Recovery from failures -understanding the positive role of human operators during incidents

Lisette Kanse & Tjerk van der Schaaf

Eindhoven University of Technology

The Netherlands

Abstract

The basic focus until now of reliability-, performance- and quality management has been on the prevention of failures and errors. Yet, in fact it is rather the negative consequences of a failure that we want to prevent, than the occurrence of an initial failure itself. This idea introduces a relatively new research area, focussing on the recovery -, or failure compensation process, which takes place (either successfully or not) after a failure has occurred and which contributes to the (complete or partial) prevention of negative consequences.

There are only a few scientific publications in which the failure compensation process plays a central role. In almost all of these, the importance of the human factor for recovery is stressed. In the failure compensation process, three phases can be distinguished, about which general agreement exists: *detection* (of the symptom(s), indicating that something has gone wrong), *explanation* or *localisation* (of the failure's causes) and *correction* (of the problem through planning and execution of ad-hoc/structural countermeasures).

The purpose of this paper is to discuss the development of a comprehensive model of the failure compensation process and the factors influencing recovery, based on findings from a literature survey and an exploratory pilot study involving incident data from a chemical process plant. The resulting insights provide a basis for organisation and system (re)design in

order to promote recovery possibilities, and underline the importance of learning positive, effective ways of dealing with errors when they occur.

Introduction

While the *negative* role a human operator can play in overall system performance has long been recognised in safety and reliability management, as can be seen from the vast amounts of research focussing on human error and its prevention, relatively little attention has been given to understanding the *positive* role that the same human operator can have in returning a system to its normal and safe state after a failure has occurred. In many areas of work / industry, after an initial error (human failure) or other type of failure has occurred, there is in most cases still a chance to recover from the failure through the timely and effective application of countermeasures. The aim of these countermeasures is to avoid the negative consequences to which the failure would otherwise lead. Depending on their effectiveness and timeliness, the countermeasures can be completely successful or only partially. The first case results in a near miss, whereas the second case still results in an accident, but the severity of the outcome may well have been reduced by the countermeasures. The detection that a failure has occurred, combined with problem diagnosis and the identification and application of countermeasures, is called the failure compensation process. Initial research (e.g. Van der Schaaf & Kanse, 2000) focussing on failure compensation has shown that especially for unforeseen failures, human operators play a very important role in the identification and application of appropriate countermeasures.

A better understanding of the failure compensation process will provide additional ways to improve system safety and reliability, which can be used in conjunction with the more traditional methods that focus on error prevention. Since the late eighties and early nineties, a small number of researchers in the domain of human reliability realised the importance of

understanding the processes followed to recover from errors and other failures, and the factors that influence these processes. The research they performed was done both in laboratory settings and sometimes also in the real world, in various domains such as aviation (Wioland & Amalberti, 1996), human-computer interaction (Brodbeck et al., 1993; Zapf et al, 1994; Frese, 1991; Rizzo et al., 1987; Bagnara et al., 1988), hospitals (Edmondson, 1996), and everyday tasks (Sellen, 1994).

In the failure compensation process, three phases can be distinguished, about which general agreement exists among researchers in this domain (e.g. Zapf & Reason, 1994; Kontogiannis, 1999; Van der Schaaf, 1988): *detection* (of the fact that something has gone wrong, a failure has occurred), *explanation* or *localisation* (of the causes of this failure) and *correction* (of the problem through planning and execution of countermeasures). Most of the existing research has focussed on the detection phase (e.g. Sellen, 1994), which is important since, after all, no corrective actions will be initiated for failures that remain undetected.

In the failure compensation process, a distinction can be made between planned and unplanned counteractions applied to avoid negative consequences of failures. For foreseen problems and failures, counteractions can be planned and can be built-in in the system as automatic safety controls, or procedures to follow under certain conditions, and so on. These planned counteractions are referred to as *defences*, or *barriers*. A detailed discussion of barrier systems (how the barrier is implemented) and functions (what is the aim of the barrier, how does it work) is given by Hollnagel (1999). Svenson (1991) has also provided more insight in barrier functions. For those cases where no defences are available or when the defences don't work properly, there is still the possibility for unplanned counteractions that have not been foreseen in the system. These counteractions are referred to as *recovery* actions and most often involve ad-hoc, creative thinking and actions by the human operator(s) in a system.

This paper is based on the first steps undertaken in a research project focussing on the failure compensation process and how people recover from failures. The overall aim of the research project is to gain more insight in the failure compensation process and all the factors influencing this process (either in a positive or negative manner). This insight can serve as the basis for the development of new, additional methods to improve safety, reliability and system performance, through which recovery will be optimally supported. The first steps of this research project include an analysis of existing literature in the domain of failure compensation, and a pilot case study performed at a chemical process plant involving near miss and incident data. The aim of the literature survey and the pilot study is to find a preliminary answer to the following questions:

- *how does the process followed for failure compensention work?*
- *which factors influence this failure compensation process?*

To answer these questions, a preliminary failure compensation process model and recovery influencing factors taxonomy will be developed, based on insights gained during the initial project steps.

Even though the pilot study has not been completed yet, the literature collected until now allows some preliminary conclusions, and some results are already available from the work done so far. In the literature, two quite comprehensive models of the failure compensation process can be found, next to several detailed models or descriptions of specific parts or aspects of the overall failure compensation process. One of these two more comprehensive models is centred around user strategies in error recovery (Kontogiannis, 1999) and another is based on the 'Incident Causation Model' and 'Eindhoven Classification Model of System Failure' (Van der Schaaf, 1992; and later version by Van Vuuren, 1998). The applicability and usability of these two models have been evaluated based on near miss and incident data collected during the pilot study at a chemical process plant. For this evaluation, and, more importantly, as a starting point for the development of a preliminary process model of the

failure compensation process and a taxonomy of recovery influencing factors, requirements have been specified based both on literature survey findings and the pilot study data.

In the next section, the approaches used during the pilot study for data collection and analysis of near misses and incidents will be discussed. After that, the identified requirements for the development of a preliminary failure compensation process model and recovery influencing factors taxonomy will be listed. Consequently, the preliminary process model and an initial list of factors influencing recovery will be presented, which have been developed based on the above-mentioned requirements and all insights gained so far. The last section of this paper will contain some concluding remarks regarding the need for additional research in the domain of failure compensation, or more specifically, recovery.

The methods used in the pilot study

For the development of a preliminary failure compensation process model and to gain insight in the factors that influence this process, a pilot case study is currently undertaken in a chemical process plant, during which incident and near miss data are collected. Incident data about real accidents (where any attempt at recovery has not been successful) as well as about near misses (with successful recovery) is included in the research project. This chemical process plant has successfully established a near miss reporting system that has been operational for six years. Via this system, near misses, dangerous situations and incidents are reported using reporting forms on which time, date, and location of the incident, and a few lines containing a description of what happened, how this could happen, potential consequences, actions taken and recommendations are recorded. The reports are entered into a computer-based incident and near miss database by safety department members. This database is also used by the safety department to identify areas in need of attention, based on the analysis of factors that played a role in larger sets of near misses and incidents combined

over a longer period of time. Other examples of the use of this database include the assessment of the effects of implemented safety measures. Key factors for the success of this system are the ‘no blame’-culture of this company regarding errors, the anonymity of the reports once analysed for their root causes and entered into the database, and the quick follow-up by the appropriate personnel in response to the reports.

The incident/near miss reporting forms that are used in this company form the basis for the data collection process. Follow-up interviews are held with those involved in the incident or near miss to obtain additional information. A data collection proforma has been developed to use for documenting the analysis of the incident or near miss. This is to ensure that the same type of data is collected for each incident. The proformas can be partially completed based on the initial incident reporting forms, additional data are added afterwards during the interview – so the proformas also provide a structure for the follow-up interviews. The data collection proformas, once completed, are reviewed for correctness and completeness by the person(s) interviewed plus local domain experts. So far the pilot study includes all the reported near misses, incidents and accidents within a time frame of three and a half weeks, plus some earlier reports used to determine what data to collect and how. Currently 56 reports have been included in the pilot study, covering a wide variety of types of incidents, with regard to possible consequences, the success or failure of recovery, the amount and type of people involved, activities and department(s) involved, time available and used for recovery, and so on. During the next couple of months following the above-mentioned three and a half weeks, new reports will be added to the pilot study if they involve a failure compensation process that appears to be different from any process previously included and analysed. Since the sample of reports used in the pilot study is predominantly a convenience sample, no statistics will be given regarding for instance the relative occurrence of different types of recovery, or recovery strategies, and factors contributing or hindering recovery. The aim of the pilot study, after all, was basically to develop a preliminary model that best describes all types of possible failure compensation processes, and this aim has dictated the sampling process.

The failure compensation process data collection proformas have been designed to collect data about failure compensation processes and factors influencing recovery. In order to obtain insight in all factors that may be relevant for recovery, data are recorded about both the events preceding the failure compensation process and the failure compensation process itself:

- the preceding failure(s)/error(s) (failure process), since it has been indicated that a relationship exists between recovery influencing factors and human recovery behaviour patterns on the one hand, and preceding failure types on the other (Embrey & Lucas, 1988)
- the functioning (or not) of defences built-in in the system
- the recovery process followed
- where applicable, the remaining negative consequences of the failure(s)/error(s), to establish the success of the recovery actions
- possible consequences if recovery would not have been successful, to establish the urgency of the need for recovery and the importance of recovery.

Based on the difference mentioned in the introduction, between barriers and defences used for foreseen failures or problems, and ad-hoc recovery actions for unforeseen problems and situations where barriers or defences do not exist or do not work, in the data collection proformas a distinction is made between planned and unplanned counteractions applied to avoid negative consequences of failures. The unplanned counteractions or recovery actions form the core of this research project.

The failure compensation process data collection proforma in its current form consists of two parts. The first part aims at a description (what, where, when & who) of the failure process (initial error(s) or failure(s)), the working of possible built-in defences, the recovery process followed and if relevant, the remaining negative consequences. The second part is more

analytic in nature and focusses on the questions *why* and *how* surrounding the complete process from initial failure(s), through defences and recovery actions, to possible remaining negative consequences.

To answer those *how* and *why* questions regarding the failure and compensation processes, the causal tree incident description technique has been used, which has successfully been applied before (Van Vuuren, 1998; Van der Schaaf, 1992) for the identification of the root causes in failure processes. For the analysis of failures (and also for those cases where planned counteractions, or defences or barriers failed to work), this technique can be applied without changes. For the analysis of (both the planned and unplanned parts of) the failure compensation process, an adapted version of the causal tree technique has been developed, to avoid excluding potentially relevant information about timing and sequences of actions and other contextual factors which a regular causal tree would normally not include. An illustration of the structure of the failure compensation process-causal tree is provided in figure 1. Of course the following order in, and the exact shape of the tree will vary for different incidents and near misses. Also, the failure compensation actions belonging to each of the process phases can be broken down in more detail, especially if more actions are performed within one phase, before the factors are identified that influenced those specific actions.

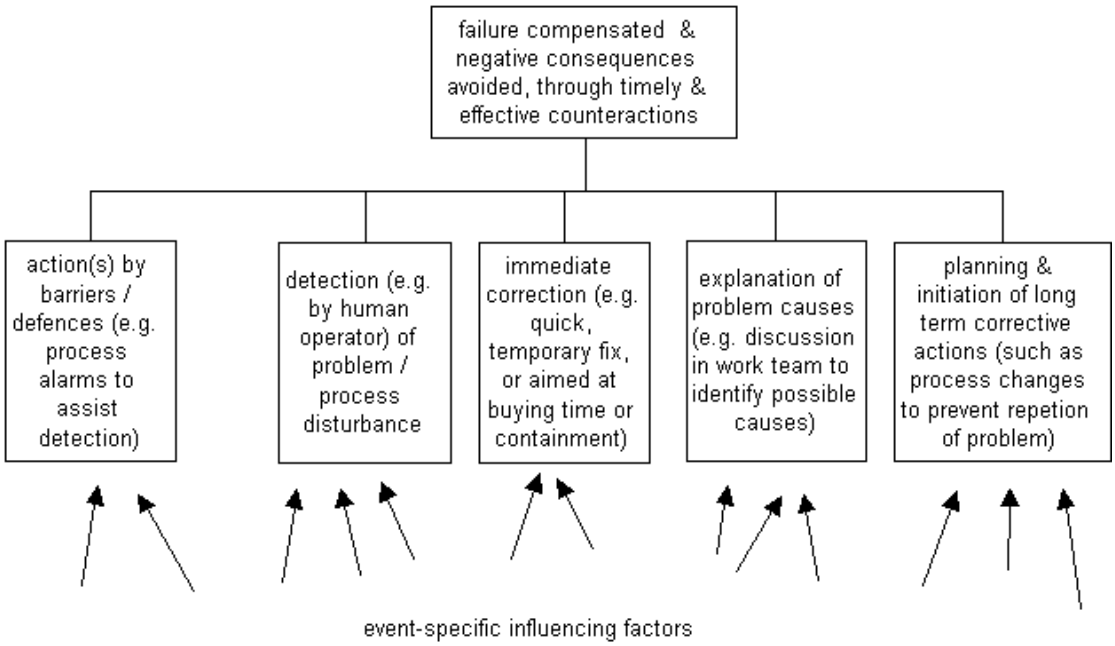

Figure 1: Example layout for causal tree of failure compensation process (barriers and recovery combined)

Implications of insights gained so far

Based on insights gained so far during the first steps of the research project a number of implications for the development of a model of the failure compensation process and the factors influencing this process have been identified. In this section these implications will be presented in the form of a list of requirements for a comprehensive model of the failure compensation process and a recovery influencing factors taxonomy.

An important finding is that the failure compensation process model needs to be flexible with regard to the three phases of the process, namely detection, localisation and correction. Analysis of incident and near miss data in the pilot study has shown that the following order

of these phases is not always the same. In fact, the more analytic localisation phase does not necessarily occur immediately after detection of a problem. Often a quick fix is required to avoid immediate consequences, so an initial, short-term correction may occur even before an analysis is made of possible causes of the detected failure. A more in-depth localisation may (or may not!) follow when more time is available after the quick fix. At that stage, a planning is made for more permanent corrections which will be executed on the longer term.

The model also needs to provide the possibility to cover different kinds of near misses and incidents, with varying amounts of time spent on and available for the different recovery phases, varying possible failure consequences, and varying amounts and types of people involved in each phase. While in the analysed near misses and incidents, in the detection phase most often only one person was involved, most often more people participated in the localisation phase, mostly colleagues from the same operating team. Correction, especially long-term correction, often involved different people again. Examples are people who have to assess the necessity of process changes to improve certain situations, or maintenance people specialising in specific parts of the process installations and – equipment, or even contractors from outside the organisation who can provide specialist skills and tools for certain corrective actions. The model needs to enable the inclusion of more actors in the recovery process.

The distinction that has been made during data collection in the pilot study, between planned and unplanned counteractions, has been useful for the identification of those countermeasures that were the result of exclusively the combination of skills, knowledge and experience of human operators, without any contribution of or intervention by defences or barriers built-in in the system. In many of the analysed incidents and near misses, however, a combination of both planned counteractions and unplanned counteractions played a role. For example situations where an alarm given via the process control panel triggers corrective actions planned and executed by human operators, actions that are not prescribed in work instructions but that have to be tailored in an ad-hoc manner to the specific characteristics of the system

status and environment at that moment. In such situations detection is triggered by planned countermeasures (the alarm), but the rest of the recovery process relies on unplanned counteractions. This leads to the requirement for the failure compensation process model to be able to incorporate both types of countermeasures in a rather flexible manner, without assigning a fixed sequence to them (such as defences first, unplanned counteractions only afterwards), while still keeping the possibility of differentiating between the two types.

Another conclusion that can be drawn based on the incident and near miss data analysed so far, with regard to the factors that influence the recovery process, is that even though some of the factors appear to influence each of the recovery process phases (such as time available), another number of factors are specifically relevant for one of the phases, or possibly two, but not all phases equally. The way in which feedback is presented for example influences observability of failures and influences the chance that a failure is detected. The localisation phase is influenced by the traceability of the preceding failure processes, aiming at an explanation for what has happened. And the reversibility of the system in which the human operator performs his job, will affect the probability of a successful correction phase. An overview or taxonomy of the factors influencing recovery can either be incorporated in the recovery process model or be developed as a separate overview, as long as the link between type of influencing factor and recovery process phase remains visible.

Figure 2 contains a preliminary model of the failure compensation process that has been developed to conform to the above-mentioned requirements.

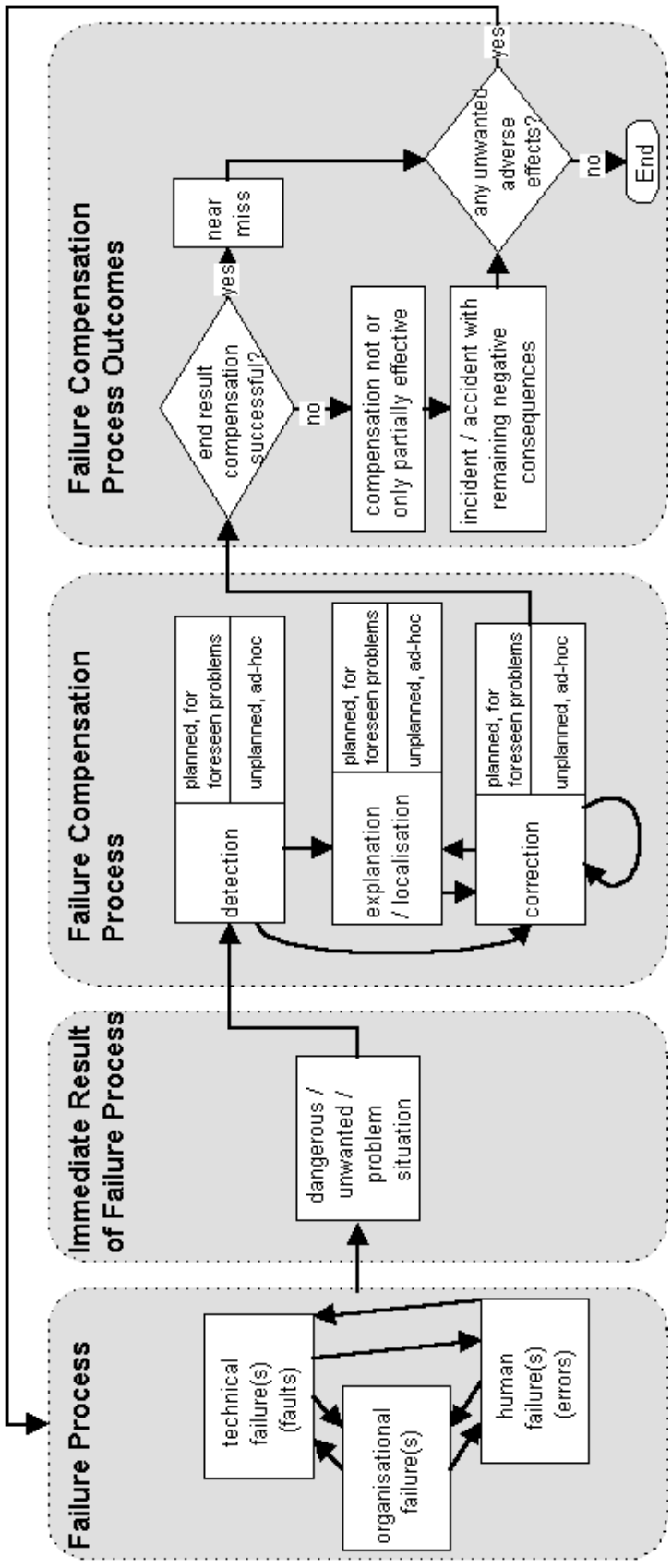

Figure 2: Preliminary failure compensation process model

Based on the insights gained both in the pilot study and the literature survey, a preliminary list of recovery influencing factors has been developed. Table 1 contains the current version of this list. Referring back to figure 2, these factors influence the third shaded box: the process followed for failure compensation. The connection between influencing factors and failure compensation process phase has not been made yet. In order to identify which factors specifically influence which phase, hypotheses still need to be formulated and tested in further research. A tentative categorisation of the recovery influencing factors has been made into six groups: factors relevant for prioritisation of recovery related tasks, occurrence related factors, person related factors, social factors, organisation factors, and technical/workplace/situational factors.

Table 1: List of recovery influencing factors

Factors relevant for prioritisation of recovery related tasks
time available for recovery task, considering other tasks requiring attention
urgency of recovery (amount of time until negative consequences arise)
importance of or need for recovery (seriousness of possible consequences if not recovered)
Occurrence related factors
type(s) of preceding failures
performance phase in which the immediate result of the failure process is detected (during planning phase / while carrying out the action / when outcome of the action is observable)
available applicable barriers/defences
Person related factors
overall process/plant (work area) knowledge
work area and process related skills
general competency in own specific job
competency in task concerned
competency with regard to specific problem occurrence
competency in problem solving tasks in general
time elapsed since last (re)training in work area/task concerned
time since last (re)training with regard to specific problem occurrence
time since last (re)training in problem solving in general
suspicion/distrust/intuition
personal attitude towards failures and failure compensation
error coping strategies
self efficacy (conviction/trust in own ability)
fatigue
shift work coping ability
feeling of personal responsibility for the failure or problem
feeling of personal responsibility with regard to recovery

pride regarding a job well done
Social factors
team attitude towards failures & failure compensation
attitudes towards co-operation with team members
team efficacy
feeling of team responsibility for the failure or problem
feeling of team responsibility with regard to recovery
Organisational factors
availability of team members/colleagues
organisation of work and responsibilities
training plan
competency assessment plan
supervision
personnel selection processes
availability, quality and usability of procedures/work instructions
shift patterns and/or personnel planning
organisational policy
management attitudes towards failures & failure compensation
Technical/workplace/situational factors
availability of equipment/materials needed
operator-process interface properties

As may already be obvious from a glance through the factors listed above, not all factors have an equally direct influence on the recovery process and the likelihood of successful recovery. For example, employee competencies will be influenced both by the selection and training processes and the ways in which competencies are assessed. Also, whether social or team factors play an important role or not depends on work organisation. If no task interdependency and co-operation exists, this may influence the available types of recovery possibilities. Another important thing to note is that this table is based on a case study in the chemical process industry. Factors which make perfect sense in such an environment, like shift patterns, may not be relevant in other types of organisations and work environments.

Conclusions

As can be seen from the previous sections, initial insights in (parts of) the failure compensation process in a variety of settings have already been produced by a small number of researchers. The pilot study described in this paper provided additional insights. The preliminary model and influencing factors taxonomy presented here provide an initial answer to the questions ‘how does the process followed for failure compensention work?’ and ‘which factors influence this failure compensation process?’.

We have seen that the failure compensation process includes both planned (barriers) and unplanned (recovery) countermeasures and that it consists of the phases detection, localisation and correction (and that localisation and correction phases may be repeated and do not necessarily occur in that order). It has also become clear that different persons can be involved in the failure compensation process at various stages and that the amounts of time spent on each of the process phases can vary between different failure compensation processes. A tentative categorisation of factors influencing failure recovery distinguises the categories priority-deciding, organisational, social, person related, occurrence related, and technical factors. Some of the recovery influencing factors may be more relevant for one process phase than for another. Also, some factors influence the recovery process directly and some have a more indirect influence on the process.

While the insights summarised above may lead the reader to think that the failure compensation process is the (only) way ahead in human reliability research, there are a few risks associated with this approach, as pointed out by De Keyser (1995):

- the risk of focussing on recovery (from failures resulting from design flaws) while neglecting a human-centred design approach from the outset;
- the risk of overestimating the chances of successful recovery, especially where failure processes are complicated and consequences are difficult to notice;

- and the risk of confusing error and responsibility for the error, which will hinder near miss reporting.

Keeping in mind these warnings regarding focussing exclusively on recovery, the message of this paper is to promote failure compensation as an *additional*, relatively new way to increase system performance, safety and reliability. It does *not* intend to suggest that focussing on failure compensation should *replace* prevention-based approaches, it should merely serve as an addition.

Some conclusions with regard to the need for additional research in the domain of failure compensation in general and recovery more specifically, can be drawn based on insights gained so far during the first steps of the research project. Even though the preliminary model and taxonomy presented in this paper provide a step in the right direction, a truly comprehensive and complete model of the failure compensation process, including an in-depth understanding of all the factors that influence recovery (both in a positive and a negative manner), still needs to be developed. In an attempt to develop the desired comprehensive model and understanding, the next steps in this research project will aim at generalisation of the pilot study's findings, via their application in two very different additional domains. In order to achieve general applicability and to fine-tune the preliminary model and taxonomy, they will not only be applied in the analysis of incidents on a much wider scale in the chemical industry, but also wide-scale and long term applications are planned in both the domain of medical errors, and the logistics/production planning domain. Based on collected incident and near miss data, hypotheses will also be formulated, and statistically tested, about the existence of certain recovery behaviour patterns (or user strategies in recovery), the (relative) importance of various recovery influencing factors, and the relationship between failure types and consequent recovery possibilities and -patterns.

Hopefully the insights gained so far via the research project described in this paper, and also future results of the next phases of this project, will both contribute to further theory

development about failure recovery, and provide a basis for the development of tools and techniques to assess recovery possibilities and promote recovery in working- and everyday environments.

REFERENCES

Bagnara, S., Ferrante, D., Rizzo, A., & Stablum, F. (1988). *Causal analysis in error detection and recovery: when does it occur?* Paper presented at the international conference on joint design of technology, organization and people growth. Venice, October 12-14, 1988.

Brodbeck, F.C., Zapf, D., Prümper, J., & Frese, M. (1993). Error handling in office work with computers: A field study. *Journal of Occupational and Organizational Psychology, 66*, 303-317.

De Keyser, V. (1995). *Evolution of ideas regarding the prevention of human errors.* Paper presented at the Man-Machine Systems (MMS '95) Symposium of June 27-29, 1995, MIT, Cambridge, MA, USA.

Edmondson, A.C. (1996). Learning from mistakes is easier said than done: Group and organizational influences on the detection and correction of human error. *Journal of Applied Behavioural Science, 32*(1), 5-28.

Embrey, D.E. & Lucas, D.A. (1988). The nature of recovery from error. In: L.H.J. Goossens (Ed.): *Human recovery: Proceedings of the COST A1 Seminar on Risk Analysis and Human Error.* Delft: Delft University of Technology.

Frese, M. (1991). Error management or error prevention: Two strategies to deal with errors in software design. In: H.J. Bullinger (Ed.): *Human aspects in computing: Design and use of interactive systems and work with terminals,* pp. 776-782. Amsterdam: Elsevier Science Publishers.

Hollnagel, E. (1999). Accidents and barriers. In: *Proceedings from CSAPC '99,* Seventh European Conference on Cognitive Science Approaches to Process Control, September 21-24, 1999, Villeneuve d'Asq, France, pp.175-180.

Kontogiannis, T. (1999). User strategies in recovering from errors in man-machine systems. *Safety Science, 32,* 49-68.

Rizzo, A., Bagnara, S., & Visciola, M. (1987). Human error detection processes. *International Journal of Man-Machine Studies, 27,* 555-570.

Sellen, A.J. (1994). Detection of Everyday Errors. *Applied Psychology: An International Review, 43*(4), 475-498.

Svenson, O. (1991). The Accident Evolution and Barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis, 11,* 499-507.

Van der Schaaf, T.W. (1988). Critical incidents and human recovery: Some examples of research techniques. In: L.H.J. Goossens (Ed.): *Human recovery: Proceedings of the COST A1 Seminar on Risk Analysis and Human Error.* Delft: Delft University of Technology.

Van der Schaaf, T.W. (1992). *Near miss reporting in the chemical process industry.* PhD thesis, Eindhoven University of Technology.

Van der Schaaf, T.W., & Kanse, L. (2000). Errors and error recovery. In: P.F. Elzer, R.H. Kluwe and B. Boussoffara (Eds.): *Human Error and System Design and Management*, pp. 27-38. London: Springer Verlag.

Van Vuuren, W. (1998). *Organisational failure: An exploratory study in the steel industry and the medical domain.* PhD thesis, Eindhoven University of Technology.

Wioland, L., & Amalberti, R. (1996*). When errors serve safety: towards a model of ecological safety.* Paper presented at CSEPC '96, Cognitive Systems Engineering in Process Control, Kyoto, Japan, November 1996, pp. 184-191.

Zapf, D. & Reason, J.T. (1994). Introduction: Human errors and error handling. *Applied Psychology: An International Review, 43*(4), 427-432.

Zapf, D., Maier, G.W., Rappenberger, G., & Irmer, C. (1994). Error detection, task characteristics, and some consequences for software design. *Applied Psychology: An International Review, 43*(4), 433-453.