68

Proceedings of the XV EUROPEAN ANNUAL CONFERENCE ON HUMAN DECISION MAKING AND MANUAL CONTROL

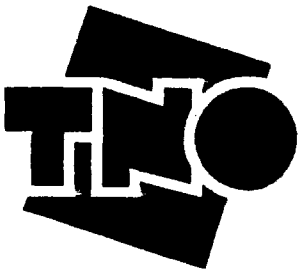
held at the
TNO Human Factors Research Institute
Soesterberg, The Netherlands
June 10-12, 1996

Program Chairman : Henk G. Stassen (Ed, TUDelft)
Organization: : Peter A. Wieringa (Ed, TUDelft)
Hans Godthelp (TNO)
Alexander P. de Vos (TNO)
P. Leo Brinkman (TUDelft)
Jan B. F. van Erp (TNO)

Human Factors Research Institute
TNO

Soesterberg
The Netherlands

Man-Machine Systems Department
Faculty of Mechanical Engineering
and Marine Technology
Delft University of Technology
The Netherlands



Frese, M.; Schaaf, T.W. van der; Heimbeck, D. (1996). *Error Management and Recovery in Technical System Design*, Paper presented at the CESA '96 IMACS multiconference, invited session on "Human error in dynamic systems", Lille France, July 9-12, 1996.

Frese, M.; Zapf, D. (Eds.) (1991). *Fehler bei der Arbeit mit dem Computer*, Bern: Huber.

Hacker, W. (1986) *Arbeitspsychologie*, Bern: Huber.

H , N.W.S. van der; Schaaf, T.W. van der (1995). Risk management in Hospitals: Predicting versus Reporting Risks in a Surgical Department. In: *Proceedings of the XIV European Annual Conference on Human Decision Making and Manual Control*, (Stassen, H.G.; Wieringa, P.A. (eds.)), Delft University of Technology, Delft.

Mulder, A.M.; Schaaf, T.W. van der (1995). Near misses as Accident Precursors. In: *Proceedings of the XIV European Annual Conference on Human Decision Making and Manual Control*, (Stassen, H.G.; Wieringa, P.A. (eds.)), Delft University of Technology, Delft.

Perrow, C. (1984). *Normal accidents: living with high-risk technologies*, Basic Books, New York.

Rasmussen, J. (1986). *Information processing and human-machine interaction*, Elsevier Science Publishers, Amsterdam.

Reason, J.T. (1990). *Human Error*, Cambridge University Press, Cambridge.

Schaaf, T.W. van der (1988). Critical incidents and human recovery. In *Human recovery: Proceedings of the COST AI Seminar on Risk Analysis and Human Error*, (Goossens, L.H.J., (ed)), Delft University of Technology.

Schaaf, T.W. van der; Lucas, D.A.; Hale, A.R. (eds.) (1991). *Near miss reporting as a safety tool*, Butterworth Heinemann, Oxford.

Schaaf, T.W. van der (1991).Development of a near miss management system at a chemical process plant. In: *Near miss reporting as a safety tool*, (Schaaf, T.W. van der; Lucas, D.A.; Hale, A.R. (eds.)). Butterworth Heinemann, Oxford.

Schaaf, T.W. van der (1992). In: *Near miss reporting in the chemical process industry*, Ph.D Thesis, Eindhoven University of Technology

Vuuren, W. van (1995). Modelling organisational factors of human reliability in complex man-machine systems. In: *Proceedings of the XIV European Annual Conference on Human Decision Making and Manual Control*, (Stassen, H.G.; Wieringa P.A. (eds)). Delft University of Technology

Zapf, D.; Frese, M.; Irmer, C.; Brodbeck, F.C. (1991). Konsequenzen für die Softwaregestaltung. In: Frese, M.; Zapf, D. (Eds.), *Fehler und Schwierigkeiten bei der Arbeit mit dem Computer*, Ergebnisse von Beobachtungen und Befragungen im Bürobereich. Bern: Huber.

Zapf, D.; Lang, T.; Wittmann, A. (1991). Der Fehlerprozeß. In: Frese, M.; Zapf, D. (Eds.), *Fehler und Schwierigkeiten bei der Arbeit mit dem Computer*, Ergebnisse von Beobachtungen und Befragungen im Bürobereich. Bern: Huber.

Zuijderwijk, M. (1995). *Near miss reporting in reliability management*, M.Sc thesis, Eindhoven University of Technology.

Finally, relating to question 4, figure 4 shows that hardly any recovery process goes through the more analytic localisation phase. Again, this could be interpreted as confirmation of Reason's GEMS model, but there is also the possibility of an explanation in terms of time stress. If recovery is present only in the very last phase of accident development (as was the case in most of the steel plant near misses) there may simply not be enough time for a time-consuming diagnostic effort; detection and correction 'just-in-time' may be all one can do in such cases.

5. Implications for MMS design

In spite of the immaturity of the proposed models and classifications, and of the small number of recovery incidents gathered so far, these ideas and results are intriguing enough to formulate the following tentative implications for designing a MMS:

* Consider recovery promotion and error management as an alternative to failure prevention, especially when certain errors or failures are predictably unavoidable.
* Do not simply "design out" failure factors without considering the possible reduction of recovery factors: raising the level of automation in process control, or installing too many decision support tools for your operators, may leave them helpless under certain situations.
* Try to support all recovery phases, primarily by means of an optimal man-machine interface: detection, localisation and correction (see section 2.4.4).
* Invest in deep process knowledge of operators: reasoning beyond procedures appears to be essential for many recovery actions. Error management supported by error training seems to be an adequate way to enhance the ability to deal quickly and efficiently with errors.

Acknowledgement

The presentation of this paper was supported by a CEC Human Capital and Mobility Network on Human Error Prevention.

References

Brinkman, J.A. (1990). *The analysis of fault diagnosis tasks: Do verbal reports speak for themselves?*, Ph.D Thesis, Eindhoven University of Technology.

Dorman, T.; Frese, M. (1994). *Error training: Replication and the function of exploratory behaviour*, International Journal of Human-Computer Interaction, 6, p. 365-372.

Embry, D.E. and D.A. Lucas (1988). The nature of recovery from error. In: *Human recovery: Proceedings of the COST AI Seminar on Risk Analysis and Human Error*, (Goossens, L.H.J., (ed)), Delft University of Technology.

Frese, M. (1991). Error management or Error prevention: Two strategies to deal with errors in software design. In: *Human aspects in computing: Design and use of interactive systems and work with terminals*, (Bullinger, H.J., (ed.)), Elsevier Science Publishers, Amsterdam.

Frese, M.; Brodbeck, F.; Heinbokel, T.; Mooser, C.; Schleiffenbaum, E.; Thiemann, P. (1991). *Errors in training computer skills: on the positive function of errors. Human-Computer Interaction*, 6, p. 77-93.

4.3 Reliability and environmental incidents in an energy production plant

In a small energy producing unit of a chemical plant Zuijderwijk (1995) classified failure and recovery root causes of 23 reliability and environmental near misses (fig. 7 and 8)

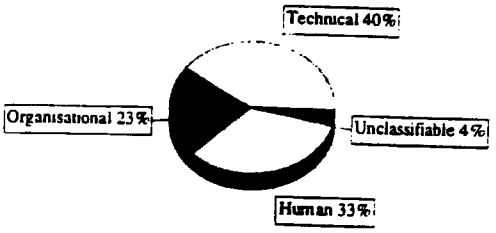


Fig. 7.:Distribution of 86 failure factors in 23 reliability and environmental incidents in an energy production plant.

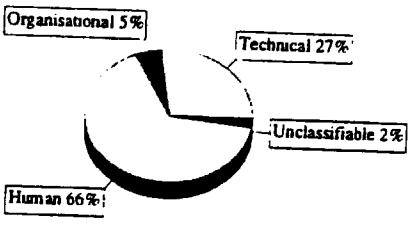


Fig. 8.:Distribution of 56 recovery factors in 23 reliability and environmental incidents in an energy production plant.

4.4 General discussion of the pilot studies

Figures 3, 6 and 8 show a range of 2 to 11 percent of unclassifiable causes (that is: luck or coincidence) of recovery. This must be interpreted as a positive answer to question 1: around 90 percent or more of all recovery factors are clearly technical, organisational or human in nature and therefore researchable and eventually manageable.

The same figures show human recovery root causes contributing 21 to 66 percent. Comparison with the failure factors of figures 2, 5 and 7 shows this human recovery range to vary at least as much as the human failure range (e.g. 33 to 56 percent). The human component should therefore also be taken seriously in terms of recovery possibilities (see question 2). This result can be seen as an additional argument for the implementation of error management in every work related training situation. If the role people play in preventing serious accidents is this big, they should be trained more rigorously in dealing efficiently with errors. Empirical results of studies in error training (Frese, Brodbeck, Heinbokel, Mooser, Schleiffenbaum & Thiemann, 1991; Dorman & Frese, 1994) have shown that error training in contrast to error avoidance training leads to higher performance. Error training means allowing and encouraging people to make errors in the training process and ultimately encouraging them to learn from these errors. As a result subjects who received error training have shown fewer errors and performed better, even in other areas of performance.

Zuijderwijk (1995) showed that the patterns of failure and recovery factors are clearly different. Rule- and skill-based factors dominate the operator failures, while knowledge-based insights are very important in human recovery. Similarly, 'material defects' are the most prominent technical failures, while 'design' covers all technical recovery factors (see question 3).

4. Pilot studies

Pilot studies have recently been carried out in steel making, energy production and surgery. A variety of system effects have been investigated: safety, reliability and environmental effects of system breakdown.

4.1 Safety incidents in a steel plant

In a Dutch steel plant Mulder and Van der Schaaf (1995) identified failure and recovery factors in the same set of 25 safety-related near misses. The results are given in fig. 2-4.

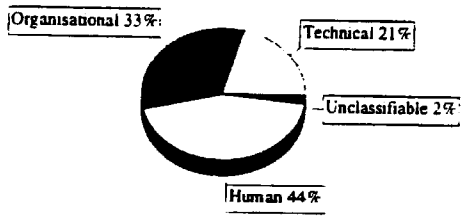


Fig. 2.:Distribution of 154 failure factors in 25 safety incidents in a steel plant.

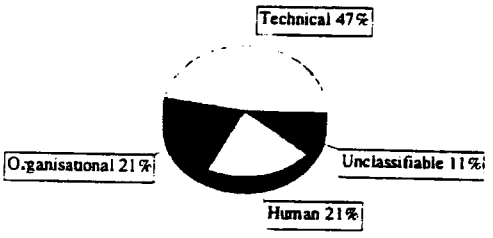


Fig. 3.:Distribution of 34 recovery factors in 25 safety incidents in a steel plant.

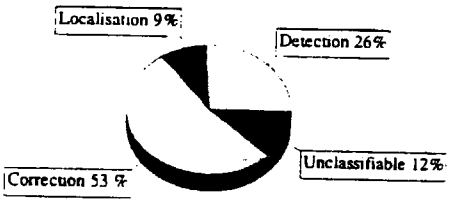


Fig. 4.:Distribution of 34 recovery factors according to recovery phase in 25 safety incidents in a steel plant.

4.2 Medical safety incidents in a surgical ward

In a large teaching hospital in Eindhoven Van der Hoeff and Van der Schaaf (1995) found the following failure and recovery factors in the same set of 17 medical near misses with patients undergoing surgery (fig 5 and 6).

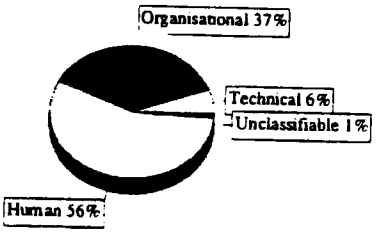


Fig. 5.:Distribution of 95 failure factors in 17 medical incidents with patients undergoing surgery.

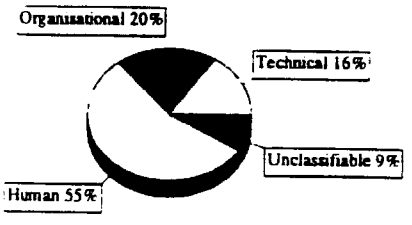


Fig. 6.:Distribution of 22 recovery factors in 17 medical incidents with patients undergoing surgery.

2.4.3 Classification according to type of recovery factor

Such a classification should be the most important one for MMS-designers. The ECM for failure root causes could serve as a basis for recovery root causes too, with the following extensions:

* Technical design of the process:
  aim at maximum reversibility of process reactions (Rasmussen, 1986) and 'linear interactions' plus 'loose coupling' (Perrow, 1984) of process components; these may be achieved by structural characteristics (e.g. buffers, parallel streams, equipment redundancy) and by dynamic characteristics (e.g. speed of process reactions, response delays).
* Technical design of the man-machine interface:
  aim at maximum observability (Rasmussen, 1986) of deviations and their effects (e.g. transparency instead of alarm inflation).
* Organisational and management factors:
  particularly an updated, clearly formulated and well-accepted set of operating procedures and a positive safety culture must be mentioned here (see also Van Vuuren, 1995).
* Human operator factors:
  optimize the cognitive capabilities (e.g. accurate mental process model) of operators through selection and (simulator-) training, but also by supporting them with software tools to test hypotheses and avoid certain biases.

2.4.4 Classification according to recovery process phase

As mentioned earlier in 2.2 this final classification aims to distinguish between detection, location and correction as the phases of impact of the recovery factors in 2.4.3.

3. Empirical research questions

Based on the proposals in section 2, the human recovery research project of the Eindhoven Safety Management Group is directed at the following empirical research questions:

1. Is recovery more than sheer luck or coincidence? If so, then the potential for recovery can be built into a MMS and managed!
2. Can recovery be classified with the same ECM root causes as for failures? If so, what is the contribution of human recovery relative to technical and organisational failure barriers? How large is the contribution of human recovery in a variety of task situations and over a variety of system effects?
3. Are recovery factors identical to failure factors in a given MMS? If so, then preventing errors and promoting recovery would focus on the same MMS aspects.
4. In which phase(s) of the recovery process do recovery factors contribute most to system performance: symptom detection, fault localisation or correction?

2.4 Classification of human recovery aspects

The preceding sections lead to the following four ways of classifying (human) recovery aspects: according to the preceding failure(s), according to the human operator's reaction after detecting an initial deviation or symptom; according to the type of recovery factor (or recovery root cause); and according to the phase in which this recovery factor makes its main contribution.

2.4.1 Classification based on preceding failure

Both the ECM (see section 2.1) and Embrey and Lucas (1988) provide the rationale for this taxonomy. Technical, organisational and human root causes of failures may be linked with their subsequent recoveries. Additional subcategories might include: recovery from one's own error, or from a colleague's (same or previous shift, when applicable); technical failure of equipment outside the central control room (CCR), of the interfaces within the CCR, of process control software, etc.
An error taxonomy developed by Frese and Zapf (1991) includes several different types of errors structured by the levels of regulation (sensorimotor level, level of flexible action patterns, and intellectual level) and the steps in the action process (goals, planning, monitoring, and feedback) according to the Action Theory (Hacker, 1986). Thus the taxonomy includes sensorimotor errors, habit errors, omission errors, recognition errors, thought errors, memory errors and judgement errors.

2.4.2 Classification according to operator reaction after symptom detection

As noted by Reason (1990) in his GEMS model people seldom go through the entire analytic process of fault diagnosis when confronted with a deviation. This was confirmed by Brinkman (1990) who collected verbal protocols during a fault finding task. He observed the following three reactions after his subjects detected an error in their reasoning process:

* Ignore the error and continue:
  rely on system redundancy and subsequent error recovery factors.
* Simply repeat the most recent sequence of actions:
  try again, without any attempts at fault localisation.
* Attempt fault localisation and optimize corrective actions:
  either by forward analysis (repeat the most recent action sequence and check every step) or backward analysis (trace back from symptom detection to previous actions, until the error is found).

By applying this classification, transitional probabilities between the recovery phases of section 2.2 might be established.

1. Systems should decrease the error detection time (error detection phase): More negative consequences will occur if errors are not detected early. Thus, the sooner the error is detected, the better for error management. Error training can decrease the time between error occurrence and error detection by increasing awareness of how many errors one makes.
2. Systems should facilitate one's understanding of errors (error explanation phase): Although it is not absolutely necessary to know why an error occurred often good error explanation helps to handle errors quickly. Systems can facilitate good error explanation by being transparent and by giving helpful feedback.
3. Systems should reduce error handling time (error handling phase): Zapf, Frese et al (1991) have described various supports for error management in software design. This includes memory aids (e.g. history function), backups, making additional actions possible without loosing track of what one was doing before (e.g. with a window technique), easy access to a known starting point (e.g. with the ESCAPE key), undoing functions (e.g. unerase), direct correction (e.g. insert function), support for error search and correction (e.g. language checks), and support for active exploration (e.g. tutorials).

2.3 Dependency of recovery on preceding errors

Embrey and Lucas (1988) discuss several factors affecting the probability of recovery from error and the error detection lag. This relationship is highly relevant to understand the role of feedback in the recovery mechanism. Their main points may be summarized as follows:

* Causes of skill-based slips and lapses are relatively unrelated to subsequent recovery factors; their human recovery probability is high and the error detection lag will be small.
* For rule- and knowledge based mistakes the opposite holds: their recovery factors depend on the same preceding failure factors; probability of recovery is small and the error detection lag is large.

The main reasons for these predictions given by Embrey and Lucas (1988) include feedback related aspects and cognitive limitations: the awareness of an error possibility and the visibility of its effects are high for slips and lapses, but low for mistakes while cognitive limitations (e.g. confirmation-, fixation- and groupthink biases) would be small for slips and lapses, but large for mistakes. For the present paper the main implication is that the nature of the preceding human error(s) should be highly predictive of any subsequent recovery.

Another feedback related aspect of errors is error messages. Zapf et al (Zapf, Frese, Irmer & Brodbeck, 1991) emphasize that good error messages should conform to the following criteria: they should be quite visible and salient, informative, easy to understand, orient the user to further actions, and be polite and short.

These failure factors (or root causes) have so far been modelled successfully by the Eindhoven Classification Model (ECM) of system failure (Van der Schaaf, 1991, 1992; Van Vuuren, 1995). In the pilot studies mentioned in section 4 of this paper, the ECM subcategories will not be used, only the main groups of Technical (T), Organisational and Management (O), and Human operator (H) failure factors will be referred to.

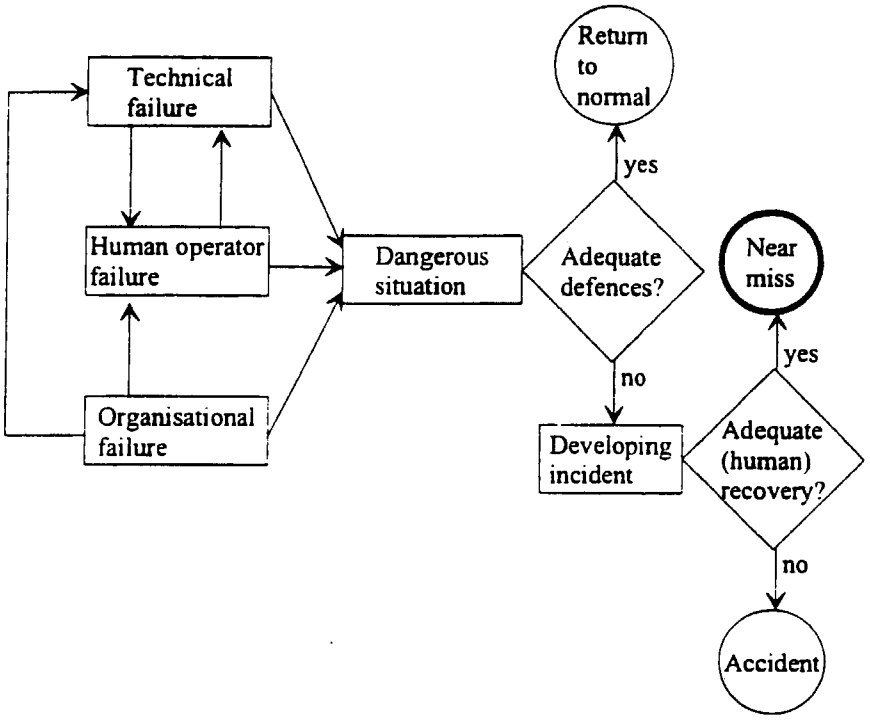


Fig. 1. The incident causation model.

2.2 Human recovery process phases

Van der Schaaf (1988) proposes that human recovery be defined as "the (unique?) feature of the human system-component to detect, localize and correct earlier component failures. These component failures may be either his or her own previous errors (or those of colleagues) or failing technical components (hardware and software)". This definition implies the following phases in the recovery process:

* Detection: of deviations, symptoms, etc.,
* Localisation: of their cause(s) (diagnosis in the strictest sense),
* Correction: of these deviations by timely, effective counter actions, after which these deviations are nullified and the system returns to a stable status.

In the theoretical framework of error management (Frese, 1991), these three phases in the recovery process correspond to the phases in the general error process: error detection, error explanation and error handling. The concept of error management (or error training) can be seen as an alternative to error prevention. The focus of this new approach is to avoid negative error consequences, to deal quickly with error consequences once they occur and to reduce future errors. Thus, an important distinction between the error per se and the error consequences has to be made. From this error management perspective three implications for system design can be deduced:

Then, the process of human recovery is described. It consists of three phases: detection of symptoms, localisation of their cause(s) and correction which returns the system to its normal status. A short introduction into the error management concept (Frese, 1991) is given.

The following section deals with the relationship of human error causes and the probability of recovery, and with the error detection lag. These theoretical predictions are mainly based on well known cognitive limitations and feedback-related aspects of the task situation. Implications for software design concerning criteria for error messages are mentioned (Zapf et al, 1991).

Four ways of classifying (human) recovery in actual process control situations are proposed, The first classification deals with the type of preceding failure(s), for instance technical, organisational or human failure respectively, with the error taxonomy developed by Frese and Zapf (1991). Another way to look at human recovery is to distinguish the reaction after symptom detection: ignore the deviating status, repeat a sequence of actions, or attempt fault localisation and correction. Thirdly and most importantly, the factors in the man-machine system that triggered or enabled recovery are categorized: technical factors related to process design (for instance to allow for reversibility), or interface design (e.g. to maximize observability of symptoms and effects); the organisational and management context (e.g. proper procedures, positive safety culture) and operator factors (e.g. accurate mental models). The fourth classification locates the phase in which a recovery factor primarily contributes to the recovery process: detection, localisation or correction. These theoretical approaches are subsequently translated into the specific empirical research questions on which this project is focusing.

Finally the results of recent pilot studies in the energy production and steel industry, as well as those of medical errors in a surgical ward will be presented and their implications for designing recovery into man-machine systems will be discussed.

2. Theoretical approaches

2.1 Incident causation model

In Van der Schaaf (1992), a simple incident causation model is used (see fig. 1) to define accidents, near misses and their common root causes consisting of technical, organisational and human (operator) factors. When incident development cannot be stopped by the system's predetermined barriers and lines of defence, the only distinguishing factor between an accident and a near miss effect is the presence or absence of successful 'accidental' or unplanned recovery.

Although actual accidents may also contain attempts at recovery, it is obvious that near misses as defined above are the optimal source of data to study the phenomenon of recovery as the positive counterpart of failure.

HUMAN RECOVERY AND ERROR MANAGEMENT

T.W. van der Schaaf

Safety Management Group
Eindhoven University of Technology
P.O.Box 513, Pav. U-8
5600 MB Eindhoven, The Netherlands

M. Frese
D. Heimbeck

Department of Psychology
University of Amsterdam
Roetersstraat 15
1018 WB Amsterdam, The Netherlands

Abstract

This paper highlights the positive role that human operators often play in preventing small failures and errors from developing into an actual system breakdown. The resulting 'near misses' may provide an insight into a powerful alternative to human error prevention, namely human recovery promotion and error management. Theoretical approaches to modelling error recovery are discussed and translated into empirical research questions. These are partly answered by a number of pilot studies. The main conclusions are that error recovery is much more than simple luck or coincidence, that root causes can be identified, and that these should have design implications for the technical and organisational context of the human operator's task as well as for an alternative training concept of error management.

1. Introduction

The research project described in this paper focuses on the positive role that human operators often play in preventing an ongoing sequence of usually small failures and errors from developing into an actual total system breakdown or accident. This new concept of human recovery may provide designers, managers and researchers with a powerful alternative approach to the traditional one of human error prevention in process control, namely: human recovery promotion and error training.

First, a simple incident causation model is presented in which the presence or absence of successful human recovery plays a decisive role in determining the effects of process deviations, technical failures and errors on the safety and reliability of man-machine systems (MMS's).