

Near miss reporting in the chemical process industry

Citation for published version (APA):

Schaaf, van der, T. W. (1992). *Near miss reporting in the chemical process industry*. [Phd Thesis 1 (Research TU/e / Graduation TU/e), Industrial Engineering and Innovation Sciences]. Technische Universiteit Eindhoven. <https://doi.org/10.6100/IR384344>

DOI:

[10.6100/IR384344](https://doi.org/10.6100/IR384344)

Document status and date:

Published: 01/01/1992

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

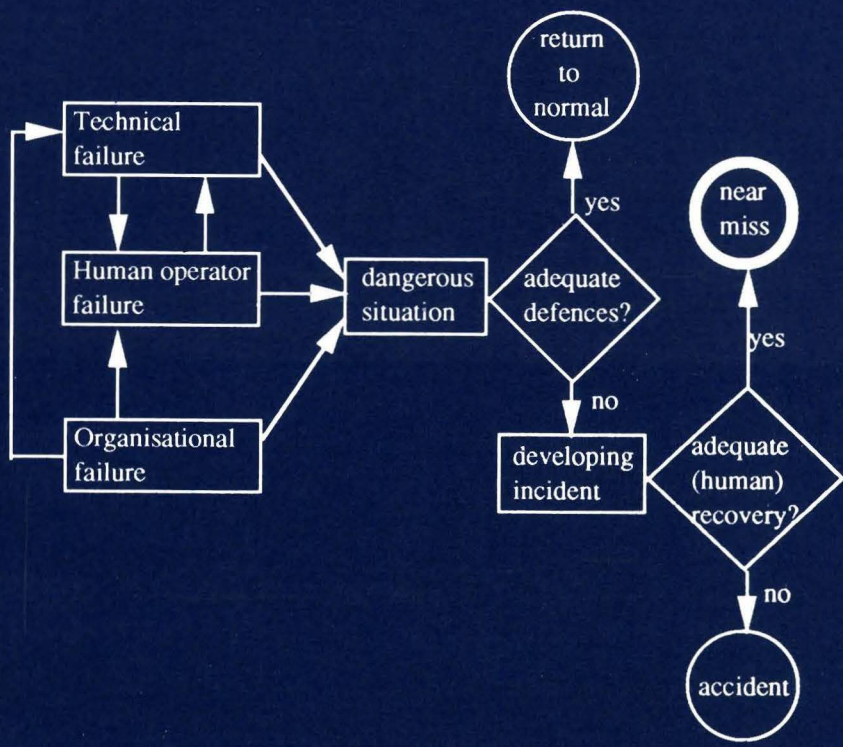
Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

NEAR MISS REPORTING in the chemical process industry



Tjerk W. van der Schaaf

Near miss reporting

in the chemical process industry

Dit proefschrift is opgedragen aan mijn vader

NEAR MISS REPORTING IN THE CHEMICAL PROCESS INDUSTRY

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr. J.H. van Lint, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op

dinsdag 27 oktober 1992 om 16.00 uur

door

Tjerk Woutherus van der Schaaf
Geboren te Medan

Dit proefschrift is goedgekeurd door de promotoren

Prof.dr.s. J. Moraal

en

Prof.dr. A.R. Hale

CIP-gegevens Koninklijke Bibliotheek Den Haag

Schaaf, Tjerk Woutherus van der

Near Miss Reporting in the Chemical Process Industry/

Tjerk Woutherus van der Schaaf.

– Eindhoven: Technische Universiteit Eindhoven, Proefschrift.

– Met lit.opg. – met samenvattingen in het Engels en Nederlands.

ISBN 90-386-0181-6

Trefw.: Near Misses, Chemical Process Industry, Safety Management,
Human Error

© T.W. van der Schaaf
all rights reserved

Contents

	Page
Chapter 1: Introduction	1
1.1 A typical real-life anecdote of near miss reporting	1
1.2 Aims of the research project	3
1.3 Historical overview of the research project	4
1.4 Overview of the thesis	5
1.5 A comparison of chronological order and ordering of chapters	6
Chapter 2: Human behaviour and industrial safety	7
2.1 The human operator as an essential component	7
2.2 Contributing factors of industrial safety and some definitions	8
2.3 A general model of human behaviour	12
Chapter 3: Why investigate near misses?	17
3.1 Usefulness of accident- and near miss reporting	17
3.2 Accidents versus near misses	19
3.3 Purposes of collecting and analysing near miss data	23
3.4 Methods for collecting near miss data	27
Chapter 4: A general framework for near miss reporting systems	31
4.1 General functional specifications	31
4.2 Basic NMMS framework	33
4.3 Implications of different purposes for NMMS design	36
4.4 Extended NMMS framework	38
4.5 Possible uses of the framework	40
Chapter 5: Classification model of process supervision and control errors	43
5.1 Classification of human errors in process supervision and control	43
5.2 Extension to classification of system failure	46
5.3. Eindhoven classification model of system failure	48
5.4 Preliminary classification/action matrix	48
5.5 Conclusions	50

	Page
Chapter 6: Practical aspects in implementation	53
6.1 Practical aspects in design and implementation	53
6.2 Problems of data collection	54
6.3 Acceptance by all employees	54
6.4 Training related to near miss reporting	56
6.5 Safety cultures	56
Chapter 7: European and national experiences with near miss management systems	59
7.1 The CEC workshop on near miss reporting and analysis	59
7.2 A survey on near miss reporting in the Netherlands	62
Chapter 8: A specific NMMS implementation at a chemical process plant	69
8.1 Introduction	69
8.2 Safety management at RAP	69
8.3 NMMS design	71
8.4 Implementation aspects	74
8.5 Preliminary results	76
8.6 Further developments	79
Chapter 9: Discussion and conclusions	81
9.1 Main lessons	81
9.2 Current status of near miss reporting	82
9.3 Future developments	82
Summary	85
Samenvatting	89
References	93

	Page
Appendix 1: The smallpox case	97
Appendix 2: The panel control near miss	99
Appendix 3: List of participants CEC Discussion Meeting	107
Appendix 4: Survey questions within the NMMS framework	109
Acknowledgements	111
Curriculum Vitae	113

Introduction

In this introductory chapter first an anecdote will serve to highlight the main features of near miss reporting. Then the aims of the research project underlying this thesis are outlined, followed by a short history of the project itself. The chapter is concluded by presenting an overview of the themes to be found in the remainder of this book, and an explanation of the order in which they are presented.

1.1. A TYPICAL REAL-LIFE ANECDOTE OF NEAR MISS REPORTING

Ives (1991) gives the following example of the value and the pitfalls of near miss reporting in nuclear power plants:

“The case in question concerned a large non-European state-controlled electricity utility, embarking on it’s first nuclear plant. An expert was employed on contract to write a utility standard for reporting and processing occurrences. The plant management were required to comply with the standard, and for this purpose they wrote an implementing procedure. The standard had an event classification system, using three classes of events, classes 1, 2, and 3, of which class 1 was the most severe. In order to help the plant staff, who were embarking on a new venture, a number of examples corresponding to each of the classes was given in addition to a definition of each class.

The text of the standard contained a section about the importance of reporting near misses (precursors to accidents). In order to encourage reporting, examples of near-misses were given, with the classification of a near-miss, in general, being one class less than the corresponding “hit”.

The standard required a site review, and a head-office level review of all reported occurrences. There was good cooperation between head-office and the plant to get the system underway. Apparent inconsistencies between the definition of the class, and the examples were fairly quickly resolved, with the help of head-office. A data-base of events was established, with an extensive "sort" facility. The system became very well respected and well used, and much improvement of performance was achieved through experience feedback. Near-misses were reported freely, from which much information was gained in order to facilitate performance improvement and the development of "error tolerant" and "error recovery" systems.

From time to time, every Company has to reorganise, - a new Chairman, productivity, profitability, financial targets, cost centres, profit centres, accountability and performance. Performance and the measurement of performance became extremely important although in the process, performance and effort often became confused as did responsibility and accountability. With such confusion, attempts to quantify various things were bound to lead to meaningless results in some cases. In order to measure performance of the plant management, (although in an interconnected system the management do not always have full control of the plant) it was decided to attempt to quantify the unquantifiable and to judge the performance of the plant (one input) on the reduction in reportable occurrences which could be achieved.

The result was immediate and spectacular. The reportable occurrences dropped by 50% in the first month and even more in the subsequent months. An analysis of the situation showed that the actual occurrences had varied little, only the numbers reported had changed. Further analysis showed that some of what had previously been reported as class 2 events were now being reported as class 3 events, and some class 3 events were not being reported at all. Near-miss reporting dried up almost completely. Whereas occurrences are almost always detectable, near-misses are often undetectable and it was clear that in the plant staff minds there seemed little point in reporting what, at the best of times, could be regarded as contentious and which would ultimately lead to their own demise. There followed time-consuming, unproductive, and at times, acrimonious disagreements between head-office and site, about the correct classifications of individual occurrences. Even worse, it was realised

that the near-misses not being reported at all were gone for ever.

Destroying a well functioning system by unthinking management is easy - re-establishing the system subsequently, and the restoration of confidence for using the system is difficult and takes a long time. In this particular case, it was necessary, because of internal politics, to develop a completely new system.”

From this anecdote already some of the main features of near miss reporting may be listed below (a more comprehensive set will be presented in later chapters):

- *learning* from local experiences is the central issue; based on these lessons, better “performance” may be achieved.
- vitally important *implementation aspects* are to be dealt with by management; their commitment must be unambiguous and continuous, and in general various forms of *support* in detecting, reporting and analysing “occurrences” are needed.
- in view of the above, a frequent faulty management decision is to start *misusing such a reporting system*, e.g. by taking the number of reports as an indicator of the organisation’s performance (see appendix 1 for a similar experience, but in an entirely different setting).

1.2. AIMS OF THE RESEARCH PROJECT

The research project carried out at Eindhoven University of Technology underlying this thesis has the following aims:

- to investigate the (potential) *role of near miss reporting in safety management*, especially in the chemical process industry.
- to investigate the role of “*human error*” as a factor in industrial safety, both qualitatively (e.g. which types of errors; which types of preventive measures) and quantitatively (how often do such errors occur; how important is human error relative to technical and organisational failure).
- to make a contribution to industrial safety management by *developing a design framework* (including a human error model) for a complete near

miss reporting system, and by indicating the *organisational success factors* in its implementation.

1.3. HISTORICAL OVERVIEW OF THE RESEARCH PROJECT

The project “Human Error in the Process Industry” within the Ergonomics Section of the Technology & Work Department at the Graduate School of Industrial Engineering and Management Science was started in 1985. In order to get acquainted with the world of chemical process control two exploratory investigations were carried out in the first two years at Dutch chemical companies. This led to the development of a prototype classification model of system failure (see Chapter 5 for the most recent version).

From mid 1988 to the end of 1991 a contract research project was carried out at a chemical processing plant of Exxon in Rotterdam, where one of the main activities was the development and implementation of a so called “Near Miss Management Systems” (NMMS), described in Chapter 8.

In the second half of 1988 a proposal was made to the Commission of the European Communities (CEC) to sponsor an international Discussion Meeting on near miss reporting. This workshop was held in September 1989 at Eindhoven (see Chapter 7).

During 1990 and 1991 the proceedings of the CEC-sponsored meeting were edited and published (Van der Schaaf, Lucas, and Hale, 1991). Also a survey amongst Dutch companies was held, both to test the outcomes of the workshop in relation to safety managers’ experiences and to assess “the state of the art” in near miss reporting in the Netherlands (see Chapter 7).

The first half of 1992 was spent in preparing this thesis and to start preparations for a number of new, related, activities:

- a large scale 3-year research project to develop, implement and evaluate a number of NMMS’s in the Dutch steel industry with financial support from the European Coal and Steel Community.
- the construction of an European network of work psychology laboratories around the theme “Human Error in Dynamic Environments”.

1.4. OVERVIEW OF THE THESIS

Apart from this Introduction, and the Discussion and Conclusions in Chapter 9, three sections may be distinguished in this thesis:

- I. *Chapters 2 and 3* deal with the *general backgrounds* of industrial safety (e.g. models of accident causation and of human behaviour) and with the contributions that near miss reporting could make in understanding and controlling accidents and incidents. Also theoretical criticisms of the near miss reporting efforts are discussed here.
- II. *Chapters 4, 5, and 6* give all the information regarding the *theoretical aspects* involved in *designing* a complete NMMS and ensuring its *successful implementation and maintenance*. A complete system to detect, describe, analyse and follow-up near misses is outlined (Chapter 4), with special emphasis on a model-based classification of system failure (Chapter 5); a number of key issues relating to organisational aspects like acceptance by employees, and “safety cultures” are discussed in Chapter 6.
- III. In *Chapters 7 and 8* the ideas from section II are *confronted with reality* as far as that is possible at the moment both on an European and national scale. Results from case studies and “expert opinions” by safety managers are presented in Chapter 7, illustrating both the possibilities and the problems involved in near miss reporting. Finally in Chapter 8 an extensive feasibility study (the Exxon project) is described in detail, recapturing almost all aspects of design and implementation in a single, practical setting; also a completely worked-out example relating to a realistic near miss is presented in Appendix 2.

In *Chapter 9* a discussion is presented of the lessons learned so far, followed by conclusions regarding the status-quo of near miss reporting. This then leads to a number of suggestions for fruitful topics and applications in the near future.

1.5. A COMPARISON OF CHRONOLOGICAL ORDER AND ORDERING OF CHAPTERS

When comparing the chronological order as presented in 1.3. with the ordering of chapters in this thesis questions might be raised concerning the relative position of Chapter 7, and also concerning that of Chapter 8; both chapters present the results of activities spread out over a two or three year period, parallel to many of the "design" activities reported in Chapters 4, 5, and 6. Therefore, one might equally expect Chapters 7 and 8 to be positioned *before* those of section II, because then they might serve as the "empirical data" on which the NMMS framework, the organisational success factors, etc., could be based.

The reason for placing Chapter 7 near the end was the fact that the NMMS framework modules as presented in Chapter 4 were used already extensively in structuring both the CEC-workshop discussions and conclusions, and also served as the basic checklist during the series of plant visits of the national survey; therefore it seemed important to present the NMMS framework *before* the results of Chapter 7.

Chapter 8 was placed at the end, immediately before the Discussion and Conclusions, for another reason: being the most complete and detailed "feasibility study" from the research project so far it could serve as an *integrated example* of practically all theoretical and practical points raised in earlier chapters; this advantage was considered to be more important than the advantage mentioned above.

Human behaviour and industrial safety

In this chapter a simple model of incident causation is presented and the relative importance of three groups of factors contributing to industrial safety will be discussed: Technical, Organisational and Behavioural Factors. Historic trends or “fashions” focussing on one of these three factors will be described, followed by recent results of the situation in the chemical process industry in the Netherlands.

Finally, the dominant model of human behaviour (or human error) by Rasmussen will be presented which in Chapters 5 and 8 will form the basis of a classification scheme for operator errors.

2.1. THE HUMAN OPERATOR AS AN ESSENTIAL COMPONENT

As technology progresses the safety of man-machine systems depends more and more on the quality of the human component (operator). This fact is very obvious in transportation, where the operator (driver) is formally and actually in control of his or her vehicle. In aviation, however, a strong trend towards software control of the aeroplane is already becoming dominant, forcing the operator (pilot) primarily into the role of supervisor or monitor of the automatic control system and into that of trouble-shooter in case of (technical) failure. In this respect a cockpit crew is facing the same situation as for instance a shift of operators in the central control room of a completely computerised chemical process plant.

This development does *not* mean that we are on our way towards industrial systems without production staff or transportation systems without drivers or pilots.

The human operator will continue to play an essential part in the safety of such complex systems because of several inherent limitations of software control:

1. Only those situations can be handled by software which are foreseen in the design phase and for which software solutions have been found and implemented. Since a substantial part of accidents (Wagenaar and Groeneweg, 1987) happen precisely because of unforeseen or "impossible" circumstances, the flexible human operator will have to be present in order to cope with these, even though he will have difficulties in doing so precisely because of those same reasons.
2. Even the safe handling of foreseen problems is never completely guaranteed, because software, being the result of a complex human activity, will always contain (hidden) errors. The human operator will then have to be able to control the system manually.

Since in this thesis it is assumed that, next to technical and management failure, the behaviour of the human operator is and remains crucial for the safety of the system the need for a proper registration and analysis of that behaviour is a logical consequence. This thesis deals with the possibilities to do just that on the basis of *near miss reporting*.

2.2. CONTRIBUTING FACTORS OF INDUSTRIAL SAFETY AND SOME DEFINITIONS

In the past (and present!), discussions on the contributing factors of industrial safety have always had strong "fashion" aspects. It seems as if every new technology starts out by stressing *technical* factors like design and construction specifications, then moves on to "discovering" the importance of *errors by individual human operators* and finally switches to *organisational and management* aspects as the most important factors. Reason (1991) describes these historic transitions very clearly for *railroad transportation* systems by noting the succession of an "engineering age" to a "human error" period and finally to the "socio-technical" era. The remarkable thing about a more recent very safety-conscious technology like *nuclear power* generation is the fact that according to Reason these very same transitions seem to be fully

recapitulated within its much shorter span: up to the mid-seventies safety measures in nuclear power plants were primarily directed at minimising the consequences of technical failures. This industry's human error concern (inspired by several very clear incidents and accidents) from 1975 on, first focussed on execution failures (like slips and lapses); after the Three Mile Island accident in 1979 one suddenly also realised the importance of cognitive failures or mistakes (like diagnostic errors and the selection of inappropriate recovery strategies).

In this thesis an *integral approach* is followed by assuming that *all three types* of contributing factors must be investigated and acted upon. The most important question then becomes: what is the *relative* importance of each factor and of the interactions between them?

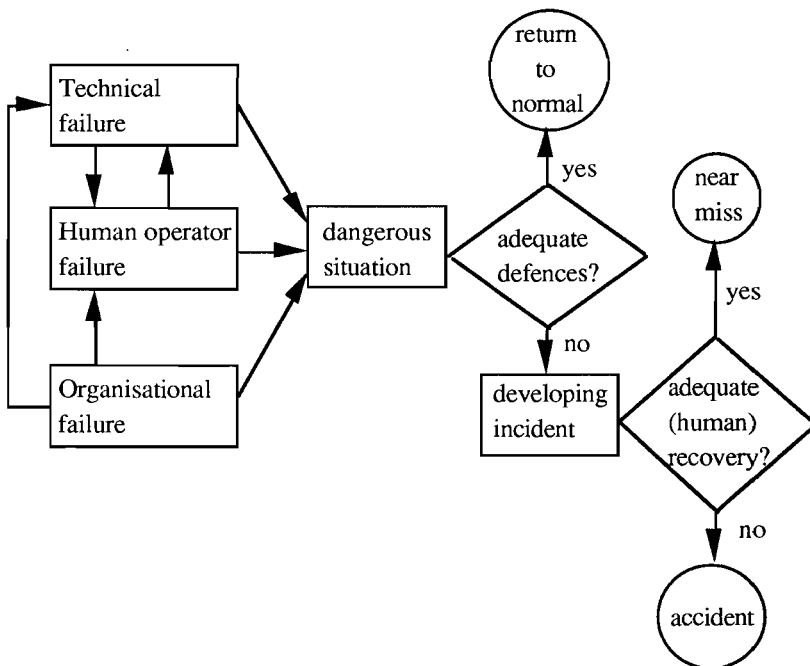


Figure 2.1: A simple model of incident causation.

Figure 2.1 shows a simple model of the main components involved in incident causation, and also *defines* three basic terms used throughout this

thesis: *accident*, *incident*, and *near miss*. Technical and organisational failures can initiate the chain of deviations leading to incident causation events both directly, and indirectly (e.g. by inducing operator failure). Only very seldom is an actually *dangerous situation* assumed to follow from such failures. Even if it does, the “built-in” defences of the process to be controlled will usually be adequate (e.g. automatic safety systems; standard procedures for control of deviations, etc.) but not always. In the latter case the *potential incident* is allowed to develop further and it is usually up to the flexibility, experience, intuition, etc. of the human operator to try to *recover* from this undesired chain of events, and restore the original situation again, or at least to prevent major injuries, damages, etc. This (*human*) *recovery* phase will have been adequate if the developing potential incident is *detected, diagnosed and corrected accurately and in time*; in that case the potential incident is changed into a “*near miss*”, that is an occurrence with potentially important safety-related effects which in the end was prevented from developing into actual consequences. If human recovery was inadequate (e.g. too late; incorrect; or not even attempted) the potential incident will develop into an actual “*accident*”, that is an occurrence with actual adverse consequences (e.g. injuries (or worse), material damages, environmental pollution, etc.). The term “*incident*” refers to the combined set of occurrences of both accidents and near misses.

According to figure 2.1 the basic causes of incidents (also called “*root causes*”) are located at the very beginning of the chain of events, and may be Technical Failures, Organisational Failures, Human Operator Failures, or (most likely) a combination of these. On the basis of this assumption we have done several studies (Van der Schaaf, 1989; 1990) on the relative roles of these three groups of main factors in the last seven years. These studies looked at all kinds of system failures, with consequences varying from zero to (near-) disaster, in three different chemical plants in the Netherlands. Using a preliminary version of the system failure model described in Chapter 5 applied to the *original* in-house incident reports we could classify the main root cause in about 90% of all cases, with the following distribution:

– Technical Failure	≈ 30%
– Organisational Failure	≈ 10%
– Operator Failure	≈ 50%
– Unclassifiable	≈ 10%

(It is interesting to note that these figures were practically identical for all three companies, in spite of large (cultural) differences between them. These figures should however not be taken too literally; e.g. because of likely under-reporting of organisational factors this figure will probably increase if investigated further.)

Nevertheless, the main conclusion must be that all three factors are of importance, with operator behaviour as the most dominant one. How then should we interpret the abundance of newspaper reports and other sources (Wagenaar, 1983) which proclaim that 90% to 99% of all such incidents are caused by “human error”?

Firstly, it may refer to the *use of “human” error in a useless way* when “human” refers not only to the person(s) directly involved in the incident but also to the designers, constructors and managers who gave the “operator” the tools to be used during task performance; in the end of course practically any design or management aspect of these “tools” and tasks may be traced to some human action or decision. At the same time such a definition then becomes useless because it does not give a single clue as to where and how improvements might be made.

Secondly a reason might be that the *incident investigation usually is rather superficial* in the sense that it often looks only at the events *directly* preceding the observable end components of a usually long and complex set of real root causes and their interactions. These observable end components often consist mainly of human actions (or the lack of them). Therefore, we propose to define “human” by *choosing a certain focus* or starting point, dictated by the goal of the investigation. If one is interested in the behaviour of control room operators then *their* task should dictate the classification: “human” error refers to *their* behaviour, “organisation” might refer to the procedures *they* have to follow for instance, and “technical design” refers to *their* workplace (e.g. control-room layout) and equipment, etc. One could equally be interested

in the role of the engineers of course, but in that case the engineers become the human/"operator" component in the analysis; company guidelines for Engineering and Design Practices are then part of the "organisation" factor, etc.

In short, we propose a *goal-directed classification* (fully described in Chapter 5), because then we can fruitfully distinguish between the three main factors determining industrial safety.

2.3. A GENERAL MODEL OF HUMAN BEHAVIOUR

Since human behaviour seems to be the dominant factor in industrial safety (at least in the Dutch process industries) a proper model is necessary for understanding it and should be chosen from the literature (see Reason, 1988, for an overview). For the purpose of the projects leading to this thesis the well known *hierarchical "SRK" model* by Rasmussen (1976) was selected: many of its concepts (but not all: see Bainbridge, 1984) are widely accepted and used by both researchers and practitioners in the field of human error and safety management, which means it is relatively easy to communicate and perhaps compare its results with other data based on the same model. Its influence is also clearly visible in more recent models (e.g. Reason, 1987; Hale and Glendon, 1987). Figure 2.2 shows the main components (e.g. stages in human information processing) and the three different main paths of information flow which determine whether task performance is mainly based on Skills, Rules or Knowledge.

The three resulting levels of (operator) behaviour are hierarchically related and defined as follows:

–*Skill-based behaviour*, referring to routine tasks, requiring little or no conscious attention during task execution. In this way enough "mental capacity" is left to perform other tasks in parallel. Example: an experienced car driver travelling a familiar route will control the vehicle on a skill-based level, enabling him/her to have an intelligent discussion, parallel to the driving task, with a passenger.

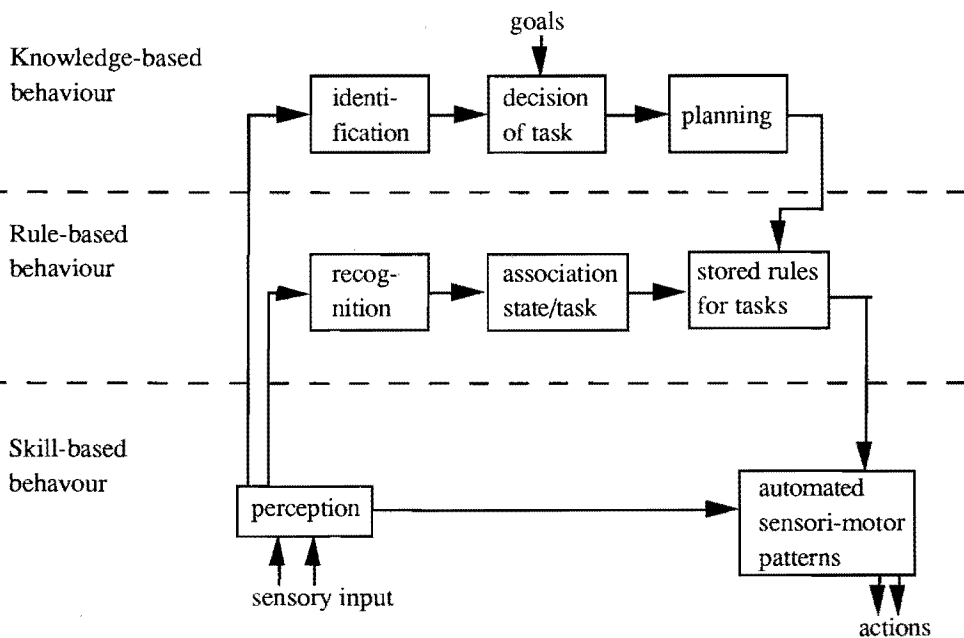


Figure 2.2: A simplified version of the hierarchical SRK model by Rasmussen (1976).

- *Rule-based behaviour*, referring to familiar procedures applied to frequent decision-making situations. A car driver integrating the known rules for right-of-way at crossings with stop signs or traffic lights, to decide whether to stop the vehicle or pass the crossing is functioning at this level. The separate actions themselves (looking for other traffic, bringing the vehicle to a full stop, changing gears, etc.) will again be performed on a skill-based level. Making these familiar decisions and monitoring the execution of the skill-based actions requires some part of the total mental capacity available to the driver, but not all.
- *Knowledge-based behaviour*, referring to problem-solving activities for instance when one is confronted with new situations for which no readily available standard solutions exist. The same car driver approaching a crossing where the traffic lights have broken down during rush hour will first have to set his primary goal: does he want to proceed as fast as possible or does he want to minimise the chance of collision? At the same time he will

have to decide whether the normal traffic rules are still applicable or whether he has to invent some ad-hoc procedures to cope with this situation. As a result, (almost) all of his attentional capacities will be allocated towards this problem-solving process, thereby stopping any other parallel tasks.

An alternative way to describe the SRK model is to trace the changes in the behaviour of someone *learning a new, complex task*. In our first driving lessons for instance even some of the subtasks in controlling a car (e.g. changing gears) may demand so much attention that we forget the steering subtask, let alone the monitoring subtask to watch other vehicle movements. Only gradually do we learn certain subprocedures to “solve” recurring “subproblems” (e.g. the pattern of movements needed to change gears; the rules of right-of-way for different types of traffic). In the next phase we learn to *automate* these subprocedures to such a degree that several of these subprocedures may then be *integrated* into more complex sets of different types of actions and decisions, triggered by an appropriate *signal*: a reaction to sudden braking lights of the car in front of us would involve a check in the rear mirror for cars immediately on our “tail”, then deciding to brake or make an evasive action, and subsequently carry out the associated movements of hands and feet. According to this view learning means *automating subtasks* and *integrating* these subtasks into larger behavioural units: first you are told at which speed to change from first to second gear, etc. (Knowledge-based); knowing this, you can determine these trigger points of action yourself by monitoring the speedometer (Rule-based), and after a while the sounds of the engine will tell you “unconsciously” it is time to change gears (Skill-based).

In this thesis the most important implication of this model is the prediction that *different types of errors* (Skill-, Rule-, or Knowledge-based) *imply different types of preventive measures*:

–*Skill-based (S-B) errors* are not easily prevented because of the highly automatic (or unconscious) “open-loop” character of this level of behaviour: either you learn to live with them, or you *change the task environment* in which they occur, when human error seems to have been “built in” (quite predictably) in the design stage. Especially *ergonomics* may contribute in

this respect, for instance by improving the layout of information presentation on VDU screens in order to prevent detection- or reading errors.

–*Rule-based (R-B) errors* often consist of inadequate habits. In such cases it might help to decrease the advantages of such behaviour and increase its disadvantages. At the same time one could, vice-versa, stress the advantages of the required behaviour and decrease its associated disadvantages. For instance one may encourage wearing safety spectacles when prescribed by company rules in several ways: allowing employees to choose the spectacles which they find most comfortable; giving positive feedback when they are actually seen using them; confronting employees with potential consequences of not wearing them when required; and fighting any “macho” image of employees taking pride in ignoring such safety rules.

–*Knowledge-based (K-B) errors* may be caused by lack of knowledge and understanding of the problem to be solved, which points at measures like *(re-)training and selection*. More often however the problem lies in *the way knowledge is being wrongly or partly used* in problem solving situations. For instance, thinking in terms of analogies does not always work; also *biases* like “confirmation” or “fixation” lead to ignoring relevant information which contradicts a preliminary diagnosis or solution. In such cases *Decision Support Systems* (e.g. Expert Systems; intelligent interfaces) may prevent such biases from exerting too much influence by reminding employees that some sources of information have not yet been taken into account, or that a number of assumptions may not be necessarily true under the present circumstances, etc.

In chapter 5 the relationship between types of error and effective countermeasures will be presented in more detail in the form of a Classification/Action Matrix (see figure 5.3.).

The SRK model has not been without theoretical criticism. Bainbridge (1984) summarizes two of the main points brought forward against it. Firstly, she mentions *problems in interpretation* of the words “skill”, “rule”, and

“knowledge”. These would not only be fairly vaguely described, but sometimes also used inconsistently. As a result it is not easy to operationalise them precisely. Secondly, the *hierarchical sequence* of types of behaviour as described in Figure 2.2 is criticised by Bainbridge as being not flexible enough (e.g. it only describes stimulus-response routes of human information processing) to model the entire spectrum of problem solving activities by operators.

However, in a situation where *none of the then available models* of human behaviour (or human error) had yet been *properly tested*, other, more practical, aspects must determine the choice to be made: in this project, where the requirement of an effective implementation of such a model in the technical setting of chemical process control (see Chapter 8) was highly important, the Rasmussen model had two important practical advantages:

1. the concepts of S-B, R-B and K-B behaviour are easily understood and accepted both by many cognitive psychologists and by engineers (which is not so strange as Rasmussen was trained as an engineer himself!);
2. due to point 1., and to the fact that the SRK model is (one of) the oldest model(s), it has spread all over the (Western) world, influencing the labelling, classification, etc. of many relevant sets of data on industrial accidents and safety programmes. Therefore, in the future it could be possible to compare one's own results directly with those of others.

As mentioned earlier, this SRK model will form the basis for the Eindhoven classification model of system failure in process control tasks (see Chapter 5), which in turn is the “analytical heart” of the framework to design near miss reporting systems proposed in Chapter 4.

Why investigate near misses?

This chapter starts with a discussion of the usefulness of incident reporting systems (of accidents *and* near misses) and then goes on to compare accidents *versus* near misses with the help of a qualitative “iceberg” model. Next, three different purposes to collect and analyse such incidents are outlined. Finally, several methods to collect near misses in a variety of settings are presented.

3.1. USEFULNESS OF ACCIDENT- AND NEAR MISS REPORTING

Reason (1991) launches several fundamental critical remarks concerning the usefulness of information based on accidents and near misses: these would only relate to the last (few) steps in an usually long chain of causal events. The information thus provided is considered to be both “noisy” (e.g. the real root causes cannot be traced back) and *too late* (e.g. it promotes reactive instead of proactive safety management). Even near miss reporting may at most raise individual safety consciousness, and, at the same time, communicate top-level concern with safety. Reason (1991) therefore proposes to look only at those factors at the very beginning of the chain of events: *management decisions* relating to the quality of hardware, procedures, organisational structures, training etc.. Auditing and controlling these “General Failure Types” would be the most efficient way of safety management.

Reason’s position may be illustrated by examining figure 3.1, showing four different feedback loops of information for safety management:

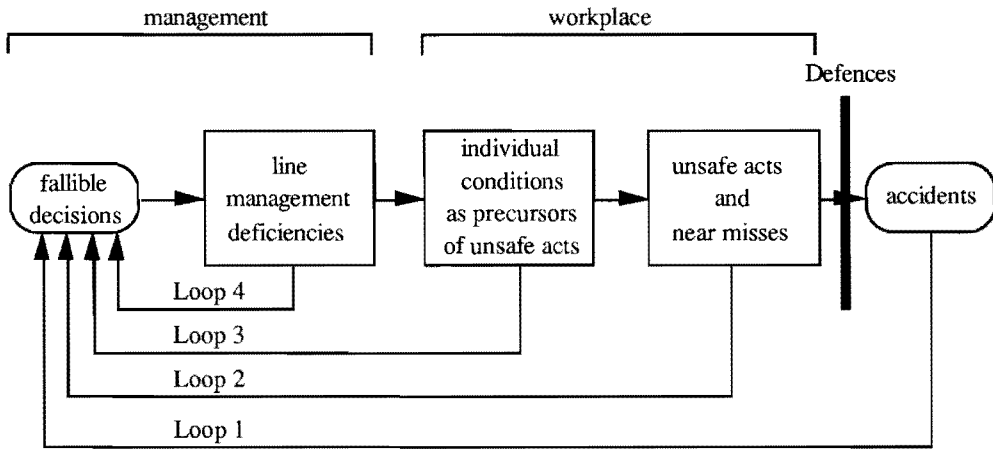


Figure 3.1: A simplified version of Reason's (1990) model of safety-related feedback channels.

- *loop 1* (accident reporting) is the most widely used channel, but contains only information which he claims to be too “noisy” and too late for efficient root cause identification and elimination.
- *loop 2* (unsafe act auditing and near miss reporting) also has limited value according to Reason, if only because such an enormous number of these occurrences happen, that measuring, let alone eliminating them would be an impossible task.
- even *loop 3* (individual conditions like poor workplace design, high work load, inadequate training, etc.) is considered as not very useful to predict future accident scenarios.
- only *loop 4* (“failure type indicators” at the level of management activities) is considered by Reason (1991) to belong to the organisational domain where safety managers can begin to exert effective and targeted control over the system. Examples of such failure types are design failures, poor maintenance procedures, incompatible goals, or communication failures.

As a reaction to Reason's criticism, in this thesis it is fully agreed that accident- and near miss reporting *alone* would be *insufficient* to support effective safety management; however, this must be true of *any* single specific tool or approach, considering the enormous complexity and variety of inci-

dent-causation processes. Also, the NMMS design to be presented in Chapter 4 clearly aims precisely at “backtracking” from the reported near miss to its set of root causes. Besides, in the “Monitoring mode” (see section 3.3.) not the specific root causes of an *individual* near miss are the basis for safety management decisions, but the statistical results of the analysis of a *large database* of such incidents.

Also, we shall see in section 3.3., Reason’s proposal to use an auditing tool of a standard set of faulty management decisions clearly aims only at the “Monitoring purpose” of near miss reporting, perhaps also somewhat at the purpose of “Alertness”, but certainly does not contribute to “Modelling”, i.e. to understanding how the development from left to right in his model can occur.

Our conclusion therefore is that the auditing tool described by Reason may certainly complement a NMMS as described in Chapter 4, and might also serve to cross-check the NMMS’s results on Organisational factors (see Chapter 5), but will not be able to replace a NMMS aimed at all three purposes to be outlined in section 3.3.

3.2. ACCIDENTS *VERSUS* NEAR MISSES

3.2.1. In the proposal to the Commission of the European Communities (CEC) to start a European Platform for researchers and practitioners in Near Miss Reporting (see section 7.1.) the following position was taken (Van der Schaaf, 1988a):

“Until now research efforts in safety management have been focussing primarily on the number of accidents (system failures leading to personal injuries and/or material damages) as the prime index for system safety. There are three main reasons for redirecting our attention in this respect:

- 1. Accidents are only the tip of the iceberg: they materialise out of sudden unsafe situations, which in turn are often caused by undesirable operator behaviour (human error). We have to know much more about these underlying precursors of actual accidents if we aim at more fundamental understanding of the process of accident production.*
- 2. Moreover another important, so far neglected, aspect of human behaviour*

is receiving attention from safety researchers: human recovery, the ability of operators to detect, localise and correct system faults caused by either human error or technical failure. In terms of system reliability it could be just as efficient to increase the probability of timely recovery as to try to prevent failures in the first place.

The two reasons mentioned above are of a fundamental nature: they aim at an improvement of the quality of (near-) accident reports. The third reason is more practical and should increase the quantity of reported cases.

3. Accidents are very rare relative to the number of near accidents and human errors. Fortunate as it may seem, this poses a real problem for complex systems with a high "catastrophy potential" (nuclear power plants, chemical plants, commercial aviation): few accidents means few cases to analyse and hardly any feedback to learn from. This leads to the undesirable situation of ad-hoc corrective measures after each single accident, because the database is far too small to generate statistically sensible preventive measures.

Hence, it is necessary to collect "near miss" data as well as accident data. The much more numerous unsafe situations (both chronic and sudden) and even more abundant human errors not resulting in serious consequences are assumed to have the same psychological root causes as the tiny subset that actually develops into an accident. The same data-base size may thus be reached much sooner, or a certain observation period may yield a much more reliable insight into the causes of (near-) accidents.

Also the effects of implemented preventive measures may be monitored and evaluated much sooner and/or more reliably in this way."

In this paragraph we will investigate the above "statements of belief" in terms of their theoretical and empirical support. A qualitative "iceberg" model will be described in order to distinguish near misses from actual accidents on one hand, and behavioural acts on the other.

3.2.2. A qualitative iceberg model

Quite often in the literature (e.g. Hydén, 1987) a pyramidal representation (often referred to as “iceberg”) is used of the assumed *continuum of events* ranging from normal behaviour via conflicts and deviations to actual accidents (see figure 3.2).

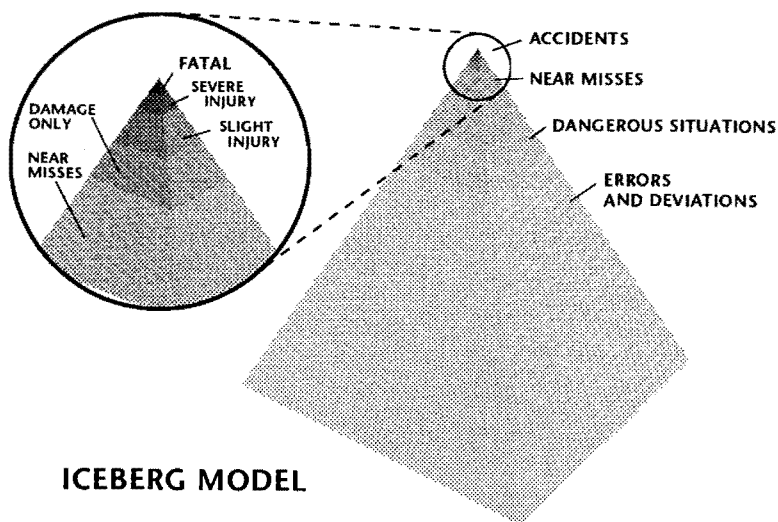


Figure 3.2: A generic pyramid or iceberg model (after Hydén, 1987).

For the purpose of this paragraph we will simplify the above figure to a mere triangle with only three layers; near misses are “caught” in between actual, but rare, accidents on the top and an enormous number of behavioural acts (e.g. errors *and* recoveries) more to the bottom (see figure 3.3), with different positions on four interdependent dimensions.

Incident causation is assumed to progress from the bottom to the top, which means that chances for early prevention of accidents decrease as you get closer to the top. The *order of incident analysis* is assumed to be top-down, but with different starting points in the iceberg depending on the type (or level) of data that trigger the detection in the first place. It is also assumed that modern investigation techniques will always try to get as far to the bottom of

the iceberg as possible and not stop at superficial descriptions of only the immediate events leading to an accident and its short-term consequences. Another vital assumption is that these three levels of the iceberg are directly related in the sense that they show largely overlapping sets of “root causes” (e.g. as in Chapter 5); a different starting level should *not* lead to an entirely different set of root causes being identified by the analysis, and should also then *not* lead to a fundamentally different set of suggested actions in order to tackle these.

The starting point of detecting and analysing incidents must therefore be determined by other dimensions, such as *frequency of occurrence* and the “*visibility*” of incidents. Figure 3.3 shows the well-known phenomenon of very rare (in some companies even absent) accidents and an abundance of errors and recoveries. It also goes without saying that actual accidents have the highest visibility, but that day-to-day behavioural acts are easily overlooked, although their consequences in less forgiving environments might have been serious.

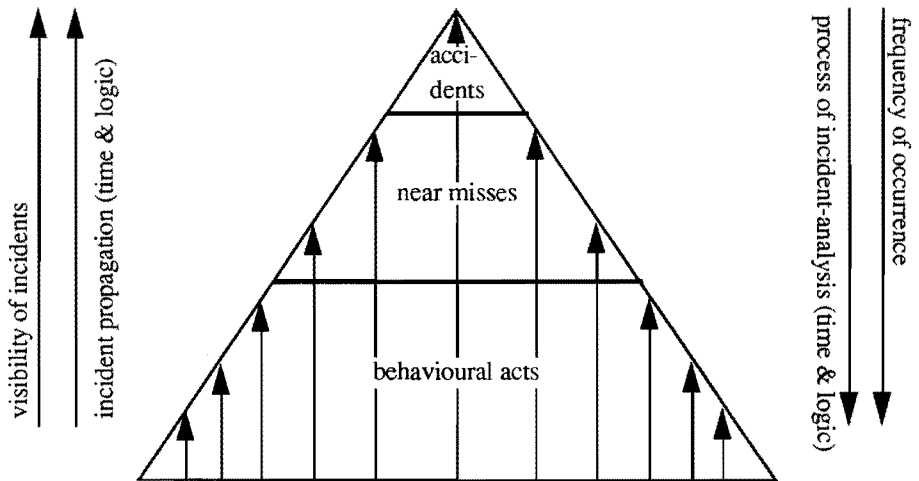


Figure 3.3: A qualitative iceberg model of the relationships between accidents, near misses and behavioural acts.

As an illustration a few examples may be useful:

- Crane driver drops a load (dangerous occurrence)

- . it hits a person standing below (an accident),
- . no one is standing underneath at the time (near miss: chance factors),
- . a coworker pushes a person out of the way (near miss: human recovery),
- . the area under the crane is restricted (near miss: management control),
- . the crane design has an automatic stop device (near miss: technical safeguard).

– Air miss, that is two planes on a collision course

- . crash occurs (an accident),
- . one pilot sees other plane just in time to take evasive action (near miss: human recovery),
- . air traffic controller spots the conflict and orders new course (near miss: human recovery, but with different agent),
- . warning device in cockpit detects collision course (technical safeguard requiring some human action or decision),
- . one plane just happens to change altitude before time of impact (chance factors).

3.3. PURPOSES OF COLLECTING AND ANALYSING NEAR MISS DATA

Three general classes of such purposes may be distinguished:

1. to gain qualitative insight into how (small) failures or errors develop into near misses;
2. to arrive at a statistically reliable quantitative insight into the occurrence of factors or combinations of factors giving rise to incidents;
3. to maintain a certain level of alertness to danger, especially when the rates of actual injuries and other accidents are already low within an organisation.

The first purpose is unique to near miss reporting, while the other two could in principle be also achieved by *accident* reporting. However, for the second purpose the advantage of near miss reporting lies in the fact that a large database may be built within a relatively short timeframe. The absence of any real adverse effects in the case of near misses may be considered as an

advantage over accidents with respect to the third purpose: looking for scape-goats will be less likely when no real harm is done, and this will give more opportunity to focus on the backgrounds of the successful preventive efforts.

3.3.1. Qualitative insight: Modelling

We may wish to get a better understanding of how serious accidents *might* occur in our plant, or more generally for research purposes; in that case we are aiming at *modelling* the “production” of such accidents within and by the system as a whole. Because the role of *human* safety-related behaviour is of special interest we should acknowledge the fact that humans are not only interesting for the *errors* they make, but also for their *error-compensation behaviour* or *recovery*; unlike most other system elements humans are assumed to have the capability to correct their own (or others’) earlier errors or even small system failures by a timely action. This human recovery aspect will be especially prominent in investigating *near-miss* situations. Some preliminary proposals for modelling human recovery can be found in Van der Schaaf (1988b, 1991b). Related ideas can be found in Norros et al (1989) and Svenson (1991). Norros et al. (1989) stress the fact that system *disturbances* should not be considered as just threats to the system, but also, based on the concept of “operation-oriented design”, as *opportunities for the users to construct their expertise* in handling the system. Svenson’s (1991) Accident Evolution and Barrier Function (AEB) Model tries to analyse why *barrier functions* fail, and how they can be reinforced.

From a safety management perspective a specific goal within this broader purpose is then to *identify likely factors* or system elements in the sequence of events leading to near misses which in turn may be considered as *precursors to actual future accidents*. From such a qualitative analysis two ways emerge to reduce the likelihood of such actual accidents: *error-inducing factors* can be eliminated (or their potential impact weakened), and *recovery-promoting factors* can be strengthened (or even introduced) in the system.

Another type of qualitative insight could be the result of regularly discussing unusual or *unique near misses*, i.e. new or unexpected combinations of circumstances might trigger an “Aha” experience with safety staff members and other employees. This means that their set of “*possible accident scenarios*”

is enriched. Not only does this help them in their general understanding of system safety but it should also keep them aware of the practical impossibility of listing all types of failure modes (for any system of some complexity) in advance; after all, in actual accidents very often the “impossible” or “unthinkable” happens (see also section 2.1.).

To summarise, the purpose of Modelling assumes that accidents and near misses have (approximately) the *same set of root causes*, and that near misses in general can be seen as *precursors* to possible accidents. General support for these qualitative assumptions can be found in Heinrich (1931), Swain (1974) and Ferry (1988), however without strong empirical evidence. The literature on so called “traffic conflicts” (e.g. near misses at intersections) however does support this validity claim in an overview paper on accident analysis and conflict behaviour by Grayson and Hakkert (1988). Near misses as precursors are also shown in many anecdotes. For example, Moraal (1983) cites a sequence of no less than nine similar near misses before the infamous accident at the Three Mile Island nuclear plant occurred. Van der Schaaf, Hale and Lucas (1991) however point out that the very same advantage of near misses of concentrating on recovery has a negative side too. Those factors at the end of the incident chain which (in the case of accidents) have prevented timely recovery will by definition *not* show up in near miss reports. Their conclusion therefore is that to avoid a truncated sample near miss analysis should concentrate on the *early steps* only of the incident-causation process (e.g. from the root causes up to the point(s) of recovery action) if one’s goal is to locate root causes as potential accidents. Finally, our own pilot data (Van der Schaaf, 1989, 1990) on root causes on the basis of existing accident- and near miss reports in the Dutch chemical process industry (see section 2.2.) also show similar distributions for both types of incidents, at least at the level of Technical, Organisational and Operator-behaviour factors.

3.3.2. Quantitative insight: Monitoring

Near misses are usually estimated to occur one or two orders of magnitude more frequently than actual accidents. For example, those case studies discussed in Chapter 7 where reliable data were available showed ratio’s of 11:1, 32:1, 80:1 and 600:1, while Petersen (1989) mentions 300:1. Even ignoring

the fact that both the definitions used, and the tasks involved were quite varied, the point to be made here is simply that many more opportunities exist to register near misses than accidents; whether this ratio is 10:1, 30:1 or 100:1 is not interesting. Many companies, and especially those which have already reduced their accident rate to a relatively low level, paradoxically can not measure their "safety performance" in a reliable way; their database of actual accidents is far too small to distinguish random fluctuation from actual trends. Because of their abundance near misses may then be used for such statistical *monitoring* purposes to decide on increasing, decreasing or stable trends.

Specific goals here might be to be able to point out to management which combinations of *factors* are *most frequently* encountered in the analysis. This would provide them with a rational decision rule of where to concentrate resources (of time, efforts and funds) in order to increase the safety level in a *more efficient way*.

Also the *effectiveness of actions* taken to improve safety could be monitored in a quantitative way: a preventive action aimed at a specific error type should result in a reduced frequency of such errors when analysing subsequent near misses; likewise, recovery promotion should be measurable by an increase in frequency of its occurrence later on.

Again, just as in section 3.3.2., *direct* evidence from process control industry to support this Purpose is lacking. However, from studies of *traffic conflicts* Grayson and Hakkert (1988) conclude that such conflicts are a valid surrogate measure for actual accidents in evaluation work.

3.3.3. Alertness

Persistent awareness of the dangers of one's workplace or of the system as a whole is crucial to any organisation's "Safety Culture", and therefore to the safety-related behaviour of all levels of its employees. This "Alertness" may be achieved by providing *feedback* to *all* employees, not only of the types of incidents being reported, but also of the way they are "processed" within the organisation, and of the results thereof. Another strong motivating factor is *end-users participating* in the development and maintenance of a near miss reporting system.

An important advantage is that near miss investigation provides a *pre-*

ventive perspective much more than accident investigation which is corrective by nature. This issue in fact comes down to the well-known contrast between proactive and reactive management (Reason, 1991). Specific goals within this last type of purpose are firstly to counteract the idea that problems have been solved because there have been no accidents recently. Knowledge of reported near miss situations may be used to stress the fact that these should be considered as *precursors* to real accidents in less “lucky” future circumstances.

Near misses also provide a wealth of *in-house* and *convincing examples* of common errors and recoveries. These may be used in training programmes for future managers and operators and in specific safety promotion campaigns.

The act itself of recognising a near miss and reporting it is a form of *employee-involvement* which should lead to improvement in safety-awareness (Swain, 1974), although Hale and Glendon (1987) point out that the exact “alerting” effect of “planned near misses” (e.g. watching a film of an incident, emergency training in simulators, etc.) is still an under-investigated area in safety management.

In conclusion, a central hypothesis in this thesis would be the following:

For many companies and authorities near misses may provide an optimum between highly visible (and detectable) but rare accidents, and very frequent but almost invisible behavioural acts, and they are therefore worth collecting and analysing.

Or, as Perrow (1984) puts it: *trivial events* (e.g. everyday failures) in *non-trivial systems* (e.g. with catastrophic potential) *should not go unremarked.*

3.4. METHODS FOR COLLECTING NEAR MISS DATA

Near misses may be collected by way of several possible techniques. They may be *reported* by the persons “experiencing” the near miss on either a voluntary or mandatory basis. They may however also, because of their “visibility”, be *observed* by registration equipment or human observers. Finally they may be *generated* in experimental conditions, usually by means of

complex *simulation* facilities.

3.4.1. Reporting-based methods

These methods expect the employees themselves to report on such incidents as part of their job. In this respect there is an analogy with the Critical Incident Technique (Flanagan, 1954), but now geared specifically towards safety-related issues. Usually references are made towards preventing accidents happening to less lucky colleagues in the future, or it may be required or expected in the course of some Total Quality Programme. An example of *voluntary reporting* is given in Chapter 8, from the process industry. *Mandatory reporting* seems to be more prevalent in some sectors of transportation, as shown by the fact that both pilots and air traffic controllers are legally required to report air misses in most countries (Cannell, 1989).

3.4.2. Observation-based methods

Outsiders with respect to the chain of events leading to a near miss may also be used to detect such incidents. A clear example of *automatic registration* is described by Taylor and Lucas (1991) on the passing of railway signals at danger. Also the famous "black boxes" in aircraft may be put into this category, where they are not only investigated after an accident, but on a routine basis after each flight to detect excursions outside planned flight parameters. In systems where near misses may be expected to occur predictably under certain system conditions (like starting up a plant) or at regular intervals (like rush hours in a congested city) *human observers* may be trained to detect them. Traffic *conflicts* (no crashes or injuries) are good examples (see Van der Horst, 1991; Brown, 1991), and in one of the cases reported by Ives (1991) engineers were on stand-by to observe operator actions under critical conditions. In such observations usually only a *sample* is taken from the set of all locations and all opportunities; otherwise it would soon demand astronomical resources.

3.4.3. Simulation-based methods

A more experimental approach is given by Masson (1991) which deals with simulation facilities. These may be used to *generate* errors, recoveries, near misses and “accidents” on the basis of suitable scenarios. Because the conditions are under the control of the experimenter very efficient data collection is possible, but the question is always whether these data are *valid* and therefore generalisable to the real world.

Another way of using simulation facilities is for *modelling* purposes; the effects of time-stress on fault diagnosis for instance could be modelled in this way, and frequent errors and recoveries could then be used to arrive at suggestions for decision support and interface design.

3.4.4. Selecting a particular method

It is very difficult to advise on one (or more) of the above methods in a particular situation. The main question to be answered first is *which purpose(s)* should have priority. Even so, at least *four other aspects* must be taken into consideration:

- *level and visibility* of the “dangers” involved; highly visible high-consequence situations could favour voluntary reporting. Dangers which are less obvious to the reporting employees suggest the use of automatic recording.
- *amount and depth of data required*: observation-based methods may “produce” many more instances of near misses, but with *less depth* than reporting one’s own (partly invisible) diagnostic misinterpretations for instance: K-B errors are less observable than S-B errors according to section 2.3.
- *phase of the (production-)system*: in the design phase a simulation/modelling approach would probably be more fruitful than when production has already been started and changes in the hardware have become very expensive.
- *acceptability to the employees*: automatic recording can give rise to concern among employees who fear a “Big Brother” regime spying on them (Algera, 1987). Voluntary recording will only work with high personnel motivation (see Chapter 6).

A general framework for near miss reporting systems

In this chapter we will focus on the *contents and the design process* of systems aimed at the reporting, description, analysis and interpretation of near miss situations. Although certain aspects of the following framework for designing such a "Near Miss Management System" (NMMS for short) will be aimed at issues like implementation, maintenance and acceptability, *the main overview of such organisational aspects will be presented in Chapter 6*. Chapters 4 and 6 may therefore be considered as "twin chapters".

After listing a few *general functional specifications* for a NMMS design framework its *seven basic steps* or modules are introduced. Subsequently the implications of stressing the *different purposes* from Chapter 3 are discussed. *An extended version* of the framework is then presented related to its functioning at higher organisational levels than that of the basic version. The chapter is concluded summarising the different possible *uses of such a framework*.

4.1. GENERAL FUNCTIONAL SPECIFICATIONS

On the basis of the assumptions and experiences presented in Chapters 1, 2 and 3 four fundamental ideas or requirements are regarded here as functional specifications for designing a NMMS:

1. the *only* function of the NMMS should be to *learn* at an organisational level from the reported near misses (see section 1.1);
2. its coverage of possible inputs and outputs should be *comprehensive* in a *qualitative* sense (see section 2.2);
3. the "heart" of the NMMS should be a *suitable model of human behaviour* (see section 2.2);
4. the NMMS should not be an "alien" system within an organisation, but be *integrated* where ever possible with other management tools in order to maximise its acceptance (see Chapter 6).

4.1.1. Learning from near miss reports

Organisational learning should be central to the NMMS, i.e. a progressively better insight into *system* functioning, not into individual performance. The final goal of the NMMS is *to control* or manage the safety aspects at the system level, not at the level of specific individuals interacting with the system. Except for instances of sabotage, the NMMS output should never lead to "apportioning blame" upon individual employees.

Another aspect of the NMMS as a learning instrument is the *dynamic* nature it should have: by building feedback loops into the NMMS it should be possible to improve its components continuously.

4.1.2. Comprehensive coverage

The NMMS should be comprehensive in several qualitative aspects:

- it should be able to handle not only near misses, but also actual accidents, damages, etc., or be capable of being linked to an existing accident reporting system;
- in its description and analysis it should pay attention not only to *negative* deviations from normal system performance like errors, failures and faults, but also to *recoveries*, the "positive deviations";
- it should focus not only on technical components and human behaviour as contributing factors to a near miss, but certainly also to organisational and managerial causes.

4.1.3. Model-based design

Following the previous point, the ideal should be a complete socio-technical system model of the organisation involved forming the heart of the NMMS. Since such a model will not be readily available, the next best option is to select a suitable model describing *individual* behaviour in a complex technical environment, as the "information processing part" of the NMMS. This model then determines not only the required input data (taken from the near miss report) but also the methods of analysing and interpreting its results in terms

of suggestions of specific measures to be taken by management (see Chapter 5).

4.1.4. Relationship with other organisational tools

The NMMS must be able to benefit from and contribute to other existing tools for measuring or understanding an organisation's performance, e.g. other safety-related information systems, audits, Total Quality Programmes, etc. This also means that the level of acceptance of a NMMS should, in itself, be considered as an important measure of an organisation's performance or "safety culture" (see Chapter 6).

4.2. BASIC NMMS FRAMEWORK

Figure 4.1 shows the proposed basic framework, consisting of seven modules which together should form the "building blocks" for different types of NMMS's.

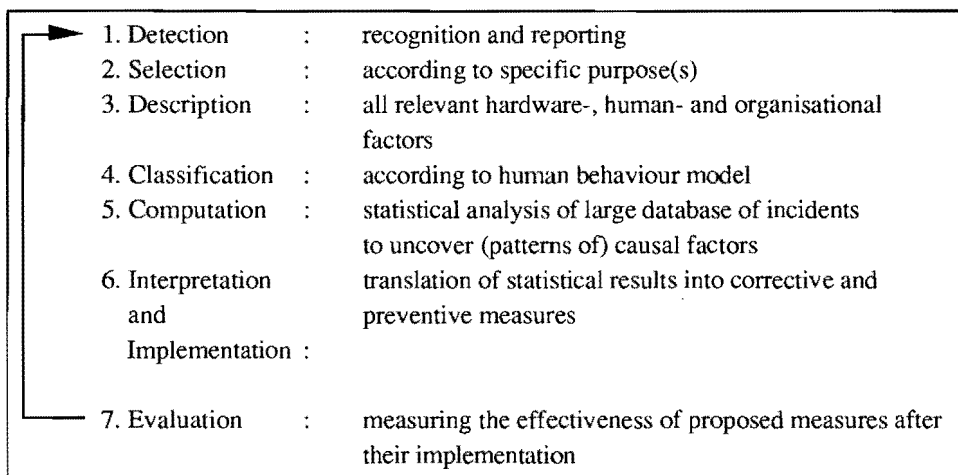


Figure 4.1: The seven modules of the basic NMMS design framework.

To explain the seven modules and their framework we will first describe the "information processing sequence" of near miss reports and subsequently the

order in which these modules should be specified when designing a NMMS for a particular situation. Furthermore, specific questions to be dealt with for each of those steps are listed in appendix 4 and in section 7.1.3.

4.2.1. Processing sequence of near miss reports in the NMMS

- Step 1.* The Detection module contains the *registration* mechanism, aiming at a complete, valid reporting of all near miss situations detectable by employees.
- Step 2.* A NMMS that works well will probably generate a lot of "deja vu" reactions on the part of the safety staff coping with a sizable pile of these reports. To maximise the learning effect and for practical reasons some sort of selection procedure is necessary to *filter out the most interesting reports for further analysis* in the subsequent modules. First of all, management objectives may of course lead to certain selection rules (e.g. special interest in personal injuries, or in product quality). Even more important however would be the presence of unique elements or unexpected combinations of elements, visible already by looking at the "raw" reports. Such reports would have to be ensured of the extra time and effort needed by the safety staff to apply all modules in these cases.
- Step 3.* Any report selected for further processing must lead to a *detailed, complete, neutral description* of the sequences of events leading to the reported near miss situation. For instance, an analysis based on Fault Tree techniques (e.g. Hoyos and Zimolong, 1988) will help the investigator to describe all relevant system elements (technical failures, management decisions, operator errors, operator recoveries, etc.) in a tree-like structure. This description will show all causal elements in their *logical order* and in their *chronological sequence* (see appendix 2 for an example).
- Step 4.* Every element in such a tree will be classified according to the chosen human behaviour model, or at least every "root cause" (the end points of the tree) will be. In this way the fact that any incident usually has *multiple causes* is fully recognised. Each near miss report is analysed to *produce a set of classifications* of causal elements instead of the

usual procedure of selecting only one of these elements as "the main cause".

- Step 5.* Each near miss tree as such generates a set of classifications of elements which have to be put into a *data-base* for further *statistical analysis*. This means that a NMMS is *not* meant to generate ad-hoc reactions by management after each and every serious near miss report; on the contrary, a steady build-up of such a database until statistically *reliable patterns* of results emerge must be allowed in order to identify *structural factors* in the organisation and plant instead of just unique, nonrecurring aspects.
- Step 6.* Having identified such structural factors (the *real* root causes), the model must allow interpretation of these, i.e. it must *suggest ways of influencing these factors*, to eliminate or diminish error factors and to promote or introduce recovery opportunities in the human-machine systems and indeed in the organisation as a whole.
- Step 7.* These suggestions to management will of course in practice be judged with regard to other dimensions (e.g. time, cost) as well, but if they are accepted by management and actually *implemented* in the organisation they will have to be *evaluated* for their actual as opposed to their predicted results, i.e. for their *effectiveness in influencing the structural factors* they were aimed at. This may be done by the NMMS itself (see the feedback loop depicted in the seven-module framework). In the period following the introduction of the measures, near miss reports should show a different frequency of occurrence for these factors. If a plant has one or more safety-performance measuring systems apart from the NMMS (like auditing-based systems), then some effect will probably be detectable by these independent indicators of safety also, depending on the degree of "overlap of content" between such separate systems and the NMMS.

4.2.2. Sequence of designing the NMMS modules

As mentioned already in section 4.1.3., the model of (human/organisational) behaviour which is chosen, becomes the heart of the NMMS; it directly defines the Classification-Computation-Interpretation group of modules which form

the "information processing section". This section in turn can handle certain types of input data, at specific levels of descriptive detail, and therefore defines the first three modules (Detection-Selection-Description). The information processing modules 4, 5 and 6 also determine the ways in which the accuracy of their predictions, i.e. the actual effects of the proposed measures, may be evaluated (module 7).

4.3. IMPLICATIONS OF DIFFERENT PURPOSES FOR NMMS DESIGN

In Chapter 3 three different purposes of near miss reporting have been mentioned: modelling (qualitative insight), monitoring (quantitative insight), and maintaining alertness. The reader will probably have noticed aspects of all three purposes in the description of the NMMS framework modules given in the previous section. In this section we will try to disentangle this inevitable but confusing listing of all seven modules in a "general" framework by indicating the subsets from these seven modules which are implied by focussing on *one* purpose at a time.

4.3.1 When the purpose is *modelling* we are only interested in reports of "new" near misses, selected from *as complete a detection phase as possible*, and subsequently *described in great detail; classification and interpretation should be flexible* enough to permit looking for "new" causal factors, which must be handled by new or existing measures.

4.3.2 Such new qualitative insights may then be formalised in the *monitoring* version of NMMS. This implies looking for *known causes of near misses only*, which are routinely classified without any real selection or detailed description at all, and fed into an already existing database to *detect any statistically significant trends* in terms of improvements in error prevention or recovery promotion. The key issue here is to monitor *whether the existing safety management* measures are able to control the *known* hazards in the system.

4.3.3 The third purpose *alertness* is of a different nature than the preceding two because it describes not so much a safety management *tool* but rather a general condition or attitude which applies to *all* levels of personnel; the awareness that, in spite of all procedures, hardware precautions and training,

the work environment still remains "dangerous" to a degree that it is sensible to follow existing safety rules even though "nothing" may have happened in a long time. The act of recognising and reporting near misses itself becomes an important *reminder* and reward to act safely; also the selection of specific examples of old, well known but still recurring problems and new, "impossible" combinations of factors, described in detail in the familiar setting of one's own workplace, should provide convincing illustrations of the fact that an absence of overt accidents is not to be equated with a perfect hazard control system. Instead, possibly serious effects of seemingly minor deviations must be stressed, as should the factors and measures which have acted as effective recoveries.

Purpose of near miss reporting

	Modelling	Monitoring	Alertness
1. Detection	everything	known problems only	recognising and reporting
2. Selection	new reports only	[not relevant]	convincing, detailed examples of new and old hazards
3. Description	detailed	[not relevant] or very superficial	
4. Classification	flexible: looking for new root causes	routine: standard set of root causes	[not relevant]
5. Computation	[not relevant]: only single events considered	periodic analysis of updated large data-base	[not relevant]
6. Interpretation and Implementation	finding (new) ways of improving prevention and recovery	[not relevant] already prescribed by module 4	near misses as precursors; focus on recovery mechanisms
7. Evaluation	[not relevant]	comparing actual and predicted effects of implemented measures	[not relevant]

Figure 4.2: An overview of different versions of the basic NMMS framework (see Figure 4.1), depending on the type of purpose.

For the sake of clarity the points raised above are summarised in figure 4.2, indicating which modules are or are not implied (in a very global way) by the three purposes mentioned.

In practice however the usual case will be that of a *combination* of two or three purposes existing at the same time. This makes the distinctions in figure 4.2 more illustrative of the use(s) of the modules themselves than as guidance for a realistic NMMS design task.

4.4. EXTENDED NMMS FRAMEWORK

The basic version of the NMMS framework described above shows its functioning at the *level of the safety department* in an organisation. The learning process thus takes place at the level of "end-users" (e.g. operators, etc.), their direct supervisors and the local safety staff. *Feedback loops* which make this learning process possible are not only the "evaluation" loop back to module 1, but also several smaller loops within the framework, e.g. when the purpose is modelling, module 6 may very well influence module 4, which in turn may change the ways in which the "input" modules 1, 2 and 3 operate.

At higher organisational levels however important extra feedback loops are necessary, leading to an *extended version* of the framework. For instance, detection of "impossible" events or classification of "new" root causes may lead to direct inputs to the *engineering department* for hardware solutions, including ergonomic improvements of the human-machine interface. *Operations management* may also have to react to such inputs by changing the work situation, e.g. staff levels, task allocation, communication channels, etc.. Finally, at the *senior management level*, sometimes far-reaching re-evaluations of the balance between production, safety and environmental priorities will have to be made. Also major changes relating to NMMS's own performance and its mixture of purposes will by definition mean that "outside" loops will be needed for such decisions. This last point is modelled by Hale c.s. (Hale, 1985; Oortman Gerlings & Hale, 1991) by considering safety management as the detection and solution of problems within a system. This process proceeds at two levels:

- the detection of problems new to the system so that preventive design changes can be made and a safety management system can be set up to keep the remaining risks under control.
 - the detection and correction of failures in the safety management system, where known hazards are not successfully being kept under control.
- The steps in the problem solving cycle for the two levels of activity are similar; see figure 4.3 for a generic description.

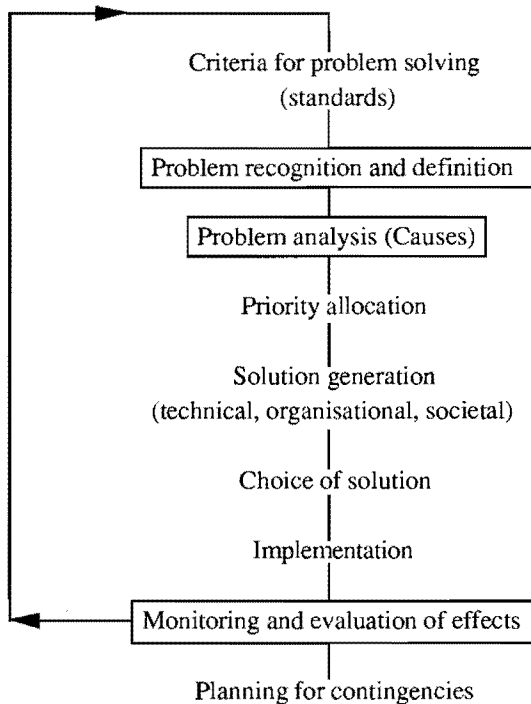


Figure 4.3: Safety management as problem solving.

Using this model the contribution of information systems based on near misses and related incidents can be located at three points in the cycle (see also Chapter 3):

- problem analysis leading to priority allocation and the generation of appropriate solutions. How can the system go wrong in ways which are not yet known? This use is aimed at *system modelling*.

- *monitoring* of the effectiveness of the current safety management system. Which existing prevention measures are not working as well as planned?
- problem recognition, the proof that a new system is vulnerable or that an old one is still vulnerable despite current attempts to make it safe and hence that vigilance in the management of safety should not be relaxed. We call this use "*alertness*" because it serves to activate people in the organisation to be and remain alert.

In short, it will be of paramount importance to ensure an optimal organisational in-bedding of the incident reporting system. This means that the basic seven-step framework needs to be placed in a broader framework defining the *life cycle* of such an information system (Figure 4.4.).

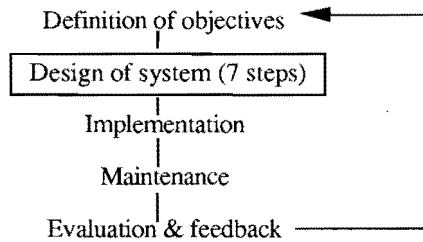


Figure 4.4: The life cycle of the NMMS.

4.5. POSSIBLE USES OF THE FRAMEWORK

Summarising the main points of this chapter we can distinguish the following ways in which the NMMS framework may be used:

- the simplest form is to use it as a *checklist for describing* the status of incident reporting systems. In this way a complete inventory of such a system is made by simply "following" an incident report being handled by the existing information processing sequence in a chronological order. An example is given in Chapter 7, where it was used as such during a number of plant visits in the course of the survey of near miss reporting in the Netherlands.
- secondly, we may regard the framework as a *normative model* for (re-) designing such systems. Having described an existing system in the way mentioned above, immediately "missing" modules and reversals in the

sequence of modules may be noted by comparing the described system with the normative framework. Of course, it may also serve as a guideline for designing a completely new reporting system, in the order described in section 4.2.2., as will be done in Chapter 8.

- finally, by taking its use as a descriptive checklist as a starting point, it may become a framework for *designing the organisational in-bedding of the NMMS*: system documentation, training programmes and decision support for learning how to use it, and the explicit design of the feedback loops in- and outside the NMMS itself (see section 4.4) may also be guided by it.

Classification model of process supervision and control errors

Introduction

In Chapter 2 it was argued that human behaviour is amongst the most dominant factors causing system failures in chemical process control. In this chapter we will present a detailed classification system of operator errors derived from the Rasmussen SRK model discussed in Chapter 2. First the “human error” part will be operationalised, taking the process control operator task as the focal point. Then the other main categories of system failure, Technical and Organisational Failure, will be added in order to arrive at a complete model of system failure. An explicit link between classification results and proposed actions will then be presented in the form of a preliminary Classification/Action Matrix. In this way the combination of model + matrix may become an actual safety management tool (see appendix 2 for a completely worked-out example). The chapter is concluded by summarising the main strong and weak points of the proposed model and the matrix.

5.1. CLASSIFICATION OF HUMAN ERRORS IN PROCESS SUPERVISION AND CONTROL

As was discussed in Chapter 2 Rasmussen has provided the basic model of human error based on three levels of behaviour: skill-, rule- and knowledge-based (S-B, R-B, K-B). This SRK model has been operationalised to describe operator errors in process control tasks by combining it with *characteristic task elements*, which as a whole cover the entire spectrum of operator subtasks.

On the basis of our own informal observations and discussions in process control rooms, e.g. Van der Schaaf (1989), and the “classical” literature on operator tasks (Crossman, 1974) the following *set of elementary operator requirements* in order to carry out process control tasks correctly, has been identified:

- a) firstly, the correct *status* and dynamics of the system to be controlled must be known to the operator;
- b) also, the (main) *goal*, or priorities of goals, must be known and understood by the operator;
- c) the operator in question must be *qualified* (on the basis of training) to do the job, and
- d) if applicable, he must obtain a *temporary permit* for activities where extra risk is involved;
- e) the preparation of the job itself starts by informing other operators, if necessary, of the work to be done (*coordination*), in view of the potential effects on *their* tasks;
- f) when arriving at the job location the local system status should be *checked* to comply with the expected conditions in as far as these would be relevant for the job;
- g) the job itself should be *planned* correctly, i.e. the correct methods should be chosen and carried out in the correct order;
- h) the prescribed tools and information sources for a proper job performance should be present and used;
- i) the execution of the required actions themselves implies successful correct movements; both *controlled*, i.e. intended, detailed, movements (e.g. to manipulate tools and request information), and maintaining the correct *body* position in order to make the controlled movements possible.

According to our interpretation of the SRK-model, *a* and *b* rely mainly on K-B behaviour; *c*, *d*, *e*, *f* and *g* all involve decisions to carry out the job in a certain way (i.e. according to the rules and procedures) and rely therefore on R-B behaviour; finally, the actual execution aspects *h* and *i* rely on S-B behaviour.

Figure 5.1. presents the classification codes, the labels of error

categories and a typical example of each. These classification codes for Human operator behaviour (*H*) first distinguish between K-B, R-B and S-B behaviour (*K*, *R* and *S* respectively); at the most detailed level of classification these combined codes are further subdivided in the order of the elementary operator requirements mentioned above; the first subcategory of K-B error (“system status”) is coded as HK1; the second type of K-B error (“goal”) as HK2, etc.

	<u>error code</u>	<u>descriptive label</u>	<u>example</u>
K-B {	HK1	system status	- not realising that part of the plant is inoperative because of maintenance
	HK2	goal	- aiming at "overspec" production instead of at "right-on-spec"
	HR1	license (permanent)	- not qualified for a certain task
R-B {	HR2	permit (temporary)	- no permit obtained, although required
	HR3	coordination	- not informing control-room operator of one's actions outside in the plant
	HR4	checks	- not ensuring that system status is as expected
	HR5	planning	- choosing wrong method for correct goal
	HR6	equipment/information	- using wrong tools/process data
S-B {	HS1	controlled movement	- making typing error on keyboard
	HS2	whole-body movement	- slipping, tripping, falling

Figure 5.1: Subcategories of operator errors, with labels and brief examples.

The practical experiences in process control rooms mentioned earlier clearly point at *biases* in describing and classifying incidents; the pilot studies mentioned in Chapter 2, the survey to be presented in Chapter 7, and also the Exxon case in Chapter 8 all show a tendency on the part of safety officers to concentrate on clearly visible S-B elements of task performance (e.g. pressing the wrong button) rather than on less obvious R-B errors (e.g. planning), let alone on the mainly cognitive, internal “activities” involved in K-B behaviour.

Therefore, in using the classification, the following *fixed order* is proposed (as indicated from top to bottom in figure 5.1.) to arrive at the best-fitting error category for causal factors of accidents and near misses: first K-B errors, then R-B and finally S-B errors. In this way *the above mentioned*

bias might be counteracted.

5.2. EXTENSION TO CLASSIFICATION OF SYSTEM FAILURE

Human (operator) Error cannot be separated entirely from the Technical and Organisational context of task performance (see figure 2.1). At the very least one should know the importance of Human Behaviour relative to that of the Technical and Organisational factors in understanding the causes of accidents and near misses. On the basis of our own pilot CCR studies (Van der Schaaf, 1989) the following extensions are suggested:

The main category "Technical Factors" is subdivided into

- Engineering (TE)*: wrong design.
- Construction (TC)*: correct design which was not followed accurately during the construction phase.
- Materials (TM)*: rest category, for those material defects not classifiable under TE or TC.

The main category of Organisational Factors is subdivided into:

- Operating Procedures (OP)*: refers to the (inadequate) *quality* of procedures (completeness, accuracy, ergonomically correct presentation), not whether they are followed or not!
- Management Priorities (OM)*: refers to any *de facto* pressure by top- or middle management to let production prevail over safety.

Again, just as in the previous paragraph, a *fixed order of analysis* is advocated: firstly, one has to make absolutely certain that the technical design etc. of one's work environment is fully adequate; only after the technical design has been established as adequate, one may question whether the organisational context was a causal factor. Finally, when the Technical and Organisational aspects are found to be in perfect order, we should focus on human behaviour as a possible failure factor. In this way we hope to counteract the sometimes strong *bias* within a company's culture (see also Chapter 6) to start and stop the analysis at the level of the end-user and leave the technical and organisational context of any mishap unquestioned.

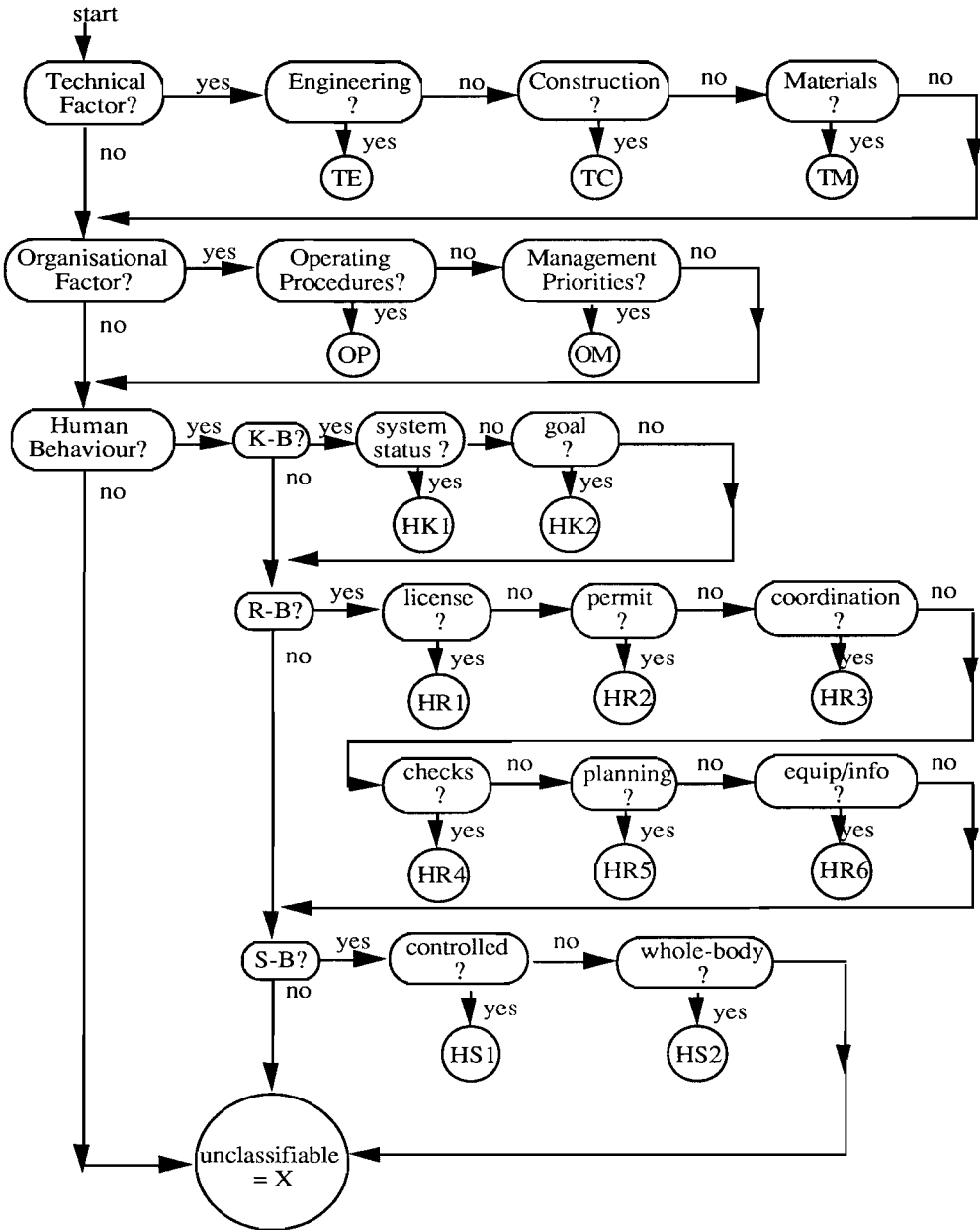


Figure 5.2: The complete Eindhoven classification model of system failure.

Apart from the biases in describing the causes of incidents mentioned above, other *problems in using this* (as in any!) *classification scheme* could be in the *definitions and their associated examples* of the (sub-)categories. These are discussed in Chapter 8, showing how e.g. the examples were constructed to ensure their validity, and what the results were of a preliminary test of their use within Exxon.

5.3. EINDHOVEN CLASSIFICATION MODEL OF SYSTEM FAILURE

Integrating all the above, we arrive at the complete “Eindhoven Classification Model of System Failure in Process Control tasks” (see figure 5.2).

The classification model as shown in figure 5.2. may also be used as a *checklist* to assist in the stage where *all relevant causal factors* should be collected for the investigation of a specific incident. In this respect is not unlike *generic Fault Trees*, like the one used in the MORT system (Johnson, 1980), which enable investigators not only to present their analysis results in a highly visible way, but also ensure that a multitude of non-technical factors (“specific job oversights and omissions”, “management system factors”) are carefully checked for their relevance.

5.4. PRELIMINARY CLASSIFICATION/ACTION MATRIX

In order to develop an actual tool for safety management it does not suffice to stop at the analysis stage of failure classification mentioned above. These classification results have to be translated into proposals for *effective preventive and corrective action* (see module 6 of the NMMS framework in Chapter 4). To fulfil this purpose a so-called Preliminary Classification/Action Matrix is proposed below (see figure 5.3.).

Its rows consist of the final classification codes as defined in figure 5.2., while its columns represent the following *five classes of actions* (based on studies at Exxon, e.g. Van der Schaaf, 1991b) available to management:

- *Equipment*: redesigning of hardware, software or interface parts of the man-machine system;
- *Procedures*: completing or improving formal and informal procedures

- *Information & Communication* for efficient *and* safe task performance; completing or improving available sources of information and of communication structures;
- *Training* improving (re)training programmes for skills needed;
- *Motivation* increasing the level of voluntary obedience to generally accepted rules by applying principles of positive behaviour modification.

	Equipment	Procedures	Information & Communication	Training	Motivation
TE	(x)				
TC	(x)				
(TM)					
OP		(x)			
(OM)					
HK1			(x)		no!
HK2			(x)		no!
HR1				(x)	
HR2				(x)	
HR3				(x)	
HR4				(x)	
HR5				(x)	
HR6				(x)	
HS1	(x)				no!
HS2	(x)				no!

Figure 5.3: Classification/Action Matrix belonging to figure 5.2.

In the matrix the most preferred action in terms of expected effectiveness for each classification category is indicated by x . The last column’s “no!’s” refer to particularly ineffective management actions, which are none the less often encountered in practice.

The entries in figure 5.3 were determined as follows:

- Technical Failures (TE, TC) point at technical improvements of the *equipment*; also S-B errors, because of their “automatic” nature, can best be prevented by changing the work environment, not by changing the person.
- Inadequate procedures (OP) imply improvements in the area of *procedures*.
- K-B errors (HK1, HK2) should be prevented by investing in operators’ background *knowledge* of process control, and in optimising the available *information sources* relating to the present, past, and future states of the process (i.e. by means of optimising interfaces and communication).
- R-B errors point at faulty decisions how to perform a certain task, given the correct knowledge of status and goal; therefore, *training* in making these choices fit better with the situation should help.
- TM and OM do not lead to specific recommendations of preventive measures; TM occurrences are, like “acts of God”, not-foreseen failures; *recurring TM problems* of course imply management failure (e.g. in checking product quality of incoming goods); OM failure relates to the local managers themselves, and therefore requires *moving to higher levels of management* to solve this (e.g. by improving company policies), than is feasible for the line-managers who are supposed to be supported by this matrix. Given the label “preliminary”, it will be clear that the details of the matrix are still very much open for discussion, and that it should be tested extensively in practice (see also section 5.5 below).

5.5. CONCLUSIONS

The main strong and weak points of the model (in figure 5.2.) and matrix (in figure 5.3.) can be summarised as follows:

- *Strong points*: – the *comprehensiveness* of the model; it deals with all relevant failure factors (Technical, Organisational, and Behavioural), and it also deals with all levels of behaviour, not only R-B, but also K-B and S-B.
 - it is fully *operationalised* in terms of recognisable task elements, and it has explicit links with the resulting *management actions*. As such it is not only a real tool for safety management, but it also offers the possibility of

validating the SRK model's implications in practice.

- *Weak points:* – the classification has not yet been adequately tested. The experiences during the pilots mentioned in Chapter 2 (using earlier versions of the classification) were positive in the sense that safety staff, managers, and operators thought the categories and the classification process were quite understandable and had a high face validity; it may be added that both student-researchers performing these pilots succeeded in classifying at least 90% to 95% of all investigated reports.
- a theoretical judgment of the operationalisations in the classification model and the matrix will always be hampered by the general vagueness of the SRK model as described by Rasmussen (see Bainbridge, 1984).

In the discussion in Chapter 8 of the most extensive application of the model so far we will return to these issues in the light of the results obtained there.

Practical aspects in implementation

In the previous chapters already on several occasions organisational aspects of NMMS *implementation* have been discussed: top-level commitment; misuse of the NMMS results; support (e.g. in the form of examples and decision trees) both for reporting employees, safety staff and line management; and the organisational inbedding of a NMMS.

In this chapter we will rephrase, summarise and extend the set of practical aspects related to designing and implementing near miss reporting systems. First five general factors will be listed, followed by a more detailed discussion of two of these: data collection, and acceptability. Also the overall important factor of training will be briefly outlined. Finally the relationship between an organisation's prevailing view of human error and its safety culture will be discussed.

6.1. PRACTICAL ASPECTS IN DESIGNING AND IMPLEMENTATION

Lucas (1987) identifies 5 factors for voluntary or mandatory near miss reporting:

1. *The nature of the information collected*: is it just descriptive reports or also causal? Is it just free text, or does it include also answers to a standard set of questions?
2. *The use of information in the database*: is there regular and appropriate feedback to all levels of personnel? Is it easy to generate summary statistics *and* clear examples from the database? Does the database generate specific error reduction strategies to be proposed to management?
3. *The level of help provided to collect and analyse the data*: are there analyst aids in the form of interview questions, flow charts, software, etc.?

4. *The nature of organisation of the reporting system*: is it local (e.g. plant-based) or central (e.g. company-based)? Is reporting voluntary or mandatory?
5. *Whether the scheme is acceptable to all personnel*: is there a feeling of “shared ownership”, or of “Big Brother is watching you”? Is the data gathered by a well known colleague or by an unknown outsider? Is everyone familiar with the purpose and backgrounds of the reporting scheme?

6.2. PROBLEMS OF DATA COLLECTION

Looking at the first point mentioned in section 6.1 in more detail, the following problems of existing data collection systems can be found (Lucas, 1987):

- *Action oriented*: tendency to focus on *what* rather than *why*.
- *Event focussed*: analysing individual accidents rather than looking for general patterns of causes in a large database; this leads to anecdotal reporting systems.
- *Consequence driven*: the amount of attention and investigation resources are directly proportional to the severity of the outcome.
- *Technical myopia*: bias towards hardware- rather than human failures.
- *Variable in quality*: both within and between reporting systems, leading to incomparable investigation methods and results.

The first three of the above problems are particularly relevant for near miss reporting, because it requires “why” information to backtrack the root causes; any selection bias in terms of actual consequences must be changed into one in terms of *potential* consequences; and finally safety management must switch from ad hoc analysis of anecdotes to structural analysis of patterns of causes.

6.3. ACCEPTANCE BY ALL EMPLOYEES

The last point in section 6.1 is actually the result of all points mentioned earlier. Three important ways that management can promote this acceptance are: anonymity, forgiveness and feedback (Lucas, 1992).

In some situations *anonymity* of those reporting is an absolute must, although the price is high: follow-up research is almost impossible.

In *all* situations where near misses are to be reported, *forgiveness* or “no blame” policies are essential (Ives, 1991).

In a more general sense, *feedback* is necessary to maintain a reporting system one it has started running well.

Two examples my illustrate these points; the first one demonstrates the importance of *confidentiality* in some situations:

CHIRP (Confidential Human Factors Incident Reporting Programme) is a clear example of a successful voluntary near miss reporting system, run by the UK's RAF's Institute of Aviation Medicine. Each year about 200 pilots and air traffic controllers report to CHIRP, not anonymously but in complete confidence, about mistakes they have made in the air and why they believe they made them (Greene, 1990).

“A good example of this process is provided by the fatigue reports submitted to CHIRP. A number of these reports are of incidents in which complete airline crews found themselves asleep while, for example, crossing the Atlantic. Although flying mythology acknowledged such incidents, it has required the CHIRP system to force the problem of the sleeping crew to be confronted and tackled.” (Greene, 1990).

The second example gives a tragic example from the Report of the Presidential Commission on the Space Shuttle Challenger Accident (1986) of the cost of *not* having (or rather: killing off by no longer following a “no blame” policy) a proper NMMS.

“Accidental Damage Reporting. While not specifically related to the Challenger accident, a serious problem was identified during interview of technicians who work on the Orbiter. It had been their understanding at one time that employees would not be disciplined for accidental damage done to the Orbiter, provided the damage was fully reported when it occurred. It was their opinion that this forgiveness policy was no longer being followed by the

Shuttle Processing Contractor. They cited examples of employees being punished after acknowledging they had accidentally caused damage. The technicians said that accidental damage is not consistently reported, when it occurs, because of lack of confidence in management's forgiveness policy and technicians' consequent fear of losing their jobs. This situation has obvious severe implications if left uncorrected."

6.4. TRAINING RELATED TO NEAR MISS REPORTING

It is often vital to set up specific NMMS training programmes: for *managers*, to accept that near miss reporting is strictly for *learning* about the safety control system; for *operators*, to recognise near miss situations and report fully; for *safety coordinators*, to describe and analyse the reported cases, looking for root causes, and to give feedback to all levels of personnel. Software tools may be helpful, but they are no guarantee of success (Hale et al., 1991). Examples of such training programmes will be given in Chapters 7 and 8.

6.5. SAFETY CULTURES

The status of a certain organisation on all of the above points in this chapter may be summarised by speaking of its *safety culture*. Lucas (1992) distinguishes three major types of organisational safety culture:

- *Occupational safety management*: concentrates on the safety of individual workers by promoting their "safety-mindedness"; the prevailing view of human error is that of the *traditional safety model* where safety control is handled by motivation, and punishment (for lack of attention).
- *Risk management*: focuses on system safety by analysing and quantifying hazards and risks; the prevailing human error view is that of *man-machine mismatch*, with solutions to safety problems in form of design changes (e.g. ergonomics) and job aids (e.g. procedures).
- *Systemic safety management*: especially prominent after a major organisational disaster, which forces the organisation to take a fundamental look at its entire safety philosophy; the appropriate view of human error is the *system-induced error concept*, which says that many human errors can be

traced back to faulty management decisions and organisational policies (Reason, 1990): human error problems will typically be solved by organisational changes.

Lucas (1992) proposes that different safety cultures will have an impact on which accidents are investigated and whether or not near miss reporting is perceived as a valuable use of resources; an occupational safety culture would probably investigate only serious personal injuries; the risk management culture might be interested in certain types of near misses with very direct and serious potential safety consequences; finally a systemic safety culture will encourage its employees to report anything related to possible deviations, either with immediate or delayed consequences for safety control.

Westrum (1988) has put forward another classification of organisations on the basis of their safety philosophies, or rather according to their typical responses to safety related incidents; he distinguishes “pathological”, “calculative”, and “generative” organisations. Lucas (1992) characterises these as follows:

The *pathological* organisation will tend to deny or suppress information on hazards and may actively circumvent safety regulations. On the other hand, *calculative* organisations use “by the book” methods but have few contingencies for unforeseen events or exceptions on the rules. The *generative* organisation accepts that a problem may be global in character and appropriate action is taken to reconsider and reform the operational system. It could well be argued that the pathological and calculative organisations will hold a traditional safety view of error causation. Calculative organisations may also accept the man-machine interface view of error. By their nature the generative organisation must hold a system-induced concept of human error.

Figure 6.1 summarises the relationship between Lucas’ (1992) types of organisational safety culture and their predominant model of human error on one hand, and Westrum’s (1988) tripartite division of organisations on the other.

The conclusion here must be that only an organisation characterized by the bottom row of Figure 6.1 would have a high probability of successfully imple-

menting a NMMS. Therefore, an organisation's "safety culture" should be one of the first aspects to be taken into account when considering the introduction of near miss reporting. Although Figure 6.1 gives some support to guide the decision whether or not to start a NMMS project, much more work in this area is clearly urgently needed.

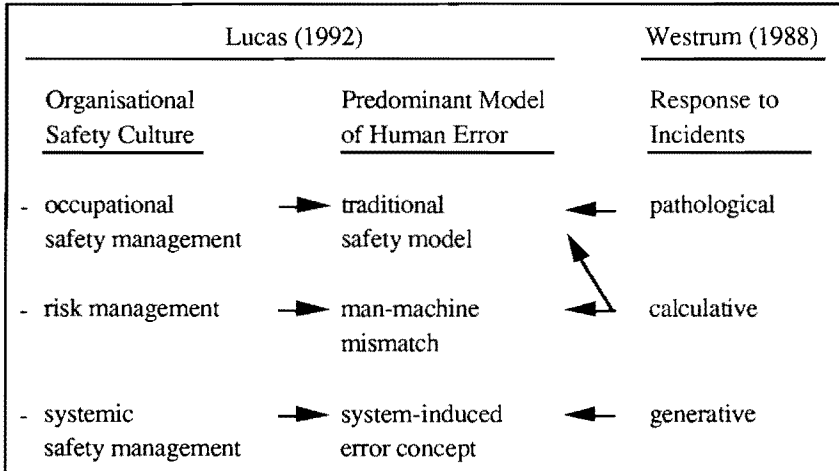


Figure 6.1: Safety culture, human error model, and response to incidents; based on Lucas (1992) and Westrum (1988).

European and national experiences with near miss management systems

Introduction

In the previous chapters the purposes of near miss reporting have been outlined and a framework of designing such a safety management tool has been presented. The importance of human behaviour as a dominant factor in incident sequences was stressed by developing a system failure classification scheme largely based on a theoretical model of operator behaviour. Also an overview was given of the organisational factors necessary for a successful implementation of a NMMS.

In this chapter the aim is to get a better insight in the *actual state-of-the-art in process industry* (and some other industrial sectors, for purposes of comparison). At the same time it will serve as a (face-) validity check of the ideas on the design and implementation of NMMS's.

Firstly the most important aspects will be discussed of an international three-day workshop on the topic of near miss reporting, held in Eindhoven in September 1989, followed by a more recent survey of NMMS's in the Netherlands.

7.1. CEC WORKSHOP ON NEAR MISS REPORTING AND ANALYSIS

7.1.1. Background

In starting-up a contract research project on near miss reporting for a chemical process plant in Rotterdam (see Chapter 8) it very soon became clear that hardly anything had been reported in the open literature on this subject.

At the same time, however, it was our firm impression that more and more industrial organisations were (informally) expressing the need for a (scientifically based) method to register and analyse near misses. Therefore some knowledge, experience and theoretical work in this area probably was present within and scattered over consultancy firms, universities and safety staff of companies, but it seemed that everyone was keeping the "dirty laundry" inside.

This led to an application to the Commission of the European Communities (CEC) Research Programme on Medical and Public Health to receive funding for a three-day informal Discussion Meeting through its Concerted Action "Breakdown in Human Adaptation (no 2: Performance Decrement)".

This proposal (Van der Schaaf, 1988a) was sent to the CEC in October 1988 and approved by December that same year. The actual workshop was held at Eindhoven University of Technology from 6-8 September, 1989, with as co-organisers Human Reliability Associates Ltd., a consultancy firm from the U.K., and the TNO-Institute for Perception in the Netherlands.

The meeting brought together a total of 12 researchers, consultants, and company staff from the Netherlands, U.K., Belgium, Switzerland and Canada. All the participants shared a common interest in near miss and accident reporting. A full list of participants is provided in appendix 3.

7.1.2. Objectives

The major objectives of this CEC-sponsored meeting were (Van der Schaaf and Lucas, 1989):

- To exchange experiences on the use of cognitive models for accident and near miss reporting;
- To enumerate the practical problems and limitations of such reporting as experienced by the participants;
- To discuss new theoretical directions related to such reporting;
- To devise an agenda of future research needs;
- To disseminate information presented and discussed at the meeting to a wider audience through the publication of edited proceedings.

7.1.3. Case studies

Case studies from a variety of accident and near miss reporting systems were presented from the industrial sectors of transportation and the process industries:

- road traffic conflicts at intersections (Brown & Van der Horst);
- signals passed at danger on the railways (Taylor & Lucas);
- air miss reporting in aviation (Cannell);
- occupational injuries (Hale);
- nuclear power plant near miss and human performance monitoring (Ives & Embrey);
- near misses and recoveries in the chemical industry (Van der Schaaf).

The case studies gave exceptionally clear insights into the problems of setting up and maintaining any such reporting system. The need emerged to consider the organisational context in which these systems are implemented. Problems here included:

- the need to have top-level management commitment (Ives);
- importance of “pride of ownership” of such a system (Lucas, Embrey);
- avoidance of the use of reporting systems as a measure of “performance” of an organisation (Ives);
- provision of appropriate feedback to all levels of personnel (Embrey);
- need to move away from a traditional view of incident causation which assigns blame to individuals (Cannell, Lucas);
- need to counter “ritualisation” (= tendency to report the same patterns of causes again and again) (Cannell);
- awareness of impact on union issues (Hale);
- avoidance on annihilating the “learning effect” of voluntary near miss reporting with sanctions against the authors of such reports (Van der Schaaf).

The case studies also illustrated problems in near miss management systems with reference to the proposed framework (see Chapter 4):

- Detection: – reliability of data gathered by observers (Brown & Van der Horst)
- Description: – need to look at organisational roots of primary causes of

- near misses (Cannell, Ives)
- proliferation of registered data due to lack of underlying model (Hale, Lucas, Embrey)
- Classification: –existence of descriptive, not explanatory “catch all” categories (Cannell, Taylor, Lucas)
- Evaluation: –mapping of “acceptable solutions” onto causes in a complex multi-causal situation (Cannell).

7.1.4. Conclusions and follow-up

It was concluded that the Discussion Meeting had indeed started an “European platform” for exchanging experiences and ideas with reference to near miss reporting. The combination of transportation and the process industry, and of practitioners and researchers was highly valued.

The proceedings were published in the form of a book in November 1991 (Van der Schaaf, Lucas and Hale, 1991).

7.2. A SURVEY OF NEAR MISS REPORTING IN THE NETHERLANDS

7.2.1. Introduction

As was mentioned in the preceding paragraph, during the CEC workshop case studies on near miss reporting from all over Western Europe and Canada were presented to reveal the state-of-the-art in this matter. Two of these (Hale et al., 1991; Van der Schaaf, 1991) concerned chemical process plants in the Netherlands. After the CEC workshop it was decided to extend this set of two with at least another dozen brief “case studies”, in order to get a better insight into the NMMS situation in this country in particular.

The main goals of this survey were the following:

1. to describe the state-of-the-art in near miss reporting amongst those process plants thought to be among the *most advanced* in terms of safety management, plus a few supposedly less advanced process plants for comparison;
2. to compare the situation in the industrial processing sector with that of *other sectors*, like discrete manufacturing, construction, and services;

3. to compare the results from 1. and 2. with those from the CEC workshop;
4. to have an informal check regarding the face validity of the NMMS framework as presented in Chapter 4, of the usefulness of a human behaviour model as one of its basic elements, and of the organisational "success factors" for implementation listed in Chapter 6.

7.2.2. Method

Three different sets of data (A, B and C) were gathered to fulfil the goals mentioned in section 7.2.1: Seven "old" case studies in process plants; seven new cases in process industry; and finally seven new cases in other industrial sectors. The results and conclusions are therefore based on a *total of 21 cases*, without any overlap with those presented in either section 7.1 or in Chapter 8.

It is also good to realise that this set of 21 cases is *not representative* of the industrial processing sector in the Netherlands, and certainly not of Dutch companies in general; in this survey we were not interested in the general picture, but mainly in the experiences and views amongst those locations or companies carrying a high general reputation in safety management.

- . *Set A*: the *seven old cases* all concerned local sites with which we had had extensive direct contacts in the period of 1985-1990, either in the form of contract research projects or by supervising students working in those plants. The insights in their safety management systems in general and in their NMMS projects in particular were updated in 1991.
- . *Set B*: *seven new process plant cases* were added between 1990 and 1992, usually as a result of reactions of the part of the process plants to presentations of the results of the CEC workshop. Almost all of these local sites carried a high general reputation in safety management.
- . *Set C*: between 1990 and early 1992 a total of seven central safety departments of very large companies *not belonging to the process industry* cooperated in this survey in reaction to the CEC workshop results: three in discrete manufacturing, one in industrial construction, and three belonging to the

services sector.

For sets B and C the approach followed was in each case identical, and as listed below:

- one of three half-day discussions were held with safety staff members directly responsible for accident and near miss investigation, its follow-up and annual evaluation.
- each discussant received a small *information package* several weeks before the first meeting took place, consisting of general information on the CEC workshop (Van der Schaaf, 1988a; Van der Schaaf and Lucas, 1989) and a short description of the NMMS framework, with specific questions for each of the seven steps (see appendix 4).
- it was agreed beforehand to keep *all* of the information given *anonymous*; a publicly available summary report of all case studies should contain *only overall results and conclusions* (Van der Schaaf, 1992).
- on publication of the CEC workshop proceedings (Van der Schaaf, Lucas and Hale, 1991) each discussant would receive a complementary copy.

7.2.3. Results within the descriptive NMMS framework

First it must be mentioned that *no* interpretable differences in results were found between sets A, B and C. Therefore, the most interesting *overall* results of the 21 case studies are presented below according to the most relevant step on the NMMS framework.

. *Step 1* (Detection):

- only in three cases there was a formal *exchange of reported incidents*, either to and from a central company database, or bilaterally between individual locations; however, due to the low level of standardisation in these reports, only very general information could be exchanged which therefore was not regarded as very useful, except in one case.
- only one was *training* its employees for problem recognition.
- one was using “ice-berg model” ratios (see Chapter 3) of accidents to near misses, etc., to evaluate the level of *completeness* of its reporting system results in terms of the *number* of reported near misses.

–only one was treating incidents involving *external employees* (from contractors) as if they had happened to its own staff; the same was true for *off-the-job* (i.e. outside the premises of the employer) incidents as compared to on-the-job ones.

. *Step 2 (Selection):*

–estimated *potential seriousness* in all cases was the prime parameter for selection; only in one case were there explicit criteria to guide this decision.

–only one case was separating *implicit work-orders* from actual reports of near misses, to avoid misuse of the NMMS (by attaching a “safety” label to a normal request for a job, giving it a higher priority).

. *Step 3 (Description):*

–almost all used a mere narrative version to describe the origins of the incident; only two were also using *FTA*-like or *MORT*-like graphical methods, as the Incident Production Tree (see appendix 2).

–none used an explicit *stopping-rule* to determine at which level of detail one should stop the backtracking process in the incident analysis, working backwards from the top-event to its root causes; depending on potential seriousness sometimes the amount of time and resources available were determined *before* the detailed investigation started.

. *Step 4 (Classification):*

–not a single site or company was using a *human behaviour model* to analyse “the human factor” in incidents and/or generate appropriate countermeasures; in three cases some elements of Heinrich’s (1931) model of accident causation were visible in the reporting form’s headings (to describe the incident itself and its immediate precursors).

–none would classify more than *one or two main causes* (plus one or two minor causes sometimes) even for complex incidents, with all the resulting problems of validity and reliability of their intuitive classification process.

. *Step 5 (Computation):*

–even simple descriptive *statistical tools* were available in only five cases.

–none used statistics to *analyse their entire database on a periodic basis*; only annual figures were generated and reported.

. *Step 6 (Interpretation):*

- all except one would almost automatically take measures *after serious individual incidents* has happened.
- to repeat a point made earlier with Step 4: none used a *model* to link causes to proposed measures; this problem - solving process occurred purely by “experience, intuition, expert opinion, etc.”.

. *Step 7 (Evaluation):*

- none would *evaluate the effectiveness* of specific measures; only a global evaluation would be made in the annual safety report.
- none *compared near miss analysis results explicitly with other indicators* of safety performance (e.g. scores on audits).

7.2.4. General results and conclusions

On the basis of the results mentioned in the previous paragraph and from the discussions on the NMMS framework and its human behaviour model the following conclusions could be drawn:

1. There was a general acknowledgement of the importance of the *learning potential of a NMMS*, making it a highly desirable safety management system in the near future, for all three purposes (Modelling, Monitoring, and Alertness). The introduction of a *human behaviour model* was seen a likely means to increase the efficiency of resource allocation, by proposing more effective measures to deal with structural root causes involving human behaviour; the lack of cognitive psychological expertise on the part of safety managers was seen as problem to achieving the above.

Back up to the NMMS in the form of *training* (for Steps 1, 3 and 4), *decision support* (for Steps 4 and 6) and, in particular, a top-down guarantee of a “*no blame*” policy on the part of management were seen as essential (but very hard to achieve) for a successful implementation, as were *feedback* and *user-participation*.

To convince line-management of the need and direction of resource alloca-

tion to structural safety measures it was deemed necessary to generate from the NMMS database not only *statistical arguments* and some *cost/benefits expectations*, but also sufficiently “rich” *verbal descriptions* of actual near misses. Many of the safety staff however foresaw difficulties to have the concept and implications of “*organisational or management failure*” accepted by managers for some years to come: safety management training of line-managers would be a solution for this eventually.

All safety staff stressed the importance of *occasional ad-hoc reactions* (after unique incidents with possibly wide implications for other parts of the industrial system), next to the need for more structural measures based on periodic analysis of the entire NMMS database.

The proposed *integration* of management tools and systems in the areas of Health, Safety, Environment and Reliability was widely applauded, specifically as to their reporting and root-cause analysis.

2. *Comparing the different case studies*, both between and within the aforementioned sets, led to the somewhat surprising conclusion that the quality of the NMMS design and implementation was not so much dependent on the prevailing safety culture or level of safety performance of the entire industrial sector or even of the company as a whole, but was thought to be largely the result of *initiatives and support from individuals at the middle management levels*, both in safety- and in line-management: a clear indication of the *lack of top-down supported standardisation* of incident reporting and analysis (see also the results relating to Step 1 in section 7.2.3.).

Another observation was that so far only one company had the official policy that serving on the safety department was a standard part of the career-track for future line managers. This had the effect of both immediately upgrading the status of safety management and on the longer term sensitizing future managers.

The *large variety* of NMMS experiences and views shown earlier to exist both within and between companies can be summarised as follows. Many locations and companies were actively trying to introduce or maintain some parts of a NMMS, with varying degrees of success due to *different sets of strong and weak points* in design and implementation. An exchange of views and experiences within and between companies and industrial sectors

in the Netherlands would therefore be extremely fruitful for all participants.

A specific NMMS implementation at a chemical process plant

8.1. INTRODUCTION

In the previous chapter an overview was presented of the experiences with NMMS systems currently operating in Western-Europe and in particular in the Netherlands. One of the case studies at the CEC workshop (see section 7.1) was that of a chemical process plant of Exxon Chemical Holland B.V. at Rotterdam, called Rotterdam Aromatics Plant (RAP). A brief report of this project up to 1991 was given in the workshop proceedings (Van der Schaaf, 1991). This chapter will contain an extended and updated version (until April 1992) of this still ongoing project, focussing mainly on the ways in which the ideas mentioned in Chapters 4 and 5 were operationalised and implemented within an actual industrial context.

Firstly, the situation at RAP will be briefly described, and their main reasons for starting a joint research project for "Human Error Prevention" with Eindhoven University of Technology. Secondly, the design and implementation aspects of a NMMS, tailor-made for RAP, will be outlined, followed by some preliminary results. Finally, those aspects of further development which have been designed, but not yet (fully) implemented will be discussed.

8.2. SAFETY MANAGEMENT AT RAP

At the start of this research project in 1988 RAP employed approximately 160 employees, 60 of whom were process control operators and as such the "target group" at the outset.

They controlled this highly automated aromatics plant by supervising the process from a Central Control Room (CCR) equipped with visual display units (so-called computer screens) as the human-machine interface. The five shifts of operators, at that time, had been working for about 16 years (approximately 5 million "man" hours) without a single "Lost-Time Injury" case, which meant an excellent "safety performance" according to that standard.

This long period without serious injuries, however, did not mean that the entire system of safety control had been without any feedback concerning the more hidden problems. It was generally acknowledged that a sizable number of so far nonconsequential errors and failures were probably happening without any systematic understanding of their causes and possible consequences. Statistically speaking, one day some of these hidden dangers could very well result in an actual injury. The existing incident- and near miss reporting system did produce some reports, but these signals originated mainly from simple, well-known hardware-related problems in the plant "outside". From the CCR, truly the information processing "heart" of the entire plant control, nothing was being reported at all. This was considered all the more unsettling because plans for further automating the plant in the future would mean that the CCR operator's task would become even more crucial to plant safety. A further concern on the managers' side was the fear that after such a long time without real injuries people would tend to become less safety-conscious during task performance.

To characterise Exxon-RAP in terms of the purposes mentioned in Chapter 3, *all three purposes* were relevant for setting up a near miss reporting and analysis system in this case; *modelling* of the effects on safety of operator behaviour, especially of the more cognitive tasks in the CCR; *monitoring* of the real effectiveness of the existing safety management system, and increasing its efficiency by allocating its resources more optimally; and finally maintaining *alertness* by being regularly confronted with warnings in the form of reported near misses. Also, all *four functional specifications* for NMMS design mentioned in section 4.1 were relevant: *learning* from such incidents; *comprehensive coverage*; based on a *human behaviour model*; and *integration* with the existing Total Quality Programme to ensure optimal acceptance. Finally, the fact that these efforts were undertaken by Exxon in a situation which by no means was alarming at the time, probably labels this

organisation as a *generative* one (see Chapter 6).

8.3. NMMS DESIGN

Following the reasoning of Chapter 4, a complete NMMS with all seven modules had to be designed. These are briefly described below, in the order of “processing” a reported near miss.

Module 1 (Detection) is actually a simplified version of the existing “incident and near miss reporting form”. The usual categories for pointing at “the single main cause” (and perhaps a few contributory factors) were deleted, leaving the reporter to only briefly describe the near miss and suggest possible ways of improving the situation giving rise to it. Also the routing through the organisation was changed in order to minimise the response delay from the safety coordinator and the production manager.

Module 2 (Selection) is meant to act as the main point for deciding which purpose(s) shall have priority in processing a given near miss: known problems will follow the *monitoring* mode (see figure 4.2), new problems will be used for *modelling*, while some of the previous categories might also be used to provide detailed, convincing examples to maintain *alertness* and raise safety awareness.

An alternative way to regard this Selection phase is to see it as the point at which it is decided that a lot or just a little is to be learned from processing a particular near miss report; this in turn justifies a substantial amount of time and effort to be spent in the following NMMS modules, or just the bare minimum of resources, respectively. In the former case a complete analysis will be performed, tracing the near miss situation back to all its root causes, while in the latter case only the most obvious, direct factor will be classified as “the cause” of the entire incident, which will then be added to the database “for statistics”. Of course such a case of “*coarse*” description and analysis might always later be selected again for further *detailed* processing.

This means in effect a *hierarchical approach*: all incoming reports are at least processed at the coarse (e.g. single main cause) level, and a few are (either directly, or afterwards) selected for further detailed processing,

depending on their “learning potential”.

Module 3 (Description) contains in the modelling and alterness modes a qualitative adapted form of a traditional fault tree, called “*Incident Production Tree*”. It contains as elements not only faults and errors, but also recoveries. In addition “neutral” elements may be added in order to make the description more complete. These are usually system characteristics (like the fact that in a continuous plant shifts of operators take over each other’s tasks) which may be relevant to understand the sequence of events but cannot be labelled as positive or negative. The relationships between these elements may be logical (AND- and OR-gates) or chronological (indicating sequences of elements, or permanent presence of elements). An example of such an Incident Production Tree is given in Appendix 2.

Module 4 (Classification) is directly based on the model described in Chapter 5, with the following changes and additions:

- Technical failure: coded as *Design Engineering* (DE), *Design Construction* (DC) or *Design Other* (DX).
- Organisational failure; only one category used here: OP, referring to the quality of not only formal and well-established, but also unofficial Operating Procedures, Work Practices, Guidelines, etc.
- Human (operator) failure, identical to the SRK-based codes in figure 5.1, but with the following additions:
 - HC1 *Permanent human capacities* are inadequate (e.g. insufficient strength, height, or eyesight).
 - HC2 *Temporary human capacities* are inadequate (e.g. occasional use of alcohol, drug, medicine, or non-chronic emotional instability).

These categories were added to comply with Exxon Chemical’s worldwide prevention programmes related to these aspects. Appendix 2 also shows and explains the classification results of the “root causes” of the realistic incident used as an example there.

Module 5 (Computation) consists of a relational database programme (dBase 4) with a so called “shell” around it (Clipper) to allow for more user

friendly interaction. For each processed report it contains the following information: report number; date; unit (= part of plant); a short description in free text of the incident; the routing through the organisation, indicated by codes of specific safety committees; a short description of follow-up actions, if any; the person responsible for implementing these; the deadline for implementation of these measures; status of report + associated actions; as many classification codes of root causes as necessary. The entire user-system dialogue is menu-based, and for every term, concept, code or label a specific help screen with background information and examples may be called up by simply pressing a standard function key.

A wide range of preprogrammed search facilities is available, with all sorts of selection modes (by report number, time period, unit, status, causal code, and any combination of these). From these analyses, output files may be generated for more advanced statistical packages. Graphics facilities enable analysis results to be displayed as pie-charts, etc., for easy and fast interpretation.

Module 6 (Interpretation) reflects, in the form of a Classification/Action Matrix as in figure 5.3, the changes and additions to the classification scheme as described earlier under module 4: for HC1 ("permanent capacities") the most effective action will be *Selection* as a sixth class of management action; for HC2 ("temporary capacities") the most obvious action would be *Motivation* (see section 5.4). When Exxon Chemical's new worldwide Safety Management Guidelines will have been approved, their codes will replace those listed above the columns of the Classification/Action Matrix in order to improve the communication possibilities with other databases of the company.

Module 7 (Evaluation) consists of the feedback loop indicated in figure 4.1, and of an external measure of safety performance called the "Safety Compliance Index".

The feedback loop in the basic NMMS framework should show whether a certain preferred action (according to the Classification/Action Matrix) had indeed an effect on the classification category it is linked with. This effect may be measured by looking at the relative occurrence of that specific error category in the near miss reports handed in during the period following the

implementation of that preferred action.

The "Safety Compliance Index" had been recently developed by RAP to calculate a monthly, overall level of safety performance, before the near miss research project started. This index is based on a broad mixture of inputs: number of safety meetings within shifts, level of adherence to safety rules as noted during regular safety observation rounds in the plant, and other "auditing" inputs covering hardware-, organisational- and human behaviour factors. Because it has no direct overlap in terms of input parameters with the NMMS results, it may be regarded as an alternative operationalisation of the same factors (e.g. quality of Technical, Organisational and Behavioural "safety control") as the NMMS. This then should give RAP an opportunity for a general cross-check of the NMMS results, especially with regards to indications of trends in level of safety performance.

8.4. IMPLEMENTATION ASPECTS

Before specifying the implementation aspects, again in the order of modules one through seven, three important general aspects must be mentioned first:

- *management support* needed to provide the level of trust required for any voluntary reporting system; RAP employees are guaranteed that the NMMS acts as a *learning instrument* only;
 - *extensive end-user participation* in the design of all modules;
 - *feedback to personnel* about all NMMS aspects; not only can the "progress" of individual reports be traced by the reporting persons, but also the NMMS output in general is quite frequent (monthly reports available to all; special near misses mentioned in the weekly magazine, or even in instantaneous warning flyers).
- *Module 1 (Detection)*: the new reporting form has been presented as a modification of the existing, well-known form in order to stress the *evolutionary* aspects of safety management at RAP, thereby stimulating its acceptability.

Because of RAP's special interest in CCR near misses, it was decided to create a *reference database* for CCR near miss reports: a comparison with later voluntary reports regarding the CCR task environment could then be

used to monitor the “representativeness” of such reported CCR near misses relative to the actual incidents in the CCR. As we saw in Chapter 2, a certain *bias* (either conscious or not) on the part of the operators might be expected, by reporting more freely on certain types of “errors” than on others.

We tried to arrive at a representative picture of CCR task performance by having a series of extensive, *confidential interviews* (based on Flanagan’s (1954) CIT) with CCR operators *before* implementation of the first NMMS modules had started. In each interview a different operator was asked to report on a CCR near miss during the last year and of his own choice, which had not been previously reported. The near miss was then described (as if it were a “forced” near miss report) in the form of an Incident Production Tree, after which all its root causes were classified according to the RAP model described earlier. After each set of five subsequent interviews the overall pattern of classification results was checked for “stability”: it turned out that the results (i.e. the relative frequencies of classified root causes) after 30 interviews did not differ overall from those of the first 25: therefore the series of interviews was stopped after 35 operators (about two thirds of the available CCR population at the time) had participated.

- *Module 3* (Description): a dozen employees already have been *trained* in qualitative fault tree analysis by an external training institute.
- *Module 4* (Classification): to aid *every employee* in understanding and applying the RAP classification scheme, a simple form of *decision support* has been developed and fully integrated within the database interface. It consists of a series of yes/no questions which follow exactly the decision tree (adjusted to the RAP model) of figure 5.2. Each question is illustrated by two examples: one based on a true incident (or an element thereof) from the RAP safety files, which should be very recognisable and valid for every operator; the other based on an aspect from a task environment familiar to both RAP operators and almost everyone else: car driving.
- *Module 5* (Computation): any report (or element of an Incident Production Tree) classified by the Classification Support Programme described above, is automatically added to the database. All database manipulations are

completely menu-driven, and its graphical output provides easy overview of the analysis results.

- *Module 7 (Evaluation)*: the fact that an already existing measure with a high degree of face validity, the Safety Compliance Index, will be used as a cross-check of the NMMS results, is also meant to increase acceptability. To “compensate” for the extra tasks (e.g. Description, Classification, Computation) imposed on the local Safety Manager by the NMMS, other *administrative safety management tasks have been automated* to a high degree at the same time: producing monthly and annual overviews, both to senior management and to operators, is automatically done after selecting a certain option from one of the database menus. The database programme may also produce an instantaneous list of all reports still to be handled or actions to be taken, plus the persons responsible for doing so. All communication to other employees is also facilitated by linking the entire NMMS database, etc. to a Local Area Network.

8.5. PRELIMINARY RESULTS

8.5.1. Acceptance

In terms of *acceptance* within RAP the first signs are quite favourable: the NMMS concept as such has been accepted by both the local safety manager and the executive production manager, even to the degree that both are actively promoting it nationally and internationally within the Exxon Chemical Company and beyond. Also the operators have indicated their vital willingness to report by increasing the number of reports by 300% to a stable level of around 100 to 120 reports per year (including now also CCR incidents!). About half of these are on actual near misses, the others on (very) minor damages or on “first-aid” type injuries.

8.5.2. Level of voluntary reporting

Two informal analyses show that this *level of voluntary reporting* is probably adequate to get a proper insight into the RAP-incident root causes:

- about 30 to 35 interview reports relating to CCR task performance were enough for an *overall* stable pattern of relative frequencies of classification results (see the Reference Database development mentioned in the previous section).
- a comparison of the overall results of the first 64 reports from 1989 with the total set of 113 reports from that year revealed no differences in classification pattern.

8.5.3. Reliability of the classification

Reliability of the classification process was the subject of a formal test in which the same set of 80 actual reports from 1989 were independently classified by the local safety manager, and a student of EUT. This classification was on the basis of assigning *one main cause* only for each report (so called “coarse” classification). The degree of overlap in the classification results of the two judges was regarded as a measure of the reliability of the classification process (see Table 8.1).

Table 8.1: Degree of overlap (in percentages of a total of 80 reports) in the classification results of two independent judges for three levels of analysis (17, 7 or 4 categories) and two sets of data (raw data = basic results of the two judges; corrected data = raw data, after correction of different main causes of the same report, and of misinterpretations of classification scheme).

Level of analysis	Raw data (n=80)	Corrected data (n=80)
<i>detailed</i> : all 17 subcategories	36%	81%
<i>middle</i> : 7 categories (D, O, HK, HR, HS, HC, X)	60%	83%
<i>main</i> : 4 categories (D, O, H, X)	70%	88%

It should be stressed that this was a rather strict test, and that a more realistic test planned in the near future (see section 8.6) would probably give more satisfactory results:

- the EUT student only had the short descriptions (in free text) of the NMMS

- database reports available,
- the backgrounds of both judges were very different: Mechanical Engineering (safety manager) vs. Management Science (EUT student),
 - both judges were still relatively new to the classification scheme,
 - the Classification Support was not yet available then.

Looking at Table 8.1 we see that 36% of all 80 reports were originally classified in exactly the same subcategory (out of 17). Further analysis showed that most of the remaining reports were classified in *adjacent categories* (e.g. HK1 instead of HK2): this is shown by the large improvement (from 36% to 60% overlap) at the middle level of analysis. As a result of further analysis of these differences in classification, two problems with the “raw” data appeared:

- 1) many times it was obvious that different aspects or task elements of the same report had actually been indicated by the judges as “the main cause” and then been classified accordingly;
- 2) in a few cases the intended meaning of the different classification categories (see Chapter 4) had not been perfectly understood by the two judges.

Both problems could be easily corrected: by demanding a clear indication by each of the two judges of exactly which “main cause” was being classified, and by explaining the entire classification scheme again to each judge; re-analysis then resulted in the “corrected” data set (at the righthand column of Table 8.1) showing a spectacular increase in percentage of agreement between the two judges.

8.5.4. “Coarse” vs. detailed classification

“Coarse” vs. detailed classification: the analysis reported in section 8.5.3. already showed a major problem (and its solution!) of coarse classification: *indicating which aspect* precisely of the “story” describing an incident is seen as the main cause. That necessitates then a second requirement for any sensible application of coarse classification: a *full* (e.g. complete, detailed, unbiased) *description* of the incident itself. Another advice could be to aim at the middle level of analysis (only 7 categories to choose from) instead of all 17 (sub)categories.

An informal test (with only one judge: the EUT student) has been performed on the 35 CCR reports from the Reference Database: these were not only classified at the coarse level, giving 35 classifications, but also later on the basis of all 35 Incident Production Trees (with a total of 306 classified root causes). It turned out that both overall distributions of relative frequencies of classification results (using all 17 subcategories) were almost identical.

8.5.5. General evaluation

Although the project is still ongoing it is worthwhile to try to (subjectively) estimate the level of progress made on each of the three purposes mentioned earlier in section 6.2:

- *modelling* has certainly been improved because of the insights into CCR task performance; a follow-up research contract on fault diagnosis support has already been started.
- *monitoring* may be judged soon when the database has grown sufficiently to apply the required statistical tools;
- *alertness* seems to be improved, not only with the safety staff, but also with the management and operator levels as manifested by their interest and cooperation in using and maintaining the NMMS.

Now, in 1992, RAP has been working without Lost-Time-Injuries for almost 20 years (6 million person hours). “Fortunately” the measurement of performance of the NMMS *on that level* is still as difficult as it was 4 years ago (i.e. still no accidents). The acceptance and overall correct and intensive use of near miss reporting however will have to do as probably the best performance measure available at this moment.

8.6. FURTHER DEVELOPMENTS

As mentioned earlier, the NMMS project at RAP is still continuing: a basic version of all modules has been implemented now, and these will be ready for formal evaluations in the near future, after which further refine-

ment will take place. We will conclude this chapter by indicating a few important new developments which will come on top of these refinements:

- *integration* with other reporting systems; e.g. on *Environmental Incidents* and on *Total Quality* aspects.
- *extension* to other groups of RAP employees (Maintenance, Engineering, Administration), and eventually also to Contracting workers.
- extension to *human recovery* aspects, when suitable classification models will become available .
- introduction of *new training tools*: a videofilm exercise has been developed to help employees *recognise* the importance of reporting all (elements of) near misses, even those which look trivial at first sight: this short movie has already been tried out extensively using EUT students as subjects, and it seems worthwhile to use for operator training in the near future.
- new *process simulation facilities* at RAP may also well be used to generate conditions under which operators are likely to “*produce*” *errors and recoveries*, and also to try out different forms of *decision support* for fault diagnosis, etc.
- finally, a very important likely boost to NMMS development and its acceptance will be a training programme aimed at all five *shift supervisors*: they will receive extensive instruction on the SRK-model and its consequences for the classification process. Afterwards they will independently classify the same set of 25 near miss reports and use the results both for a better understanding on their part, and of course also to give feedback on the clarity of the classification scheme (see section 8.5.3) and its associated Support software. Both types of feedback will help them to motivate their own shift operators to produce near miss reports whenever possible.

Discussion and Conclusions

In this final chapter first the main lessons from the applications mentioned in Chapters 7 and 8 will be recapitulated. Secondly, the current status of near miss reporting as a safety tool in the chemical process industry will be reviewed. Finally, future developments will be outlined.

9.1. MAIN LESSONS

In Chapter 7 already, specific lessons were drawn based on the *CEC workshop* (section 7.1) and the experiences during the *national NMMS survey* (section 7.2). These lessons were also reflected in the one *detailed feasibility study* so far, at Exxon-Rap, described in Chapter 8.

The main lessons in *designing a NMMS* from the applications mentioned above are:

- models of human behaviour, let alone models of complete organisational behaviour, are not being used in these industrial safety management systems at the moment, in spite of the fact that safety managers fully acknowledge the general importance of human behaviour and its organisational context, in “producing” incidents;
- two main reasons for the situation as described above are the *lack of theoretical and practical knowledge* of human/organisational behaviour within these industries, and the *lack of integrated tools* offered by researchers, based on such models, to describe, analyse and follow-up incidents.

The main lessons with respect to *implementation aspects* concern the ways in which *acceptance by all employees* of the NMMS may be established:

- in *all* cases a clear “*no blame policy*” for reporting near misses is a vital success factor;
- in *all* cases *specific training programmes* and support tools must be developed, with heavy *involvement of the end users*;
- in *all* cases *continuous feedback* is necessary to show exactly who is doing what with the information reported, and to acknowledge that (at least in voluntary reporting systems) the *willingness to report* freely, completely and unbiased is essential.

9.2. CURRENT STATUS OF NEAR MISS REPORTING

As already mentioned in section 7.2.4, the general picture is that of *many local NMMS initiatives* in industry, each with their specific strong and weak points. Therefore, an exchange of information, not only between plants and companies, but also between theoretical ideas from researchers and practical views or experiences from safety staff would be beneficial to all parties concerned.

Furthermore, at this moment the purpose of *modelling* usually is the only reason mentioned for these NMMS initiatives; only a few companies also are recognising the monitoring possibilities, while the purpose of alertness seems to be Utopian for most of them

9.3. FUTURE DEVELOPMENTS

9.3.1. *Evaluation* of NMMS assumptions, components and complete systems is an important step to be made *as soon as possible*. The difference between the three purposes of Modelling, Monitoring and Alertness must be reckoned with in such evaluations. On the longer term more precise *cost-benefit analyses* will be possible, when the NMMS results in terms of the traditional output indicators (e.g. number of incidents) become visible

For example the “iceberg” assumptions mentioned in section 3.3. seem logical and reasonable, but have not yet been properly tested. Both the qualitative assumption of overlapping sets of root causes, and the quantitative one on the ratio of accidents of near misses etc., will be extensively tested in

the next few years in the course of a NMMS research project at a very large steel plant, which (still) has several hundreds of actual accidents (both injuries and fatal ones) each year. In this project where human recovery and the Alertness purpose are the main themes and which is financially supported by the European Coal and Steel Community's Safety Fund we hope to be able to register and compare extensive sets of accident- and near miss causes from the same sections, for a proper test of the iceberg model's assumptions. The CEC workshop also has shown that experiences from the *transportation sectors* (e.g. traffic conflicts; air misses) can be useful for the chemical process industry (and vice-versa). Closer cooperation between safety experts from those domains therefore should be established.

9.3.2. The effectiveness and efficiency of near miss reporting systems (and of safety management in general) may be even further increased by adding *human recovery promotion* to the already existing human error reduction strategies: the growing availability of *simulation* facilities may constitute an important boost to the modelling and training of such human recovery capabilities. This positive view of humans as system defences certainly deserves much more theoretical and empirical work in the future.

9.3.3. *Integration* of a NMMS with other new developments in safety research should be taken seriously; e.g. near miss reporting, experiments with local "safety circles", and auditing tools like those by Reason (see Chapter 3) could very well be made mutually reinforcing.

For the purpose of this thesis the "spinoffs" of near miss reporting schemes for *Quality, Reliability and Environmental programmes*, although important, must be considered as *positive by-products*. The main points of overlap between these areas are:

- the possibility of *measuring* system performance on a behavioural level in a quantitative way;
- raised *awareness* of system defects as a first step towards eliminating them;
- a "zero defects" *attitude* in terms of goal setting with respect to "acceptable risk"; prevention (or timely recovery) is preferred over correction.

In the long run these points of overlap should lead to more cooperation

between safety staff, environmental managers, reliability engineers and quality managers; they will eventually probably realise that many “root causes” of the problems in their respective areas of interest are very much alike, if not identical.

9.3.4. Near miss reporting is already expanding to *areas of application* outside the “traditional” ones of process control, civil aviation and other transportation sectors. The most promising new areas could be:

- *medical treatment*, because of the obvious fatal (not always “calculated”) risks involved, and the extremely complex organisational structures (e.g. of hospitals) which have probably hindered near miss reporting efforts so far most of all.
- *software development*, because of its growing catastrophic potential (in case of unforeseen latent software errors, or viruses), and because of its errors being almost 100% of human origin: an obvious candidate for application of human behaviour models in its development and testing procedures.

Summary

During the last decades industrial safety management has shown substantial improvement as accounted for by the number of accidents per unit of time per employee. In the chemical process industry in particular, the remaining number of serious injuries or damages in some cases have decreased to a level where they, statistically speaking, are no longer suitable to give informative feedback. In other words, there are too few accidents left to use them as a database for actions leading to further safety improvements.

Besides this *quantitative* problem (which may seem a luxury problem to many other industries) the very idea of focusing on just the negative outcomes of process control deviations neglects the valuable lessons to be learned on the basis of positive outcomes. Every time an operator, manager, procedure, or piece of equipment “behaves” in an unexpected way and thereby prevents a likely breakdown of the production system (e.g. as in reduced product quality, environmental releases, etc.) or restores the required levels of safety and reliability, these *positive deviations* could be detected, reported and analysed in order to improve the *qualitative insight* into system functioning on the whole.

A third reason for also paying attention to other events besides actual, but rare, accidents is a more *psychological* one. After several years (or: millions of working hours) of not being confronted with the grim consequences (e.g. an injured colleague) of residual safety risks in their own work environment, people at all levels of the organisation may be expected to take safety for granted and slowly but surely start to loosen their safety-related work habits and attitudes.

It is the main goal of this thesis to show that near miss reporting and analysis is a substantial step forward in solving the three problems mentioned above. Near misses are:

1. much more numerous than actual accidents, thus (partly) solving the quantitative problem;

2. contain valuable information on system functioning by showing why things in the end did *not* go wrong, and thus improve the qualitative insight into the actual practice of process control and
3. near miss reports frequently contain the very reason for having extensive safety rules, training programmes, and redundant safety equipment by showing these defences “in action” in stopping a possible accident sequence and turning it into a near miss situation. In this way they provide a psychologically convincing reminder of the need to keep safety awareness for oneself and one’s colleagues a top priority.

If an organisation for one or more of the above reasons decides to introduce or improve a near miss reporting system it will face two types of problems. Firstly, how to (re)design such a reporting system to become an effective and efficient safety management tool, and secondly, how to introduce and maintain it, with an emphasis on user acceptance and system support.

In this thesis the following *design* aspects are extensively discussed and illustrated:

- *how to model “human error”* in relation to technical and organisational failure. A detailed classification model of operator behaviour is developed, based on Rasmussen’s SRK model. By adding to this some global types of technical and organisational errors it is extended to a classification scheme of system failure (but with an emphasis on operator behaviour);
- how to use such a classification model then as the basis of a *framework for a complete “near miss management system”* including the following seven steps:
 - . Detection: usually on the basis of voluntary reporting by employees;
 - . Selection: of those reports with the highest informative value;
 - . Description: of the selected event, by means of qualitative fault tree techniques;
 - . Classification: of each of the many basic causes, according to the aforementioned system failure model;
 - . Interpretation of the classification results, to come to theoretically

supported suggestions for management actions; and finally,

- Evaluation: by means of an explicit feedback loop, to analyse the effectiveness of such implemented actions.

The *implementation* aspects of a near miss management system are not to be underestimated (they are probably comparable to implementing a successful Total Quality Programme). Three essential aspects are discussed: top-level management commitment; unbiased reporting by employees; and support for middle-management (e.g. safety officers) who are responsible for describing and analysing the reported events:

- *Management commitment* is vital to ensure that organisational *learning* from near misses should be its only function. At the least a voluntarily reported near miss should never have any negative repercussions for those reporting it;
- *Unbiased reporting* may be motivated by training all employees in recognising near miss situations; by showing them exactly what is being done with the reports they handed in; and by giving them fast and frequent feedback of the results;
- *Supporting the safety staff* is necessary to fully appreciate the cognitive backgrounds of the human error model, and to ensure an objective and uniform approach in describing, classifying and interpreting the reported events.

All of the insights and suggestions mentioned in this dissertation are primarily based on two major sources: an international workshop on near miss reporting, held in Eindhoven in 1989, and a three-year contract research project (1988-1991) to design and implement an actual near miss management system for a chemical plant in Rotterdam. Furthermore, the thesis describes a first step towards validation through a series of discussions with safety managers in the Dutch (chemical process) industry.

Finally, in an overview of important future developments, the need for empirical research into the assumptions of near miss reporting is stressed. A promising new theoretical field is that of modelling the human contribution to

positive deviations in system functioning (i.e. *human recovery*). The already available knowledge may be successfully applied to related fields such as Quality-, Reliability-, and Environmental Control, and also to new applications like medical treatment in hospitals, and the development and testing of complex software.

Samenvatting

- Gemeten aan het aantal ongevallen per persoon en per tijdseenheid is de veiligheid in de industrie de afgelopen decennia aanmerkelijk verbeterd. Vooral in de chemische procesindustrie gebeuren relatief zo weinig ongelukken meer dat trends, statistisch gezien, soms dreigen te verdwijnen in de ruis ten gevolge van toevalsfactoren. Het wordt dan moeilijk een database op te bouwen op basis waarvan verdergaande veiligheidsmaatregelen kunnen worden voorgesteld.
- Naast dit *kwantitatieve probleem* (in veel andere bedrijfstakken trouwens als “luxe” probleem beschouwd) blijft er in zo’n situatie ook zeer waardevolle bedrijfsinformatie onbenut. Immers, door zich te beperken tot de negatieve gevolgen van afwijkingen in de procesbeheersing negeert men de lessen die getrokken kunnen worden uit bestudering van de positieve gevolgen: iedere keer dat een operator, manager, bedieningsvoorschrift of technisch onderdeel zich op onverwachte wijze “gedraagt” en zodoende een waarschijnlijke systeemstoring voorkomt, zou zo’n *positieve afwijking* kunnen worden waargenomen, gerapporteerd en geanalyseerd. Hierdoor zou het *kwalitatieve inzicht* in het functioneren van het gehele productiesysteem toenemen, waardoor de productkwaliteit, milieubeheersing, veiligheid en betrouwbaarheid verbeterd kunnen worden.
- Een derde reden om niet uitsluitend naar feitelijke, maar zeldzame, ongevallen te kijken, is van meer *psychologische aard*: als men als werknemer al jarenlang niet meer geconfronteerd is met de concrete gevolgen van veiligheidsrisico’s op de eigen werkplek zal men er menselijkerwijs minder zwaar aan gaan tillen. Langzaam maar zeker zal men deze ogenschijnlijke veiligheid als iets vanzelfsprekends gaan zien, en zich in gedrag en attitude wat nonchalanter opstellen.
- Het hoofddoel van dit proefschrift is om aan te tonen dat de rapportage en analyse van “bijna-ongevallen” een belangrijke bijdrage kan leveren aan het oplossen van de drie bovengenoemde problemen.

Bijna-ongevallen (ook wel “near misses” genoemd) hebben immers de volgende positieve eigenschappen:

1. ze zijn veel frequenter dan feitelijke ongevallen, waardoor het kwantitatieve probleem (op zijn minst gedeeltelijk) wordt opgelost;
2. ze bevatten waardevolle bedrijfsinformatie met betrekking tot de redenen waarom het uiteindelijk *niet* tot een feitelijk ongeval, productiestoring, etc., kwam, zodat men meer kwalitatief inzicht in het werkelijke systeem-functioneren krijgt, en
3. ze tonen het werkelijke nut aan van de vele veiligheidsregels, -trainingen, en -apparatuur doordat ze vaak beschrijven hoe zulke veiligheidssystemen daadwerkelijk een dreigend ongeval omgebogen hebben tot een near miss; als zodanig zijn het psychologisch overtuigende signalen om veiligheidsbewustzijn steeds weer te benadrukken.

. Als een organisatie vanwege één of meer van deze redenen besluit om near miss rapportage in te voeren of te verbeteren, spelen er twee soorten problemen. Ten eerste moet het ontworpen systeem een effectieve en efficiënte ondersteuning zijn van het veiligheidsmanagement; ten tweede moet dit instrument op de juiste wijze geïntroduceerd en onderhouden worden, waarbij gebruikersacceptatie en managementondersteuning belangrijke aandachtspunten zijn.

. De volgende *ontwerpaspecten* worden in dit proefschrift besproken:

- het *modelleren van “menselijk falen”* in relatie met technisch en organisatorisch falen. De ontwikkeling van een gedetailleerd classificatiemodel van operator gedrag wordt beschreven, alsmede de uitbreiding daarvan tot een model van systeemfalen;
- het formuleren van een *raamwerk* voor een volledig “near miss management systeem”, bestaande uit zeven stappen:
 - . Detectie: meestal op basis van vrijwillige rapportage;
 - . Selectie: van die rapporten waaruit het meeste geleerd kan worden;
 - . Beschrijving: van de geselecteerde gebeurtenis, door middel van een kwalitatieve foutenboom;

- . Classificatie: van de basisoorzaken, volgens het model van systeemfalen;
 - . Interpretatie: van de analyseresultaten, naar suggesties voor managers met betrekking tot verbeteringen;
 - . Evaluatie: van de resultaten van de genomen maatregelen.
- . Naast de ontwerpaspecten verdienen ook de *implementatie-aspecten* ruime aandacht: deze zullen waarschijnlijk vergelijkbaar zijn met die voor een "Total Quality" project. De volgende drie essentiële organisatorische randvoorwaarden worden genoemd:
- *Management steun*, door te verzekeren dat de gerapporteerde near misses alleen gebruikt zullen worden om er in algemene termen van te leren, en nooit om de rapporteurs of andere betrokkenen te straffen;
 - *Eerlijke en volledige rapportage*, door alle werknemers te trainen in het herkennen van near miss situaties; door te laten zien wat er precies gebeurt met de rapporten; en door snelle, frequente feedback van de resultaten naar de rapporteurs.
 - *Ondersteuning van de veiligheidsstaf*, door de cognitief-psychologische achtergronden van het gedragsmodel uit te leggen en gebruiksvriendelijke software voor de database te ontwikkelen. Hierdoor wordt bevorderd dat de near misses op een juiste, uniforme wijze worden beschreven, geklassificeerd en geïnterpreteerd.
- . Twee belangrijke bronnen van informatie hebben ten grondslag gelegen aan de inzichten en suggesties in dit proefschrift: ten eerste een internationale workshop over near miss rapportage die met steun van de EG in 1989 te Eindhoven is gehouden. Ten tweede een driejarig onderzoekscontract (1988-1991) met een chemische fabriek van Exxon in Rotterdam waarbinnen een compleet near miss management systeem werd ontworpen en ingevoerd. Bovendien zijn in Nederland de verkregen inzichten getoetst aan de ervaringen van een aantal veiligheidsmanagers uit de chemische procesindustrie en andere sectoren.
- . Tenslotte wordt voor de toekomst de behoefte aan empirisch onderzoek naar de aannamen achter near miss rapportage onderstreept. In theoretisch opzicht is het modelleren van "human recovery" (d.w.z. het vermogen van

mensen tot herstel van het systeemfunctioneren) een veelbelovend nieuw gebied. De huidige kennis kan trouwens al direct toegepast worden op verwante gebieden als Kwaliteits-, Bedrijfszekerheids- en Milieuzorgsystemen. Ook medische zorg in ziekenhuizen en de ontwikkeling van complexe software lijken te kunnen gaan profiteren van de beschreven inzichten in het registreren en modelleren van menselijk handelen in complexe omgevingen.

References

- Algera, J.A. (1987). *Feedback on job performance*. Inaugural lecture. Eindhoven University of Technology. (in Dutch).
- Bainbridge, L. (1984). Diagnostic skill in process operation. *Proceedings of the International Conference on Occupational Ergonomics*, volume 2, 1-10. Toronto, May 1984.
- Brown, G.R. (1991). Use of traffic conflicts for near miss reporting. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Cannell, W. (1989). *Air miss reporting in aviation*. Paper presented at the CEC workshop on Near Miss Reporting. Eindhoven, September 1989.
- Crossman, E.R.F.W. (1974). Automation and Skill. In: E. Edwards and F.P. Lees (eds.), *The human Operator in Process Control*. Taylor and Francis, London.
- Ferry, T.S. (1988). *Modern Accident Investigation and Analysis*. Wiley. New York.
- Flanagan, J.C. (1954). The critical incident technique. *Psychological Bulletin*, 51, 327-358.
- Grayson, G.B. and Hakkert, A.S. (1988). Accident analysis and conflict behaviour. In: J.A. Rothengatter and R.A. de Bruin (eds.), *Road Users and Traffic Safety*. Van Gorcum, Assen.
- Green, R. (1990). Human error on the flight deck. In: D.E. Broadbent, J. Reason and A. Baddely (eds.), *Human Factors in Hazardous Situations*. Clarendon Press, Oxford.
- Hale, A.R. (1985). *The human paradox in technology & safety*. Inaugural lecture. Delft University of Technology.
- Hale, A.R. and Glendon, A.I. (1987). *Individual Behaviour in the Control of Danger*. Elsevier. Amsterdam.
- Hale, A.R., Karczewski, J., Koornneef, F. and Otto, E. (1991). IDA: an interactive program for the collection and processing of accident data. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds), *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Heinrich, H.W. (1931). *Industrial Accident Prevention*. McGraw-Hill. New York.

- Horst, R. van der (1991). Video analysis of road user behavior at intersections. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Hoyos, C.G. and Zimolong, B. (1988). *Occupational Safety and Accident Prevention*. Elsevier. Amsterdam.
- Hydén, C. (1987). The development of a method for traffic safety evaluation: *The Swedish Traffic Conflicts Technique*. Bulletin 70. University of Lund.
- Ives, G. (1991). Near Miss Reporting pitfalls for nuclear plants. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Johnson, W.G. (1980). *MORT Safety Assurance Systems*. Marcel Dekker. New York.
- Lucas, D.A. (1987). Human performance data collection in industrial systems. In: *Human Reliability in Nuclear Power*. IBC Technical Services, London.
- Lucas, D.A. (1992). Understanding the human factor in disasters. *Interdisciplinary Science Reviews*, 17, 185-190.
- Makin, P. and Sutherland, V. (1991). A fatal inversion? *Occupational Safety & Health*, nov. 1991, 40-42.
- Masson, M. (1991). Understanding, reporting and preventing human fixation errors. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Moraal, J. (1983). *Manageable ergonomics*. Inaugural lecture. Eindhoven University of Technology (in Dutch).
- Norros, L., Toikka, K. and Hyötyläinen, R. (1989). *Constructing skill-based FMS - Lessons for design and implementation*. Paper presented at IFAC/IFIP/IMACS Symposium on Skill Based Automated Production. Vienna (Austria), November.
- Oortman Gerlings, P.D. and Hale, A.R. (1991). Certification of safety services in large Dutch industrial companies. *Safety Science*, 14, 43-59.
- Perrow, C. (1984). *Normal Accidents: living with high-risk technology*. Basic Books. New York.
- Petersen, D. (1989). *Techniques of Safety Management: a systems approach*. Aloray. New York.

- Rasmussen, J. (1976). Outlines of a hybrid model of the process operator. In: T.B. Sheridan and G. Johannsen (eds). *Monitoring Behaviour and Supervisory Control*. Plenum Press. New York.
- Reason, J.T. (1987). Generic Error-Modelling Systems (GEMS): a cognitive framework for locating human error forms. In: J. Rasmussen, K. Duncan and J. Leplat (eds). *New Technology and Human Error*. Wiley. New York.
- Reason, J.T. (1988). Framework models of human performance and error: a consumer guide. In: L.P. Goodstein, H.B. Andersen and S.E. Olsen (eds). *Tasks, Errors and Mental Models*. Taylor and Francis. London.
- Reason, J.T. (1990). *Human Error*. Cambridge University Press. New York.
- Reason, J.T. (1991). Too little and too late: a commentary on accident and incident reporting systems. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Report of the Presidential commission on the Space Shuttle Challenger Accident (1986). Government Printing Agency. Washington DC.
- Rouse, W.B. (1981) *Models of human problem solving: detection, diagnosis and compensation for systems failures*. Preprint for proceedings of IFAC conference on analysis, design and evaluation of man-machine systems. Baden-Baden, FRG, September 1982.
- Schaaf, T.W. van der (1988a). *Moving from accident research towards methods for near miss reporting*. Proposal for a workshop to be funded by the Commission of the European Communities.
- Schaaf, T.W. van der (1988b). Critical Incidents and Human Recovery: some examples of research techniques. In: L.H.J. Goossens (ed.). *Human Recovery*, Proceedings of the COST A1 Seminar. Delft, 1987.
- Schaaf, T.W. van der (1989). Systemfaults and Human Behavior. In: *Handbook of Maintenance Management*. Samson: Alphen a/d Rijn (in Dutch).
- Schaaf, T.W. van der (1990). Man as the strongest link in the chain. In: J. van Wijk (ed.). *Magazine of the Dutch Society of Reliability Technology*. Revue Arts: The Hague (in Dutch).

- Schaaf, T.W. van der (1991a). Development of a Near Miss Management System at a Chemical Process Plant. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds.). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Schaaf, T.W. van der (1991b). *Controlling human error and human recovery in the process industry*. Paper presented at the Exxon "Human Behaviour Technology" Group Meeting, Deauville (France), October.
- Schaaf, T.W. van der (1992). *A Survey of Near Miss Reporting in the Netherlands*. Report EUT/BDK, Eindhoven University of Technology.
- Schaaf, T.W. van der, and Lucas, D.A. (1989). *Report to the Commission of the European Communities of the Eindhoven Discussion Meeting on Near Miss Reporting*. Eindhoven University of Technology.
- Schaaf, T.W. van der, Hale, A.R. and Lucas, D.A. (1991) Conclusions of the CEC workshop at Eindhoven. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Schaaf, T.W. van der, Lucas, D.A. and Hale, A.R. (1991). *Near Miss Reporting as a Safety Tool*. Butterworth-Heinemann. Oxford.
- Svenson, O. (1991). The Accident Evolution and Barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis*, 11, 499-507.
- Swain, A.D. (1974). *The Human Element in Systems Safety: a guide for modern management*. InComtec Ltd., Camberley.
- Taylor, R.K. and Lucas, D.A. (1991). Signals passed at danger: near miss reporting from a railway perspective. In: T.W. van der Schaaf, D.A. Lucas and A.R. Hale (eds.). *Near Miss Reporting as a Safety Tool*. Butterworth-Heineman. Oxford.
- Wagenaar, W.A. (1983). *Human Error*. Inaugural lecture. University of Leiden (in Dutch).
- Wagenaar, W.A. and Groeneweg, J. (1987). Accidents at sea: multiple causes and impossible consequences. *International Journal of Man-Machine Studies*. 27, 587-598.
- Westrum, R. (1988). Organisational and inter-organisational thought. World Bank Workshop on Safety Control and Risk Management. Washington D.C., October.

The smallpox case (Makin & Sutherland, 1991)

“Some time ago the international health organisations undertook a concerted campaign to eradicate smallpox. Most cases of the disease occurred in the ‘third world’ and the ‘front line troops’ for the campaign were health visitors. Each of these had a geographical area for which they were responsible. In order to motivate the health visitors a bonus scheme was introduced.

Arguing that the final goal was the eradication of small pox, a scheme was devised whereby each visitor was rewarded according to the absence of smallpox in their area. However, although the visitors consistently earned good bonuses, smallpox remained endemic. When considered from the visitors’ perspective the reasons for this apparently paradoxical situation becomes clear. If you are rewarded for the lack of cases, the incentive is to turn a blind eye. When in doubt don’t report. The system is obviously open to abuse.

Management finally realised the potential for abuse, and the reward system was turned on its head. Instead of being rewarded for the absence of cases, visitors were now rewarded for finding cases. The results were dramatic, undiscovered cases now came to the attention of the authorities and could therefore be treated. As we are all aware, smallpox is now officially ‘dead’. However, it is doubtful that this would have been the case had the original reward system not been changed.”

The Panel Control Near Miss

In this appendix an *example* will be given of the way in which an actual near miss report would be handled according to the procedures set out in Chapters 4 and 5. First the main characteristics of this near miss will be described, followed by discussing the application of all relevant NMMS steps and their results; it is assumed here that the purpose of *Modelling* is the main goal of these analytic efforts (see figure 4.2.), which means that the Description-, Classification- and Interpretation phases of the NMMS are the ones discussed below.

1. MAIN CHARACTERISTICS OF THE “PANEL CONTROL” NEAR MISS AS AN EXAMPLE

The near miss presented here is loosely based on an *actual* near miss in the Dutch chemical process industry, but it has been *both simplified and somewhat extended* to serve as an useful example for an audience not familiar with that specific process.

It was chosen and adapted to illustrate a combination of different *types of causes*. That is why its *complexity*, as shown in the Incident Production Tree later on, probably is somewhat higher than that of the average reported near miss.

It also shows the importance of future developments in safety research, stressing the reporting, describing and analysing not only of failures, but also of *recovery*; however, the focus on *failures* in this thesis explains the detailed analysis of the failure aspects and the brief description of the recovery elements in this example.

Finally, the example given here shows the possibilities of the Incident Production Tree method to *go beyond the single near miss* originally reported, by *adding alternative failure (or recovery) elements* if these seem realistic according to the source(s) describing the near miss backgrounds.

That is why the Tree not only contains AND gates, but *also OR gates*.

2. DESCRIPTION AND ANALYSIS OF THE “PANEL CONTROL” NEAR MISS

The application and results of all NMMS phases relevant to the purpose of Modelling (see figure 4.2.) are described below:

2.1. Detection

The incident took place at a Central Control Room (CCR) panel controlling a so-called Hydrogen Concentration Unit (HCU). A sudden change in the flow of the feedgas to the HCU triggered an *alarm* in the control room which was subsequently detected and interpreted by the operators responsible for this unit in a correct and timely fashion; their appropriate corrective actions resulted in preventing a costly “trip” (e.g. automatic shut-off) of the entire unit.

2.2. Selection

The following reasons existend for reporting this incident as a near miss and for a detailed analysis by the safety and production staff:

- the consequences of an actual HCU trip (which had barely been prevented!) would have been very costly in terms of production losses;
- although the late recovery (triggered by the feedgas alarm) had been successful, it was immediately obvious than an opportunity for earlier detection and recovery by a CCR operator had clearly been missed.

2.3. Description

A thorough investigation involving operators, safety coordinator production- and engineering staff resulted in the following *verbal description* of what had happened; the numbers in brackets refer to specific components shown in the *graphical description* of the same incident, the Incident Production Tree (see figure 1)

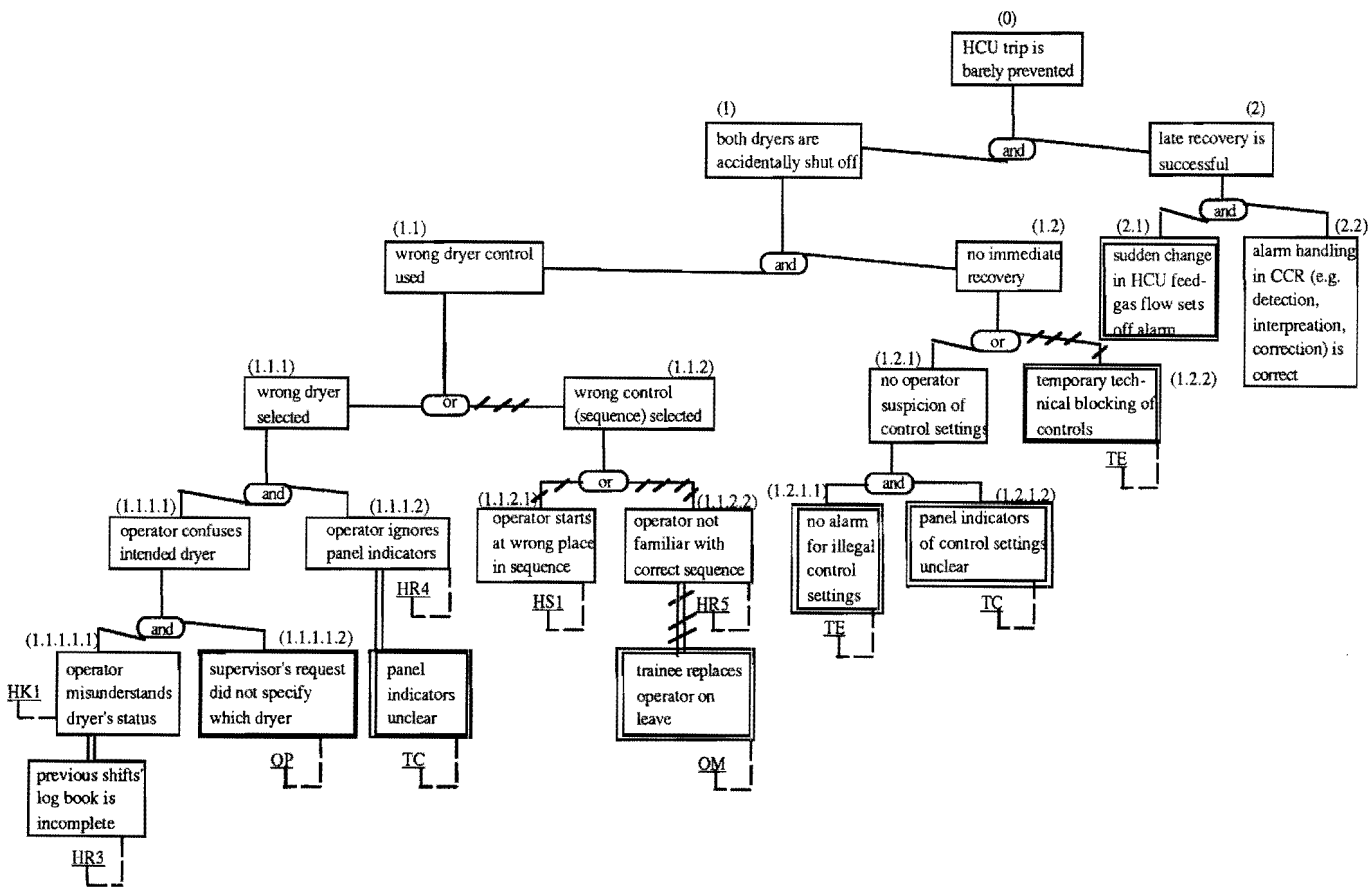




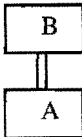



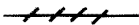


Figure 1: Incident Production Tree of the Panel Control Near Miss.

	logical "and" gate
	logical "or" gate
	incidental tree-component
	permanent tree-component
	linear (e.g. non-branching) link: B further specifies the consequence of A
	chronological order: first A, then B (A and B at same hierarchical level)
	end-point (e.g. "root cause") classification code of A
	connection within the <u>actual</u> incident
	<u>plausible</u> , but not historic, connection within alternative incident
(x.x)	hierarchical sequence number of tree-component

Legend of Figure 1

The so called top-event (0) is the fact that an HCU trip had barely been prevented by a successful "late recovery" by CCR operators (2). The immediate cause of the feedgas alarm (2.1) which was adequately handled by the operators (2.2) was the fact that both *dryers* of the HCU had accidentally been shut-off at the same time by an operator (1). Normally, one of these two dryers *must* be operative while the other one is being regenerated. Then this last dryer must be started and the former one stopped for a regeneration process, and in this way the two dryers alternate continuously. In order to perform this "dryer-switching" operation an operator has to close and open a

series of four valves by pressing the related buttons on the control panel in a *specific fixed order*. Something had gone wrong in doing so, e.g. the wrong dryer control button had been used (1.1), and, even more seriously, this had *not been noticed and corrected* by the operator in charge (1.2.1 and 1.2).

The “illegal” status of the resulting control settings, indicated on the panel interface by the positions of buttons and switches, had not been noticed by the operator, because these panel indicators were very unclear from an ergonomic point of view (1.2.1.2), and because no alarms existed in general for any “illegal” combination or sequence of control settings (1.2.1.1).

It appeared that the wrong control had been pressed (1.1) because the operator had selected the wrong dryer (1.1.1), ignoring the status information available on the panel (1.1.1.2), again because such indicators were generally considered by the operators to be unclear.

The conclusion was that the operator had started the “correct” series of actions on the *wrong* dryer (1.1.1), being confused about which dryer had to be started and which one had to be stopped. (1.1.1.1).

This was triggered by an earlier misunderstanding of which dryer was operative and which was not (1.1.1.1.1), based on reading the incomplete logbook of the previous shift’s activities.

This misunderstanding of the dryers’ status had *not* been corrected by the prescribed formulation of his supervisor’s request to “start dryer A and shut-off B”; in stead, the supervisor had simply asked him “to switch both dryers” (1.1.1.1.2).

During the discussions of how *this* specific sequence of events had happened, suggestions were made by operators and engineers that other failure components, which were also considered as feasible, could be added to the Tree, thus adding to the general insight into how this incident *and similar ones* could be “produced”, and enlarging the set of related causal factors.

Two examples of these additions, resulting in OR-gates, are given here. First, it was considered quite possible that the same incorrect control button (1.1) could have been pressed because of a sequence error on the correct dryer (1.1.2). The operator could have simply hit the wrong button while intending to follow the correct sequence (1.1.2.1.), or he could have been mistaken in the correct sequence itself, because of lack of experience (e.g. trainees were sometimes replacing experienced CCR operators on leave).

Another important addition was the fact that “immediate recovery” (1.2) would probably not have been possible anyway, even if the operator would have realised at once that he had used the wrong button! To protect the remotely operated valves from being damaged, a *technical blockade* had been built into the interface such that for a number of seconds after a control button had been pressed this valve’s motions could not be reversed by the operator changing the control setting again to the original position!

2.4 Classification

The results of applying the classification model of system failure (see figure 5.2) to the eleven endpoints of the Incident Production Tree in figure 1 show a typical, large variety of classifications.

– *Technical factors:*

- the panel indicators (1.1.1.2 and 1.2.1.2) appeared not to have been *constructed* according to the human factors guidelines built into the design specifications →”TC”
- two obvious examples of *engineering* failure (“TE”) were the absence of an alarm for illegal control settings (1.2.1.1) and the unforeseen consequences of the technical blockade device (1.2.2) which, ironically, was designed explicitly for reliability purposes!

– *Organisational factors:*

- the supervisor’s “relaxed” way of communicating with his operators implicitly assumed that the operator’s idea of the system status was the same as the supervisor’s, and that both were correct (1.1.1.1.2); since this proved to be a *chronic informal procedure*, this endpoint was considered as a *permanent* one (see figure 1), and coded as “OP”.
- staffing policy of replacing (expensive) senior operators on leave by (inexpensive) trainees was judged to reflect *Management failure* with respect to economic versus safety priorities (“OM”).

– *Human Behaviour:* examples of all three main subcategories (S-B, R-B, K-B) of human (operator) error could be found:

- the operator’s misunderstanding of the status of the HCU dryers (1.1.1.1.1)

- was seen as belonging to the K-B “system status” category: “HK1”
- the incidental failure of the previous shift to record all changes concerning this system status in the logbook was coded as a R-B “coordination” failure: “HR3”
 - the fact that the operator ignored the status information available on the panel interface (1.1.1.2) was classified as a R-B “checking” error, because this check should be carried out in view of the possible consequences of any mistake on the part of the operator: “HR4”
 - a trainee selecting the wrong sequence of actions (1.1.2.2) to be carried out to reach the desired goal would be committing a R-B “planning” failure: “HR5”
 - accidentally pressing the wrong button (1.1.2.1) when the *intended* sequence of actions was correct, could be a clear example of S-B “controlled movement” error: “HS1”

2.5 Computation

In view of the emphasis on the Modelling purpose in this example, the Computation phase is not relevant here.

2.6 Interpretation

The closeness of escaping the consequences of an actual unit shut-down, and the fact that several OR-gates in the Tree indicate even more plausible ways of repeating this problem in the future suggest the following measures to be considered as preventive actions (see figure 5.3):

- short-term actions*:
 - the *panel indicators* should be changed to comply with human factors guidelines; in this respect it would be preferable to go beyond changing just the displays and controls related to this specific near miss; rather the *entire panel interface* should be ergonomically re-evaluated in terms of layout, labelling, display/control compatibility, etc.
 - an even more structural preventive measure could be the technical solution of building into the interface a number of *safeguards* which would make illegal combinations or sequences of control actions simply impossible;

however, all possible situational and action scenarios should be checked then in order to prevent the same kind of unforeseen problems as encountered by originally installing the technical blockade of the valves (1.2.2.)!

– *long-term actions:*

- changing *informal procedures and habits to ensure “fool-proof” communication* within and between shifts of operators would probably be of a more long-term nature, given the assumption that these habits would have evolved over a long period and precisely because they were seen as both efficient and safe (or at least acceptable).
- also the introduction or reinforcement of *training programmes* to understand the backgrounds of the fixed sequence of actions and of related procedures would take time to develop, implement and maintain; this is even more true probably of changing key aspects of plant- (or even company-) *policy regarding staffing levels* for CCR tasks, when the general trends are towards decreasing these levels!

2.7 Evaluation

Again, just as was mentioned in 2.5 above, in view of the Modelling emphasis this Evaluation feedback is not directly relevant; however, in terms of *feedback to the organisation in a broader sense* (see figure 4.3) it will be obvious that both process designers, interface construction engineers, and managers at several levels of the plant and the company could clearly benefit from the analysis as presented above.

List of participants at CEC Discussion Meeting on “Near-misses”, Eindhoven, 6-8 September 1989

<u>U.K.</u>	Dr. William Cannell Dr. David Embrey Dr. Deborah Lucas Prof. James Reason Mr. Roger Taylor	Civil Aviation Authority Human Reliability Associates Human Reliability Associates University of Manchester British Rail Research
<u>The Netherlands</u>	Prof. Andrew Hale Ir. Richard van der Horst Prof. Jan Moraal Drs. Tjerk van der Schaaf	Delft University of Technology TNO-Institute for Perception TNO, and Eindhoven University of Technology Eindhoven University of Technology
<u>Belgium</u>	Drs. Michel Masson	University of Liège, and ISPRA Joint Research Center
<u>Switzerland</u>	Mr. Geoffrey Ives	Colenco
<u>Canada</u>	Dr. Gerald Brown	University of British Columbia

Survey questions within the NMMS framework

A descriptive framework is proposed, consisting of 7 modules (of phases) which together should form an (ideal?) “near miss” management system.

1. Detection module aimed at reporting of the *occurrence* of near misses/ incidents by employees.

Question: how to motivate this (self-)report activity?

2. Selection “interesting” reports (those with high feedback value) must be selected out for further analysis.

Questions: – which selection criteria?
– which decision methods?

3. Description detailed structure incorporating all relevant components (system characteristics, technical faults, errors, recoveries, etc.) and their (chrono-)logical relationships.

Questions: – how detailed?/which stopping-rule?
– which (tree-like) technique, and which type of data-base?

4. Classification components must be classified according to a system model comprising both the technical, procedural and human aspects, but with an emphasis on the last.

Questions: – classification of *all* components or only of the “root” causes, etc.?

– which human-operator model best suited?

5. Computation – facilities for statistical analysis of data resulting from 4.
– facilities for manipulation of the structures of 3. for sensitivity analyses and simulation.
6. Interpretation translation of results sofar in *structural* measures (--> general factors) and *ad-hoc* measures (--> specific/unique factors).
- Questions: how to estimate (and change!) company “culture”/tradition?
7. Evaluation following the effectiveness of implemented measures: feedback to 1., but also using other, independent measures of “safety performance”.

Acknowledgements

The author would like to acknowledge, in chronological order, the following essential contributions to the research project reported in this dissertation:

- for their assistance in the data collection: Rob van Tijen, Raymond Chin and Kees Eijkelenkamp;
- for their continuous support of the Exxon project: Loek Bollen and Jan Koppelman;
- for her creative and effective partnership in setting up the CEC workshop and publishing its proceedings: Debbie Lucas;
- for their support of the CEC workshop in various ways: Jim Reason, Andrew Hale and David Embrey;
- and finally, for her human recovery during the production of the dissertation itself: Marleen van Baalen.

Curriculum Vitae

Tjerk van der Schaaf was born in Medan, Indonesia, on 1 March, 1955. After finishing his Gymnasium- β at Dordrecht he studied psychology at the State University at Leyden. In 1981 he graduated cum laude from the Department of Experimental Psychology on a thesis on auditory perception. From 1981 to 1985 he participated in research projects on "decision making under stress" and in applied projects on cognitive ergonomics at the TNO Institute for Perception at Soesterberg. Since 1985 he is a staff member of the Graduate School of Industrial Engineering and Management Science, Ergonomics Unit of the department of Technology and Work, of the Eindhoven University of Technology. He has been mainly involved in the areas of human behaviour and industrial safety, decision support for fault diagnosis and information presentation on VDU screens.

STELLINGEN

Behorende bij het proefschrift

NEAR MISS REPORTING IN THE CHEMICAL PROCESS INDUSTRY

van

Tjerk Woutherus van der Schaaf

1. Het toeschrijven van incidenten aan de factor “menselijk falen” is slechts zinvol, wanneer duidelijk aangegeven wordt over welke categorie *mensen* men het dan heeft: ontwerpers, leidinggevendenden, of degenen op direct uitvoeringsniveau. (Dit proefschrift, hoofdstuk 2).
2. Het is efficiënter de menselijke vaardigheden tot het verrichten van herstelhandelingen (“human recovery”) te ontwikkelen dan te trachten het daaraan voorafgaande menselijk falen (“human error”) maximaal te voorkomen. (Dit proefschrift, hoofdstuk 3).
3. De grote populariteit van het zogenaamde SRK model van Rasmussen is toe te schrijven aan het samengaan van vaag omschreven, maar zeer aansprekende concepten enerzijds, en het ontbreken van validiteitsstudies anderzijds. (Rasmussen, 1976; Dit proefschrift, hoofdstuk 2).
4. De beoordeling van het veiligheidsniveau van bedrijven door de overheid dient primair gebaseerd te zijn op aantoonbare veiligheidsinspanningen en pas secundair op de concrete eindproducten daarvan, met name op aantallen gerapporteerde ongevallen. (Dit proefschrift, hoofdstuk 8).
5. De Wereldgezondheidsorganisatie (WHO) definieert gezondheid als méér dan de afwezigheid van ziekte; in analogie hiermee is een bedrijf of organisatie niet zonder meer veilig te noemen als er zich geen zichtbare ongevallen voordoen.
6. Volledige procesbeheersing is alleen te bereiken door naast de *gewenste* produkten ook de altijd aanwezige *ongewenste* produkten (o.a. ongevallen, milieu-overlast) te registreren en te analyseren.
7. De overdraagbaarheid van cognitieve modellen laat begrijpelijkerwijs te wensen over: zij dienen immers in de eerste plaats als begripsmatig referentiekader voor de auteurs ervan (zie Bainbridge, 1990).

8. Wanneer slechts weinig bedrijven bereid zouden zijn om universitair onderzoek, dat niet direct tot toepasbare resultaten leidt, te sponsoren, zou dat wel eens meer kunnen liggen aan het onvermogen van onderzoekers om hun onderzoeksvoorstellen duidelijk te verwoorden, dan aan de potentiële toepassingsmogelijkheden ervan.
9. De zegswijze “Als het kalf verdronken is, dempt men de put” geeft een te rooskleurige beschrijving van de werkelijkheid, waarin het zojuist verdronken kalf meestal nog de schuld van het ongeval krijgt, en het verder niet nodig geacht wordt de put te dempen of deze van een omheining te voorzien.
10. Mistdetectoren, derde remlichten, ABS-remsystemen en het voeren van verlichting overdag zijn te beschouwen als technische “oplossingen” voor een *sociaal probleem*: het verkeersgedrag van de Nederlandse automobilist.

Near misses, as precursors to actual, similar accidents later on, may suggest timely preventive action to avoid costly corrective measures. They are also much more numerous than accidents and therefore an attractive data source for quantitative safety management purposes. Finally, they can motivate employees to keep alert in a relatively risky work environment where no serious incidents have occurred for some time.

This thesis explores the contribution that near miss reporting and analysis can make to industrial safety management, in particular with respect to understanding and controlling the "human factor". It offers a framework to design a complete Near Miss Management System, based on a theoretical classification model of system failure. Also, organisational aspects of implementing such reporting systems are outlined. Finally, the state of the art in Western Europe and an extensive feasibility study in the Netherlands are described.

The dissertation is concluded by discussing its relevance for other areas of application: Quality-, Reliability- and Environmental Control; medical treatment in hospitals; and the development and testing of complex software.