous heating of goods

Operator's competence and preparedness
Marking and labelling of goods and equipment
Instructions
Misunderstanding / faulty identification of goods container, equipment, vehicle
Equipment
Design, Construction, Material, Test
Function, Control, Cleaning, Maintenance
Alarm; test
Handling

Extreme Weather conditions
Fire in surroundings

14.4 Temporary storing (not developed)

15. Protective systems functioning

15.1 Transfer en Route

15.1.1 What precautionary measures had been taken on the place of accident to:

– Reduce probability of accident; *(free text)*
Observed effect *(free text)*
– Reduce effect s of accident; *(free text)*
Observed effect *(free text)*

15.2 Temporary stop (not developed)

15.3 Loading / Unloading

15.3.1 What precautionary measures had been taken on the place of accident to:

– Reduce probability of accident; *(free text)*
Observed effect *(free text)*
– Reduce effect s of accident; *(free text)*
Observed effect *(free text)*

15.4 Temporary storing (not developed)

16. Rescue operation / Rest-Value Securing

16.1 Fire-Brigade Turn-out Report (Data not dealt with above)

Call out time
Time of arrival
Number of units

16.2 Actions taken to reduce consequences

Evacuation	(Free text)	
Fire fighting	(Free text)	
Clearing	(Free text)	
Decontamination	(Free text)	

17. Target of Accident/Consequences

17.1 Directly involved actor (driver, operator)		
17.1.1 Dead		
17.1.2 Injured	Degree of disability	Lost Time Injury
17.2 Staff of involved enterprises		
17.2.1 Number of dead		
17.2.2 Number of injured	Degree of disability	Lost Time Injury
17.3 Environment		
17.3.1 Contaminated Land	Area	
17.3.2 Contaminated Stream, lake, sea		
17.3.3 Rare species	Free text	
17.3.4 Cultural values	Free text	
17.4 General Public		
17.4.1 Number of dead		
17.4.2 Number of injured	Degree of disability	Lost time injuries
17.5 Investments		
17.5.1 Goods	Estimated value	
17.5.2 Vehicles	Estimated value	
17.5.3 Equipment	Estimated value	
17.5.4 Loss of production	Estimated value	
17.5.5 Buildings	Estimated value	
17.6 Societal functions		
17.6.1 Communications	Free text	
17.6.2 Municipal water source	Free text	
17.6.3 Sewer works	Free text	
17.6.4 Electricity	Free text	
17.6.5 Institutions	Free text	

B.2 Information Retrieval and Analysis

FACTORS OF RELEVANCE FOR THE OCCURRENCE OF THE ACCIDENT

14.1 Transfer en Route

14.1.1 Road Condition; Standard, state (Planning, construction, maintenance)
14.1.2 Transport Planning & Scheduling
14.1.3 Cargo Planning (Packing, wrapping, distribution in vehicle, securing, tank cleaning)
14.1.4 Driver's Performance (haulage planning, driving)
14.1.5 Truck Condition (Vehicle and tanks/ design and maintenance)
14.1.6 Traffic Condition

14.2 Temporary stop **(not developed)**

14.3 Loading / Unloading

14.3.1 Site condition (Planning, construction, maintenance)
14.3.2 Equipment on site (design and maintenance)
14.3.3 Equipment on vehicle (design and maintenance)
14.3.4 Planning of goods transfer
14.3.5 Operators performance

14.4 Temporary storing **(not developed)**

ADVANCED DATA COLLECTION AND ANALYSIS / AUDITING

– Collect information on what the conditions are for safe operation in the actual case.
– Identify the authorities, the organisations and the departments involved in the processes behind the factors indicated as relevant in connection with the accident. Use a generic ActorMap as in figure 3.5 as a support and create a Map specific of the actual case as in figure 3.6.
– Identify what the identified actors are engaged in when effecting these factors, the relevant process modes.
– Describe these modes by collecting information, as described in part 7.9, regarding the form and content of:

• The information directed downwards in the system about what to achieve and how
• The information directed upwards about the actual condition.
• Regulations and rules affecting the activities

Use the sketchpad in figure 7.6.
– Analyse for mismatches regarding information-flow and preferences of co-acting units.

We are facing a period of technological change, deregulation, fierce competition, and increasing public concern. In this dynamic environment risk management can no longer be based on responses to past accidents and incidents, but must be increasingly *proactive*.

To be proactive, risk management must apply an *adaptive*, closed loop *feedback* control strategy, based on measurement or observation of the level of safety actually present and an explicitly formulated target safety level. Thanks to human flexibility and creative intellectual powers, a human organisation presents a particular potential for such an adaptive control, given the right conditions – people are a very important safety resource, not only an error source.

In this approach, risk management can only be discussed in depth when considering carefully the decision making involved in the *normal operation* of the hazardous processes posing potential for major accidents. A key problem in this context is the information flow among the decision-makers at all levels of society: How are objectives, values, and operational targets communicated? How are the boundaries of safe operation identified and communicated? How is operation monitored through routine operational reports and reports from incidents and accidents? What do guidelines look like when an improved, consistent "safety control" must be established from a proactive control point of view?

This book discusses these issues on the basis of the present rapid evolution of new cognitive approaches to the study of decision making in action and dynamic, learning organisations, and the rapid change of modern information technology with its potential for design of effective decision support systems.

The book is based on material brought forward in an iterative process ongoing for five years, where, in between meetings, documents in electronic form, with ideas, proposals, comments and questions has been passed to and fro between the two authors.

Jens Rasmussen, professor, D.h.c., HURECON, Denmark
Inge Svedung, senior lecturer, PhD, Karlstad University, Sweden

RÄDDNINGS VERKET
Swedish Rescue Services Agency

S-651 80 Karlstad
phone +46-13 50 00
fax +46-13 56 00
www.srv.se

Ordernumber R16-224/00
ISBN 91-7253-084-7

Order from Räddningsverket
phone +46 54 13 57 10
fax +46 54 13 56 05