Linköping Electronic Conference Proceedings
No. 23

Proceedings of the Resilience Engineering Workshop

25–27 June, 2007
Vadstena, Sweden

Editors
Rogier Woltjer, Björn Johansson and Jonas Lundberg

Cognitive Systems Engineering Laboratory
Division of Human-Centered Systems
Department of Computer and Information Science
Linköpings universitet
SE-58183 Linköping, Sweden

Copyright

Linköping Electronic Conference Proceedings, No. 23
Linköping University Electronic Press
Linköping, Sweden, 2007

ISBN 978-91-85831-37-1
ISSN 1650-3740 (online)
http://www.ep.liu.se/ecp/023/
ISSN 1650-3686 (print)

Table of Contents

Preface

The field of Resilience Engineering is comparatively young. The term was coined a few years ago, reflecting dissatisfaction with the then prevailing view of how safety in complex systems should be achieved. The idea was to view safety as an emergent system property rather than something that can be achieved by having reliable components. A core issue for Resilience Engineering was to achieve systems that are able to recover from disturbances. The agenda for the new field was to achieve engineering tools and methods of monitoring and improving resilience, as well as predicting the effects of change.

The new field took off after the first symposium on Resilience Engineering, held in Söderköping, Sweden, in 2005. A group of distinguished researchers from various fields attended that symposium, and the outcome of the symposium was the book "Resilience Engineering: Concepts and Precepts" (Hollnagel, E., Woods, D.D., & Leveson, N. (Eds.), Aldershot: Ashgate, 2006). In that book, the authors presented a variety of perspectives on Resilience Engineering that caught the attention of many others. This was evident at the second Symposium on Resilience Engineering which was held in Juan-Les-Pins, France, in 2006. The number of submitted contributions to the event was so large that the symposium had to be extended by a day.

It was after this event that the idea of having a workshop on Resilience Engineering in Sweden came up. At first, the workshop was intended to be a Swedish happening. However, we, the organizers, felt that it would be appropriate to write the call in English in case someone from outside Sweden would like to participate. This turned out to be a wise decision: of a total of seven presentations, all but two are presented by non-Swedes. During mid-spring, we were also quite worried that there would be too few participants. Luckily, this also turned out to be wrong. The beautiful location, in combination with a number of excellent contributions and two distinguished key-note speakers, attracted many national and international participants: a promising formula for a fruitful workshop filled with stimulating discussions.

Our first key-note speaker is Professor Sidney Dekker of Lunds universitet. Professor Dekker is a specialist in system safety, human error, reactions to failure and criminalization, and organizational resilience. In addition to this, he is an experienced pilot. He is also a member of the 'core group' that met at the first Resilience Engineering Symposium in Söderköping.

Our second key-note speaker is Professor Erik Hollnagel of Linköpings universitet and École des Mines de Paris. Professor Hollnagel has spent most of his life working with safety, human performance modelling, and cognitive systems engineering, in industry and academia. He is a leading person within the Resilience Engineering community, co-organizer of both previous Resilience Engineering Symposia, and founder of the Resilience Engineering Network.

The workshop has been organized into four main themes: Resilience in Aviation, Design and Resilience, Resilience Theory, and Pragmatic Resilience. The individual presentations within the themes have been given a generous amount of time to make room for discussion, emphasizing the fact that it is a workshop where each participant is given good opportunity to clarify their points and exchange ideas. Finally, we hope that the environment and the cuisine of Vadstena Klosterhotell will encourage discussion also in the "spare time" of the workshop, and perhaps provide opportunities for new forms of cooperation between the workshop participants.

There are a number of people who made this workshop possible. We would like to thank:

Anette Larsson, our administrator, for helping us in finding a pleasant venue for the workshop. Karin Lundblad and Josephine Speziali for handling the registration and other tasks at the workshop. The reviewers, who remain anonymous, for reading the submitted papers and providing good comments. And finally, Erik Hollnagel for coming up with the idea of having a Resilience Engineering workshop in Sweden. Obviously we would not be here without him.

Linköping, June 2007

Björn Johansson, Jonas Lundberg, and Rogier Woltjer

Cognitive Resilience: Reflection-In-Action and On-Action

Jonathan Back, Dominic Furniss, Ann Blandford

University College London Interaction Centre, United Kingdom
{j.back, d.furniss, a.blandford}@ucl.ac.uk

Abstract. Identifying cognitive strategies that people use to support resilient performance has rarely been the focus of experimental work. Our experiments have found that the pervasiveness of failures during human computer interaction can be recognized by individuals, but underlying cognitive and attentional causes cannot. Understanding how individuals recover from failure and adapt to new environmental demands can be studied in the laboratory, however, this requires a paradigmatic shift away from developing traditional 'single cause' explanations. Previous research has strongly suggested that individuals are reliant on 'bottom-up' cues from the environment when planning future actions. By systematically manipulating factors that influence an individual's awareness of environmental cues, work reported in this paper has revealed some novel insights. Resilient individuals are able to spontaneously generate new strategies in-action that support response to regular disturbances. Furthermore when provided with a 'window of opportunity' to reflect-on-action, individuals can rehearse future actions so that the influence of any residual strain (or load) can be mitigated against (feedforward strategy). Further work on understanding strategies adopted by resilient individuals may facilitate the development of systems that explicitly support cognitive resilience.

1 INTRODUCTION

Cognitive psychologists have found that 'human error' can be provoked within a laboratory environment and that the development of causal accounts enables the frequency of certain types of errors to be predicted (e.g., Byrne and Bovair, 1997; Gray, 2000). Demonstrating that 'human error' is not the product of some stochastic process has led to a better understanding of human cognition but has had little impact on research and practice in safety, risk analysis, and accident analysis. Laboratory studies have focused on errors that occur during practiced routine performance, where a participant performs an incorrect sequence of actions. Outside the laboratory, identifying incorrect action sequences is not possible since the context in which those sequences took place cannot be easily understood. Dekker (2005) suggested that error classification disembodies data: it removes the context that helped to produce the behavior in its particular manifestation. "*Without context, there is no way to re-establish local rationality. And without local rationality, there is no way to understand human error*" (Dekker, 2005, p 60). We argue that 'cognitive resilience' is an intrinsic component of local rationality. Identifying cognitive strategies that people use to support resilient performance might help to account for behavior. Individuals are resilient if they are able to recognize, adapt to and absorb variants, changes, disturbances, disruptions, and surprises (Woods & Hollnagel, 2006). This paper will discuss the extent to which cognitive strategies that support resilience are identifiable in the laboratory.

One of the first attempts to demonstrate the non-stochastic nature of errors was suggested by Rasmussen and Jensen (1974). The idea that errors can be categorized as being skill-based, rule-based, or knowledge-based allows errors to be attributed to different cognitive factors. However, whether an error is classified as skill-based, rule-based, or knowledge-based may depend more on the level of analysis than on its ontogeny (Hollnagel, Mancini, & Woods, 1988). For example Gray (2000) argued that the same behavior, e.g. "taking the wrong route during rush hour", can result from lack of knowledge (not knowing about a faster route) or misapplication of a rule (knowing that one route is the fastest during rush hour and the other is fastest on the off hours but applying the 'off hours' rule in the rush hour). In addition, this behavior could be caused by a slip (taking the more familiar route when the intention was to take the less familiar but faster one) or be intentionally wrong (too much traffic to get into the correct lane).

The focus of laboratory work on human error has been to develop 'single cause' accounts of slip errors. Slip errors can occur systematically even when individuals have the required 'expert' procedural knowledge to perform a task correctly. For example, Byrne and Bovair (1997) showed that post-completion error (a type of slip) is sensitive to working memory demands. If the environment imposes high working memory demands then this type of error is more likely. Therefore, an individual who has an increased capacity to process information is less likely to make a slip error. This type of finding is of interest to cognitive scientists but is of little use to researchers and practitioners in safety, risk analysis, and accident analysis. An understanding of human performance is only useful when the context (local rationality) that helped to produce the behavior is understood. Elucidating this context may be possible if cognitive strategies that people use to support resilient performance can be identified.

This paper reports on a series of experiments that aimed to reveal some of the strategies that individuals use during human computer interaction. These strategies help individuals to detect, recover from and mitigate against failure. Previous research has strongly suggested that users are reliant on 'bottom-up' cues from the environment when planning future actions (Payne, 1991). It is hypothesized that the development of cognitive strategies is dependent on an individual's awareness of environmental cues. By systematically manipulating factors that influence an individual's awareness of cues, different strategies that support resilient performance may emerge.

2 SELF-REPORTING AND RECOGNIZING FAILURES

Errors are one measure of the quality of human performance. For example, Miller (1956) identified an important property of working memory by discovering that individuals make errors when recalling more than 7 (+/-2) elements of information. However, the everyday concept of error presupposes a goal. This can make the classification of errors difficult if an individual is interacting in an exploratory way to satisfy a learning goal, especially when a user is adopting a trial-and-error approach. A better understanding of error is only possible if a way of differentiating between errors and exploratory interactions (where errors or sub-optimal moves can be an expected or even a desired outcome) is possible. However, humans are not always able to describe their goals

or able to recognize the extent to which a goal has been addressed. In an attempt to investigate this issue, a problem solving game was designed that allowed participants to verbally self-report erroneous and exploratory interactions (*see* Back, Blandford, & Curzon, 2007a). Twenty participants were encouraged to develop their own distinctions between what should be considered erroneous or exploratory. The game specified a series of locations (rooms) and placed objects within rooms or within the player's inventory (possessions). Objects such as a locked door were not designed as permanent obstacles, but merely as problems to be tackled. Solving problems frequently involved finding objects and then using them in the appropriate way. One aim was to discover whether self-reports provide useful information about the strategies individuals use to mitigate against error. Two types of report were possible: 1) An 'Elective Report' made at any time during interaction; 2) A 'Debrief Report' which required a participant to review a trace of their own behavior immediately after a task was completed.

When comparing the elective reports with the debrief reports no significant differences were associated with the frequency of erroneous reports. However, exploratory interactions were significantly more frequently reported using the elective self-report mechanism. Woods, Johannesen, Cook, and Sarter (1994) argued that self-reports can be biased by hindsight which prevents them from being a useful tool for understanding interaction. Our analyses showed that the elective mechanism was able to elicit a significantly wider range of exploratory move types than the debrief mechanism. This supports the notion that outcome knowledge (knowing how things turned out) biases self-reporting processes, especially when reporting exploratory moves. A qualitative analysis revealed that exploratory self-reports provided useful information about problem solving strategies that participants were trying out. Crucially, many exploratory reports (65%) outlined strategies that participants used to avoid making persistent errors.

During interaction, the pervasiveness of errors was recognizable but underlying cognitive and attentional causes were not. Only 20% of elective error reports associated were reasoned accounts of error. During debrief reporting, participants were more able to provide a reasoned accounts (72% of these reports were reasoned). Based on these findings we argue that the error recognition process is dependent on cognitive context and the availability of environmental cues. Reasoning about errors during interaction is harder than when performing a debrief report because different environmental cues are 'salient'. During the debriefing session participants were required to debug their task performance. Critically, participants were not reminded of task objectives. Therefore, the only way of detecting erroneous moves was to recall intentions based on the availability of environmental cues. When performing a debrief report immediately after interaction, participants were able to reconstruct intentions and were actively looking for environmental cues that could be used to execute those intentions.

In summary, an opportunity to reflect-on-action is essential for an individual to reason about why failures occurred, enabling future strategies to be formulated. However, an understanding of the exploratory strategies that individuals actually use can only be elicited during interaction (reflection-in-action).

3 REFLECTION-IN-ACTION AND ON-ACTION

Schön (1987) describes two types of reflection: reflection-in-action and reflection-on-action. The former takes place as events unfold, where the participant will perceive the situation as new but implicitly compare it to prior experience, situate possibilities for new actions and carry out experiments to decide a course of action. The latter happens further away from the event temporally, where the participant will formalize the situation and actions so they can evaluate and think about the situation. For example, a footballer will be reflecting-in-action during the game by responding to opportunities presented to him by his team mates and the opposition; during the half time break the team‘s coach will facilitate reflection-on-action by describing what was good, what could be improved, and how to change their tactics.

The Repetitions-Distinctions-Descriptions (RDD) Model (Nathanael & Marmas, 2006) provides a graphical illustration of how reflection-in-action is distinguished from reflection-on-action. Figure 1 shows an abstracted version of the RDD model presented by Nathanael and Marmas (2006, p. 233). Here repetitions account for the normal routine actions of individuals, where these are abnormal or there is opportunity to try something different then a ‘distinction’ in the normal routine can be made and the participant reflects-in-action (RIA) to alter their practice, this altered practice can then be absorbed in normal routine if appropriate. Reflection-on-action (ROA) occurs in detached moments where participants may formalise new understandings of their situation for action i.e. the situation is not only distinguished but described and reflected upon away from the event.

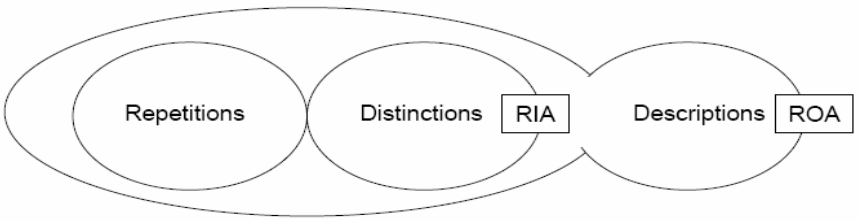


Fig. 1. The Repetitions, Distinction and Descriptions (RDD) Model adapted from Nathanael and Marmas (2006, p. 233). RIA = Reflection-in-action; ROA = Reflection-on-action

4 STRATEGIES FOR REFLECTING-IN-ACTION AND ON-ACTION

By systematically manipulating factors that influence an individual’s awareness of environmental cues, some novel insights into the nature of cognitive strategies people use to support resilient performance can be revealed. A simulation of a ‘Fire Engine Dispatch Center’ was developed. Two experiments using 24 participants each were run (see Back, Blandford, & Curzon, 2007b). Experiment 1 investigated the frequency of two classes of slip error under different cognitive and perceptual load scenarios. Experiment 2 investigated if a ‘window of opportunity’, used to rehearse procedural steps, reduced error rates. Results from both of these experiments demonstrate that individuals can develop cognitive strategies to maintain resilient performance when reflecting in-action and on-action. Two systematic error manifestations are briefly outlined below.

Mode Error - A visual display that informed participants of GPS signal status was provided. Participants were required to attend to this signal so that they could determine what type of route information had to be sent to a particular fire engine. Analysis revealed that if participants placed the mouse cursor close to the signal status display, they were significantly less likely to forget to attend to the display before selecting an appropriate route construction method. Avoiding this type of error can be considered a cognitive skill since it involves spontaneous personalized cue creation by reflecting-in action.
Initialization Error - When commencing a new trial an individual had to decide which call to prioritise before clicking on the 'Start next call' button. Forgetting to perform this call prioritisation procedure resulted in an initialization error. In Experiment 2 participants were given 4 seconds to reflect on requirements before commencing a trial: Within-subjects Conditions - A) call prioritisation always visible; B) call prioritisation not visible during reflection time. In Condition A participants were significantly better able to avoid initialization errors. Condition A allowed participants to reflect-on-action.

5 CONCLUSIONS

Rehearsal (reflecting-on-action) and personalized cue creation (reflecting-in-action) are examples of cognitive strategies that people can use to support resilient behavior. When a 'window of opportunity' for reflection exists then any residual strain (or load) can be mitigated against (feedforward strategy). Resilient individuals are able to spontaneously generate new strategies in-action that support response to regular disturbances (e.g., learning to use the mouse cursor as an environmental cue). Understanding how individuals recover from failure and adapt to new environmental demands can be studied in the laboratory, however, this requires a paradigmatic shift away from developing traditional ‘single cause’ explanations. An understanding of human performance is only useful when the context that helped to produce the behavior is understood.

REFERENCES

Back, J., Blandford, A. & Curzon, P. (2007a). Recognising erroneous and exploratory interactions. To appear in *Proceedings of INTERACT 2007*.

Back, J., Blandford, A. & Curzon, P. (2007b). Slip errors and cue salience. To appear in *Proceedings of ECCE2007*.

Byrne, M. & Bovair, S. (1997). A working memory model of a common procedural error. *Cognitive Science, 21* (1), 31-69.

Dekker, S. (2005). *Ten questions about human error: a new view of human factors and system safety*. Lawrence Erlbaum Associates.

Gray, W. D. (2000) The nature and processing of errors in interactive behavior. *Cognitive Science, 24* (2), 205-248.

Hollnagel, E., Mancini, G. & Woods, D. (1988). *Cognitive engineering in complex dynamic worlds*. Academic Press.

Nathanael, D. & Marmas, N. (2006). The interplay between work practices and prescription: a key issue for organisational resilience. In E. Hollnagel & E. Rigaud (Eds.) *Proceedings of the Second Resilience Engineering Symposium* (pp. 229-237), 8-11 November 2006, Juan-Les-Pins, France.

Miller, G. (1956). Human memory and the storage of information. *Transactions on Info Theory, IT-2* (3), 128-137.

Payne, S. J. (1991). Display-based action at the user interface. *International Journal of Man-Machine Studies, 35*, 275-289.

Rasmussen, J., Jensen, A. (1974). Mental procedures in real-life tasks. *Ergonomics, 17*, 293-307.

Schön, D. (1987). *Educating the reflective practitioner*. San Francisco: Jossey-Bass.

Woods, D. D., Johannesen, L. J., Cook, R. I. & Sarter, N. B. (1994). *Behind human error: Cognitive systems, computers, complexity and hindsight*. CSERIAC, 94-01.

Woods, D. D. & Hollnagel, E. (2006). Prologue. In: Hollnagel, E., Woods, D. D. & Leveson, N. *Resilience engineering: Concepts and precepts* (pp. 1-7). Aldershot, UK: Ashgate.

Barriers to Regulating Resilience: Example of Pilots' Crew Resource Management Training

Stéphane Deharvengt

Direction Générale de l'Aviation Civile, 50 rue Farman, 75720 Paris cedex 15, France
stephane.deharvengt@aviation-civile.gouv.fr

Abstract. Regulation in high risk industry is not considered as a characteristic for resilience. This article identifies issues surrounding the introduction of a new regulation in an ultra safe system that is designed to build more resilience into the system. The development and implementation of Pilots' Crew Resource Management regulation within the French Civil Aviation Authority is reviewed. Interviews and questionnaires form the basis for the analysis of the intent and practices of those in charge of high level decisions, those having the knowledge of human factors discipline, and those whose job it is to implement this regulation. However the gap between the regulation as imagined, and the regulation as implemented, illustrates the resistance of the system towards this approach to regulation and the potential drifts. The article presents the findings as characteristics of the regulatory process concerning the introduction of resilience. The lack of internal expertise and lack of implementation monitoring explain the present shortcomings of regulatory authorities and ultimately questions the role of regulation regarding the engineering of resilience. At a time when high profile regulations are enacted that aim for adaptive solutions in aviation, the presented retrospective offers insights into present and future issues.

1 RESEARCH CONTEXT

The resilience concept is discussed for high risk activities like medicine, aviation, or power production (Woods, Hollnagel & Leveson, 2006). However it is also informative to look at how those systems are regulated since they cannot thrive and reach a very high safety level without the constraints of regulation by national or international agencies (Amalberti, 2001). The safer the system, the less resilient it becomes because of the rigidity of the normative strategy. The central question of this article is to evaluate the potential of regulation to be used as a tool to introduce more resilience. The introduction of pilots' CRM training regulation by French Civil Aviation Authority (DGAC) is used to illustrate some barriers to building resilience via a regulatory process.

The onset of this research stems from formal and informal feedback received concerning Crew Resource Management (CRM) training of poor quality being delivered. The research question states as a formal hypothesis that CRM training is stabilizing the training at a low quality level, which is satisfactory for all interested parties (Deharvengt, 2007). Different viewpoints of individuals involved in the regulatory process are examined, both from an historical perspective and at the relevant levels of DGAC hierarchy. The initial intentions of those in charge of regulating CRM at the early stages are examined: on one hand the successive heads of the Direction du Contrôle de la Sécurité (Safety Oversight Authority) in charge of decision making in the rulemaking process

are interviewed, and on the other hand a human factors perspective is sought from the only people that actually possessed high level knowledge of the discipline within DGAC during the 90s. Consideration is then given to the implementation conditions from the perspective of the inspectors in charge of monitoring the airlines' Air Operator Certificate. Comparative research is conducted in parallel to investigate the airline industry and their perception of CRM delivery (Pariès & Mourey, 2006).

2 RESILIENCE THROUGH CRM REGULATION: LESSONS LEARNED

2.1 A Promising Regulatory Initiative

In the 90s, French civil aviation was under great stress. The context is that of an economical downturn for airlines as well as fear of increased competition European wide with the implementation of a European license (JAR FCL, Flight Crew Licensing) and common airlines' operating rules (JAR OPS1). The implementation of ICAO requirements for human factors threatened the validity of French pilots' licenses. Concurrently, the advent of glass cockpit and its early dramatic accidents (e.g. crash of A320 at the Mont St Odile in early 1992) brought into question the transforming role of the pilots in the cockpit.

International networking between leading human factor experts and the exchange of ideas enabled the importation of the CRM concept into Europe, as well as its subsequent adaptation to answer the airlines' needs of the day. Those experts offered a particularly welcome solution to the pressing issues that were confronting the DGAC management and industry (airlines and unions) (Pariès, Amalberti, 2000). Together they formulated the outlines of the CRM regulation as a human factors' response to airlines' safety needs and local issues. This regulation is therefore original in the sense that it does not set rigid requirements, but tries to provide flexibility or adaptive capacities for airlines to train their crews.

2.2 A Poor Lonesome Regulation

For DGAC management this new training methodology is useful in the sense that, contrary to normal "individual" pilot training, CRM offers the pilots an opportunity to interact inside a group of professionals and discuss operational issues. The rationale is that this interaction leads to a positive change in operational behavior. Achieving this change and controlling it is perceived as particularly suited for monitoring airlines. CRM training is considered to be a tool to control individual behaviors acts, and as a leverage to control the behavior of the airline, hence improving visibility of the safety of the airline. This logic coincides with the changing way that the authorities monitor the activity of the airline, from a former field approach towards requiring, certifying, and monitoring airlines' organizational systems. This has resulted in a gain in resources and efforts. The first finding is that regulation that tries to regulate resilience corre-

sponds to the present regulatory approach as understood by the management of regulators by addressing the system's characteristics.

The final CRM regulation was officially enacted in 1997, but already in effect since 1993. The regional offices were initially supported by a few DGAC human factor experts. However, in a context of European harmonization, the incorporation of JAR OPS 1 into the French regulation scaled down the CRM requirements in form and substance in 1999. The amendment corresponding to the full French CRM regulation was expected to close the bridge of transition. It is not until 2001 that this amendment was approved in Europe, but the situation in France remained unchanged due to the absence of updating of the national regulation until July 2006. CRM was no longer important for DGAC in early 2000 and the regulatory process did not bridge the gap until very recently. Additionally an analysis of US NTSB (National Transportation Safety Board) and French BEA (Bureau d'Enquêtes et d'Analyses) recommendations over a recent period of 10 years shows that focus on CRM related issues is negligible. A second finding is that political pressure is required to initiate the critical momentum for the success of a regulation of resilient nature, but that even with momentum the success is very short lived.

2.3 And a Long Way from Implementation

The initial intent of DGAC management when introducing the CRM regulation was to introduce a new organizational surveillance tool into the arsenal of the airline inspectors. The inspectors themselves often relate CRM training to experience feedback and flight operations safety analysis. However, the report from the field is very different.

Even though the inspectors have knowledge and appreciation of the CRM training and content, the evidence shows that they devote very little time on this topic during their surveillance of the airlines. Half of the inspectors queried recognized that they themselves have a lack of knowledge about what CRM training is and about how to evaluate a CRM program. As a consequence, their surveillance is limited to acknowledging the existence of a CRM program on paper. Feedback from other regulatory agencies around the world indicates a very similar trend worldwide regarding implementation of CRM. This also confirms the evolutionary trend of surveillance tasks towards more of a paperwork approval process and away from field interaction with the airlines. A third finding is the inadequate match between an adaptive regulation like CRM and the present regulatory oversight process.

The implementation of CRM regulation was never an opportunity to question its content (or lack thereof) nor the means to evaluate the airlines' training programs and trainers which validates the initial hypothesis that the state of CRM delivery was agreed by all interested parties. The rest of the hypothesis (stabilization towards a low quality level) is refined by the comparative research in the industry and postulates that CRM delivery has not transcended beyond the initial stages of concepts to become a risk management tool for the airline: CRM remains on the roadside. The final finding is that a drift occurs with adaptive regulations: when confronted with a concept the end-users do not know

how to manage, regulators and industry fall back on implementing the rule to the letter, thus missing the positive adaptive benefits originally intended by the regulation.

2.4 Lessons for Regulating Resilience in Ultra-Safe Systems

Implanting adaptive regulations in ultra-safe systems is difficult. After initial acceptance with enthusiastic interest, the implementation eventually produces poor results in the field, along with disinterest or misunderstanding on the part of regulators. Efforts are invested, but compliance to the regulation is achieved with minimal resources on both sides. It follows that the usefulness of the effort is considered as wasted ("CRM has lost it") since low quality products are approved. The positive benefits for the pilots and for the overall system safety are never realized, and other alternatives are sought.

The last two barriers on the road towards ultra-safe systems (Amalberti, 2003) may, in actuality, be "risks" of regulatory activity. One is the one-sided optimization of the rulemaking strategy at the management level ("we are protected because we have the word CRM in the regulation") that does not make sense at operational level because the oversight that field inspectors perform is different from the oversight required for an adaptive system. The inspectors typically do not have any knowledgeable subject matter expert to consult when they have questions. Additionally, they receive typically very little CRM expertise or training beyond perhaps attending a CRM course. Their risk is increased and they protect themselves by defaulting simply to strict compliance to the CRM regulation.

The second barrier is the loss of visibility of the risk in the regulatory process: the CRM regulation continues till the end without any questioning of its value since no one understands the mechanism ("we don't know how or why, but it must be useful somehow so we keep it"). The lack of internal feedback and drifts in manners of implementation of regulations is also demonstrated in research and experience in several other areas such as recreational aviation (Poirot-Delpech, Prévot, Raineau, 2006), helicopter first flight initiations (Soria, Hermann, Bestit, 2003) or internal DGAC working group for aerial work.

3 PRESENT PERSPECTIVE

A number of regulations bearing a striking resemblance to CRM are being introduced: human factors cockpit certification rule, competency based training for multi crew pilot license (MPL) or Safety Management Systems. Whether they aim to analyze the coupling of man and machine, to train for competence rather than performance or to systematically identify risks in operations, each refer to an adaptive strategy, but also assumes an important knowledge in the area of human and organizational factors, and they are all largely under specified. The study on CRM shows that the rulemaking authority has a clear influence on the development of such strategies.

However, authorities presently bear a lot of pressure: cost and workforce reductions, litigation cases, justification of their activities, pressure from industry, and extensive reorganization in Europe with the creation of the European Aviation Safety Agency. In this context, strict application of regulations is often the result with a consecutive loss of flexibility, unrecognized drifts at the local level, or "tick in the box" syndrome. In a high risk industry adaptive regulations often translate into rigidity for the system. Rather than questioning the relevance of regulating or not, a more challenging question is how the regulators attempts to engineer resilience into the system. This relates directly into why the industry may resist or misunderstand resilient strategies.

4 CONCLUSION

Resilience needs expertise and flexible and learning organizations. This raises a fundamental issue: are regulatory authorities able to introduce and monitor resilient tools in the industry they regulate if they are not themselves attuned to resilience? The findings in this article should prompt authorities to question their strategy of expertise and monitoring of their practices when trying to engineer resilience through regulation.

REFERENCES

Amalberti, R. (2003). *The limit of safety: A transversal approach of risk management in high risk technologies.*

Deharvengt, S. (2007). *Réglementer dans un domaine à risque : L'exemple de la formation CRM des pilotes de ligne*. DGAC report.

Hollnagel, E., Woods, D. D. & Leveson, N. (Eds.) (2006). *Resilience engineering: Concepts and precepts.* Aldershot, UK: Ashgate.

Moulin, L. & Joseph S. (2005). *L.O.S.A.N.G.E. (Line Operations Safety Analysis using Naturalistically Gathered Expertise) - Report n°3: Airlines data collection and Normal Operations Monitoring*. DGAC report.

Pariès, J. & Amalberti, R. (2000). Aviation safety paradigms and training applications. In N. Sarter & R. Amalberti (Eds.), *Cognitive engineering in the aviation domain* (pp. 253-286). Hillsdale, NJ: Lawrence Erlbaum Associates

Pariès, J. & Mourey, F. (2006). CRM and HF training regulations: A reality check based on the French example. *7th International Symposium of the Australian Aviation Psychology Association*. Sydney, Nov. 2006.

Poirot-Delpech, S., Prévot H. & Raineau, L. (2006). *Une approche socio-anthropologique de l'aviation générale : L'insécurité des réglementateurs*. DGAC report.

Soria, L., Hermann, E. & Bestit, L. (2003). *Analyse et synthèse des points forts et des risques potentiels des situations de baptême de l'air et propositions de fiabilisation*. DGAC report.

Acknowledgement

The author would like to acknowledge the involvement of C. Valot (IMASSA) in the creation of the original hypotheses and in his continued support, as well as the work of the consortium (Dedale SA., SynRjy, Amok, EPAG) for the investigation with French industry concerning pilots, cabin crew and maintenance human factors training. Finally, the author is thankful for the support of DGAC in funding the consortium and to all DGAC personnel contacted during the course of this research.

Disclaimer

The ideas expressed in this paper only reflect the opinion of the author and must not be considered as official views from any national or international authorities or official bodies to which the author belongs.

Contribution of Resilience to the Analysis of Flight Crew Decision-Making: Example of a Near-CFIT in Public Transport

D. Delaitre, D. Nouvel, Y. Pouliquen, S. Travadel

BEA – Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile
Statistics and Safety Analysis Division, Le Bourget, France
{didier.delaitre, david.nouvel, yann.pouliquen, sebastien.travadel}@bea-fr.org

Abstract.. It is noticeable that in some incidents crews deviate from standard procedures and continue the flight in deteriorating conditions until a triggering factor makes them return towards normal flight conditions. To be more precise, the procedures that frame the conduct of a flight refer to standards and are within a safety envelope that calls on training and reduced capacity for adaptation. The course of the flight and the reality of operational constraints may lead the flight crew to fly at the limits of the envelope. The situation can then deteriorate in a more or less prolonged or serious manner. When the crew reacts, if they do, their capacity for adaptation will either allow them to return to a normal situation or not. An investigation often makes it possible to explore the reasons for deviations from standards, though it is more difficult to explore the crew's determination to continue the flight in deteriorated conditions: the factors that lead a pilot to perceive danger and to decide to take corrective action remain little known, as do the resilient processes that are mobilized. Based on an example of a near-CFIT, we will demonstrate the need to better characterize the evolution over time of a crew's capacity to react when faced with a dangerous situation in order to limit the consequences.

1 INTRODUCTION

On Sunday 23 November 1997, on final ILS approach to Orly airport (Paris), the Captain of the MD83 registered F-GRMC, performed a go-around in Instrument Meteorological Conditions as the aircraft was passing the Outer Marker. The minimum radio height during the go-around was sixty-seven feet.

This document initially describes the specific context of the flight and the aircraft's manoeuvres during approach as analyzed on the basis of flight documents, recorded data and witness statements.

Causes clearly identified by the investigation are then presented along with the safety recommendations made by the BEA. The standard investigation process was particularly useful to highlight the reasons why the crew deviated from the approach path.

It seems it is more complex to analyse how the sequence then continued for so long into a deteriorated situation, far more challenging to highlight what the criteria were – if any – that triggered the Captain's decision to perform a go-around. The final part considers the possibilities presented by the principles of resilience engineering in undertaking investigations and safety studies in the future.

2 DESCRIPTION OF THE OCCURRENCE

2.1 Specific Context

Flight crew details

The crew consisted of a Captain instructor and two FO's on LOFT. The two FO's on LOFT occupied the co-pilot and observer seats alternately.

The airline

At the end of 1996, the airline had changed ownership and important management changes had been put in place. The arrival of an extra aircraft in April 1997 allowed significant growth in the MD83 sector. Since, in the winter of 1996-1997, it had been decided that there would be no recruitment, there was a shortage of flight crews for the winter of 1997-1998. There were 10 pilot instructors in the MD83 sector for forty-four captains and forty-two first officers. Around six months before the incident, the airline had thus decided to train twenty-two FO's and six Captains and undertake two first JAR 25 qualifications. The first wave of training, which included the two co-pilots on LOFT, had begun in October 1997.

Meteorological conditions

In the afternoon, low clouds, mist and fog, thick in parts, persisted to the north of the Seine. At Orly, at 12 h 30, the RVR at the threshold of 07 was 375 meters. With such visibility, the crew was not qualified to perform the planned landing since the Flight Officer was only qualified to perform restricted category 1 approaches. The Category 1 approach to runway 07 at Orly required an RVR of 600 meters.

2.2 History of Flight

Preparation, takeoff and en-route

On the previous day, the crew had flown the Orly-Nice-Orly-Toulon route legs and earlier that morning, they had flown the Toulon-Orly-Marseille route legs.

The aircraft landed at Marseille at 10 h 35. During the preparation of the Marseille-Orly flight, the crew received a meteorological dossier. The alternate airport was Paris-Charles de Gaulle. The flight dossier indicated that the aircraft was carrying 20,000 pounds of fuel. The Captain stated that he had loaded sufficient fuel in reserve to return to the South of France in case the meteorological conditions made a landing at Orly impossible.

At 11 h 25, the aircraft took off from Marseille with 131 passengers and 7 crew. The co-pilot was pilot flying. The flight took place without any notable events until the

preparation of the approach to Orly. The auto-throttle and AP 2 were engaged throughout the flight.

The crew prepared category I, II and III precision approaches to runways 07 and 26 at Orly. At 11 h 53, Paris ATC announced RVR of 400 meters on runway 07. At 12 h 07 the Captain took over as pilot flying. At 12 h 14 min 43 s, the crew contacted Orly Approach which announced RVR of 500 meters.

Approach

During approach, the modes displayed on the FMA (figure 1) changed 30 times. The following description does not show all these modifications. Numbers 1 to 9 refer to the main steps of the approach as shown in figure 2.

***12 h 26 min 23 s* – Error in track selection**
The Captain selected track 258° on the VHF NAV 1 (left) instead of 065°.

Track 258° corresponded to runway 26, which had been used for the previous landing in Orly.
The co-pilot did not check the display.

(1) ***12 h 29 min 34 s* – End of radar vectoring and transfer to Tower**
Until this point, the aircraft was vectored by Orly approach to intercept the localizer.

At that moment, the aircraft was at an altitude of 3,000 feet, at a speed of 160 kt, on heading 020° for interception of the runway 07 ILS.

(2) **Crossing track 065°**
The co-pilot had selected track 065° on the OL VOR. He announced that the aircraft was crossing this track.

Intercepting the runway 07 ILS, the runway line-up deviation indicator began to move on the Captain's HSI as well.

(3) ***12 h 29 min 53 s* – RVR announcement**
Orly Tower announced RVR of 400 meters.

Such an RVR corresponded to a category 2 approach.

Subsequently the Captain did not call out the actions he took in relation to the automatic systems.

(4) ***12 h 30 min 20 s* – Crossing glide path**
The aircraft went above the approach path.

(5) ***12 h 30 min 40 s* – Descent**
The Captain armed the "autoland" mode, displayed an altitude of 2,000

The selected altitude of 2,000 feet corresponded to the preparatory go-around altitude.

feet, selected a descent speed of around 2,300 feet per minute and a heading of 090.

The aircraft began to descend in clear skies.

(6) Error detection and Orly Tower indication
The Captain then realized that he had selected an ILS heading of 258° instead of 065° and corrected it. Orly Tower indicated that the aircraft was 1.5 NM north of the track.

While the Captain was correcting the error and extending the flaps, the aircraft passed below the glideslope

(7) ***12 h 31 min 26 s* – GPWS and AP off**
At a radio-height of 916 feet, the GPWS "Glideslope" warning was recorded by the Quick Access Recorder (QAR) for 45 seconds.

The aircraft entered the fog at that moment or a few seconds later. During the descent, the FO saw that the bar of the glideslope was up against its stop and said "glide" twice.

The Captain disconnected the AP but did not initiate any manoeuvres.

It was not possible to identify the reason why he did so.

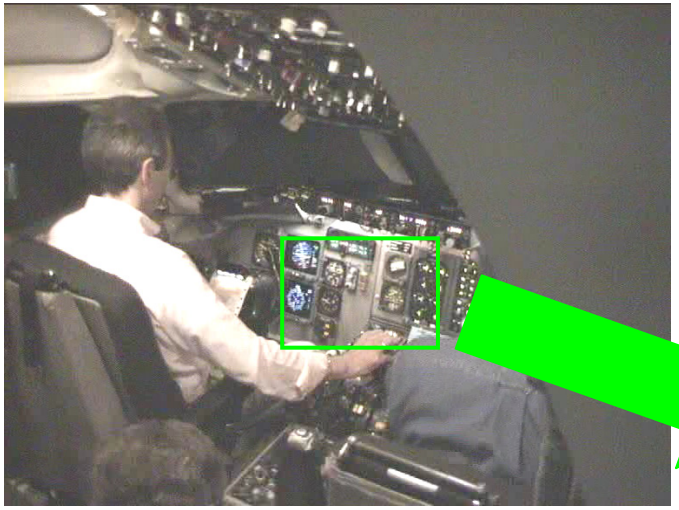
(8) ***12 h 31 min 49 s* –AP on**
The Captain connected the AP and then armed the "autoland" mode.

The Captain probably connected the AP because he saw "LOC CAP" displayed on the FMA and thought he could still carry out the approach.

(9) ***12 h 31 min 56 s* – AP off and go-around**
The Captain disconnected the AP and initiated a go-around.

At that moment, the radio-height was about 200 feet. At 12 h 32 min 09 s, the minimum radio-height of 67 feet and the Outer Marker signal were recorded. The co-pilot later stated that he saw the ground and read a radio-height of about 50 feet.

Fig. 1



engine mode (green)	armed mode (amber)	horizontal mode (green)	vertical mode (green)
SPEED	AUTOLAND	HEADING	ALTITUDE HOLD

Horizontal Situation indicator

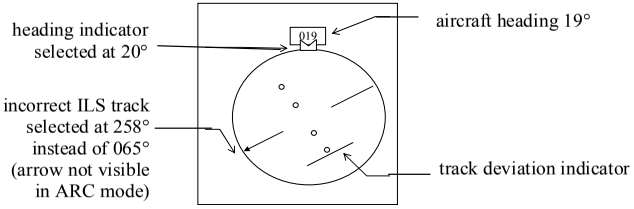
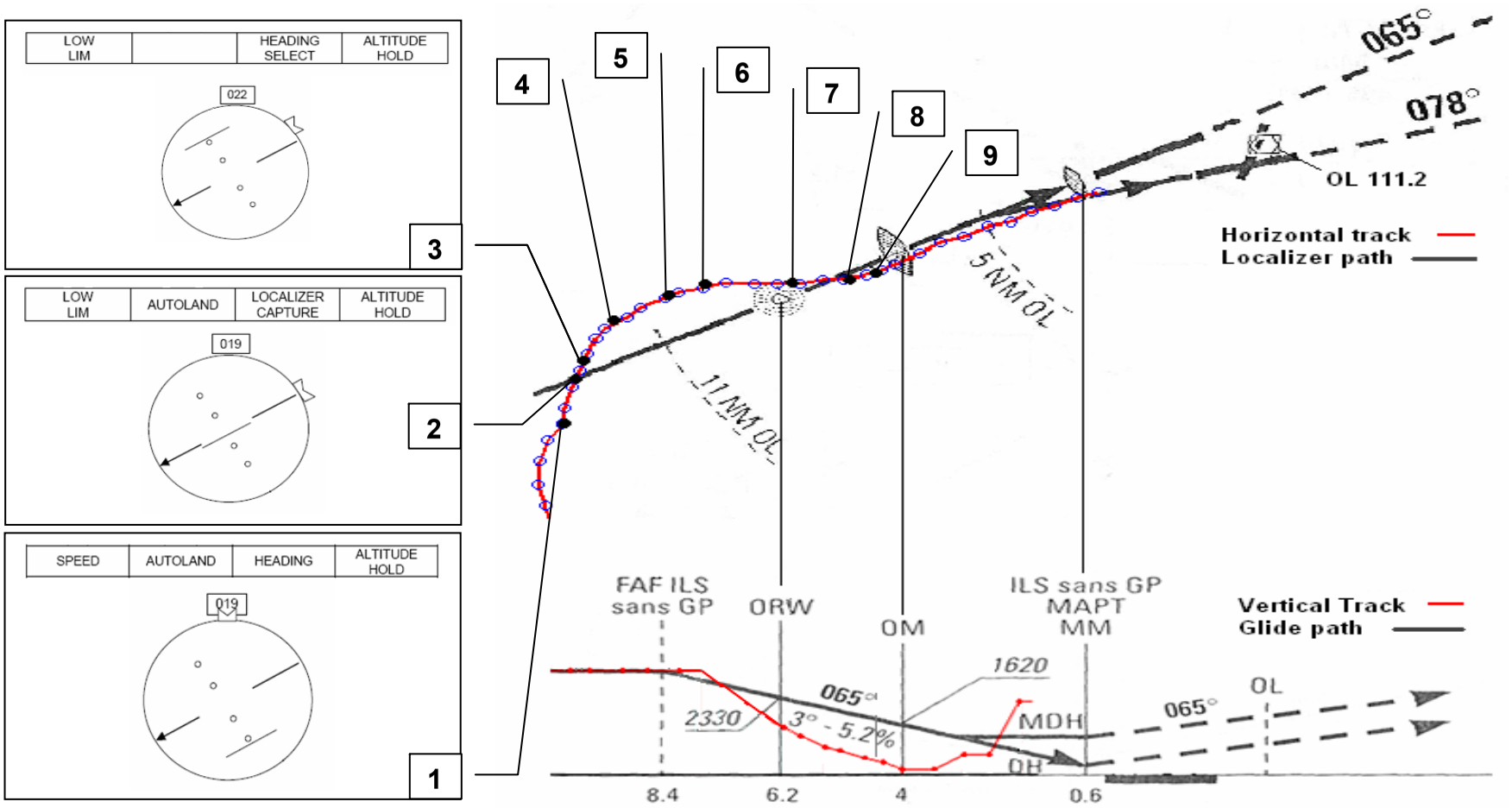


Fig. 2



This is an illustration and should not be considered as the real trajectory.

3 RESULTS OF THE INVESTIGATION: PROBABLE CAUSES AND ASSOCIATED SAFETY RECOMMENDATIONS

The report concluded that the incident resulted from the decision to put the aircraft into descent when, as a result of a display error, it was neither on the localizer track nor on the glide path, and with no context defined for this improvised manoeuvre. Consequently, the BEA made three recommendations concerning the presentation of horizontal and vertical position data on new generation aircraft and the difference between the active modes displayed on the FMA and those in which the aircraft is effectively engaged at any given moment

The operator's company culture directly contributed to the incident through the importance it attached to accelerated training given to new copilots and to undertaking commercial flights. As a result, the BEA issued recommendations about training, regarding the calculation of flights really performed as members of the crew by pilots in training and the number of in-flight inspections, particularly in case of a major increase in an airline's activity.

Other contributory factors were:

- the pilot's fatigue;

The BEA proposed that information should be provided to airlines in order to allow the modification of flight planning so as to avoid pilots exceeding the statutory work time. It was also suggested that regulations on flight crew work time take into account all aspects that cause fatigue.

- the imbalance in the flight crew, made up of a very experienced instructor and an under-trained FO, which led to the abrupt disappearance of teamwork and procedures the moment the workload increased. The Captain did not state his intended actions to the inexperienced FO, who he considered to be a student and who thus became a simple spectator. Finally, rather than aborting the approach, he continued with it while trying to understand what was going wrong.

Concerning this question, the BEA recommended the presence of an additional pilot trained in supervision during flights in the context of LOFT.

- aircraft warning system ergonomics and a fault in the automatic pilot system.

It was recommended that the certification requirements take into account the overall management of alarms in the cockpit. As regards the automatic pilot, the BEA recommended that clear specifications concerning ILS capture be ensured.

Some other safety recommendations were made by the BEA that mainly concerned aerodrome documentation, ground systems and meteorological and administrative procedures.

4 CONSIDERATION OF NEW ANALYSIS MODEL INTEGRATION

To explain the inappropriate decision by the crew, the BEA focused on systemic factors that may, for instance, have contributed to the pilot's high level of fatigue and the high workload during the approach. Ten years later, it may be useful to try to analyze the crew's behaviour through different perspectives, taking this opportunity to define new models.

Indeed, new models would better account for the complex interaction between the parameters that determine our system and its safety margins. We can suppose that the Captain's situational awareness depended on factors such as his state of mind – fatigue and increasing workload – and on his interpretation of the instrument displays. Since the workload evolved erratically and the instrument displays reflected the motion of the aircraft as decided by the Captain, in response to his situational awareness, these parameters interact non-linearly. Moreover, parameters such as the Captain's situational awareness and the spatial position of the aircraft evolved in different time frames.

The crew was forced into the position of managing a crisis while they were handling the airplane's flight track alone, after the end of radar vectoring by the controller. We can consider that the triggering conditions for such a crisis resulted from the progressive lowering of barriers throughout the flight up until ILS interception: at departure, the composition of the flight crew would only have allowed them to continue the approach as far as the OM, bearing in mind the meteorological conditions at the destination; the Captain's take-over of the controls led him to being cut off; the error in selecting the track on the HSI constituted an additional disturbing factor. It would, however, be reasonable to question the validity of this interpretation. In fact, in the course of the investigation, simulations were performed in a flight simulator with a view to confirm the modes triggered by the crew. They revealed that in a similar situation – wrong track selection – it was possible for a pilot to put the aircraft into a descent that would lead the flight into a deteriorated situation.

In the case of this event, the crisis became apparent as soon as the automatic system was unable to intercept the ILS and the regulatory mechanisms did not make it possible to counter the previous failings. From this moment on, the Captain tried to manage the crisis alone by calling on techniques and means that he knew and to which he usually had recourse.

The disconnection of the AP at 12 h 31 min 26 s by the Captain might be regarded as a marker point in an ongoing process, which in this case led him to the decision to go around. Finally, according to the Captain's statement, the key factor in initiating a missed approach was non-stabilization; neither the altitude nor alarms were taken into account in his assessment. Therefore, it seems that his decision was out of phase in relation to the actual flight sequence.

Thus, it appears that the evolution of this event places it into the category of a resilient process, something that the models traditionally employed in accident investigation make it impossible to develop.

GLOSSARY

LOFT	Line Oriented Flight Training
FMA	Flight Mode Annunciator
GPWS	Ground Proximity Warning System
HSI	Horizontal Situation Indicator
ILS	Instrument Landing System
FO	First Officer
AP	Automatic Pilot
QAR	Quick Access Recorder
OM	Outer Marker
RVR	Runway Visual Range
VOR	VHF Omnidirectional Radio Range

FINAL REPORT

The Final report (French and English versions) is available on the BEA website: www.bea-fr.org

Cybernetics and Resilience Engineering: Can Cybernetics and the Viable System Model Advance Resilience Engineering?

Arthur Dijkstra

KLM Royal Dutch Airlines / Delft University of Technology Netherlands
Arthur.Dijkstra@xs4all.nl

Abstract. Cybernetics as the science of control in the animal and machine provides a paradigm for inquiry into organisational behaviour. Management cybernetics supplies complementary perspectives on managing complexity and organisational performance. Using the Viable System Model (VSM) a qualitative diagnosis can be made of the communication structures in the viable organization. Viability is the ability to maintain the organisational identity in a changing environment. This notion compares well with some proposed aspects of resilience. VSM is suitable for diagnoses of the viability of an organisation and might therefore also be an useful concept for diagnosis and understanding of resilience. A specific function in the VSM scans the organisational environment for threats and opportunities. This "outside and then" function negotiates with the 'inside and now" function of the organisation about adaptation. This seems to be in line with the proposed requirements for resilience such as anticipation, attention and response. This paper proposes further exploration of management cybernetics for possible answers to the challenges of resilience engineering (RE).

1 INTRODUCTION

In my literature study for my PhD on Safety Management Systems (SMS) I am exploring cybernetics and its applications for management. This paper is intended to share my ongoing discoveries and ask the question how cybernetics can support us in finding ways to engineer resilience.

Cybernetics is concerned with communication and control, therefore it seems compatible with recent safety science development akin RE. In the safety science literature, including publications such as Resilience Engineering, concepts and precepts (Hollnagel, Woods & Leveson, 2006), references to the field of cybernetics are not widespread. The most common reference is to the Conant and Ashby theorem (1970) about the requisite variety a control most poses in order to remain in control. Especially, when the notions of safety as used in the RE domain point to notions such as "loss of control", "unexpected interaction between (sub-)systems", I would expect more reference to cybernetics the science of control and communication in the machine and animal (Wiener, 1948).

Cybernetics laws, like gravity, cannot be disregarded. This raises the question how can cybernetics support us in understanding successes and failures of resilience. Remarks for the requirement of "a new language", "higher order variables" and how to model resilience might be to some extend fulfilled by examining the insights from cybernetics.

Since the safety paradigm is shifting to systems theoretical concepts, cybernetics becomes available as a compatible theory to study safety and resilience.

In this paper I will propose a further use of cybernetics. In specific I will address management cybernetics, described by Beer as "the science of which management is the profession". In his study for the invariance's in communication and control and based on Ashby's laws of variety, he developed the Viable System Model (VSM). This model is helpful in designing and diagnosing the organisational structural mechanisms of communications and control. These structures are produced by people's interactions and provide the organisation with its own identity. The ability to keep this identity in a changing environment is a indication of viability. Also a resilient system must have the ability to anticipate, perceive and respond (Hollnagel, Woods & Leveson, 2006) in an environment of scarcity and pressure. In this essay some pointers will be given towards concepts in management cybernetics that may support maturing of resilience engineering.

2 CYBERNETICS LAWS

Cybernetics is concerned with the properties of systems that are independent of their material components, hence the title of the seminal book by Norbert Wiener: "Communication and control in the machine and animal". This makes cybernetics applicable for different systems such as electronics, brains, organisms and organisations.

A critical concept is that of difference. Ashby (1956) uses *Variety as a measure for the number of possible system states* that can be differentiated from each other. Variety itself cannot be counted (Ashby, 1956) but it can be compared e.g. this system has more variety than that system.

Ashby's law of requisite variety states that:"A controller has requisite variety when he has the capacity to maintain the outcomes of a process within targets, if and only if he has the capacity to produce responses to all those disturbances that influence the process". This means that situational variety, as exposed by the system in different situations, must at least be equalled by the response variety of the controller. This is based on the cybernetic law that: **"ONLY variety absorbs variety"** (Ashby, 1956). An example of this is a person driving a car. When the driver is able to keep the car on the road under conditions where his driving is disturbed by other cars and weather conditions the driver is said to have requisite variety. However when disturbances, such as slippery road and a deer crossing the road, result in an accident the driver is said to have had no requisite variety.

3 THE VIABLE SYSTEM MODEL

Viability means the survival or preservation of identity in a changing environment. Beer argues that a system that maintains its existence is a viable system otherwise it would not exist. In a viable system the variety balancing act between environment and organi-

zation seems to function sufficiently. Three elements of a viable system are shown figure 1. For clarity the three elements are shown separate while actual M (management) is part of O (operations) which is part of E (environment). In a viable system the operations, those activities that produce the identity of the organisation (e.g. flights for an airline), are serviced (through e.g. scheduling, accounting) by the management. The operations interact with their relevant environment as does the management. The variety of the environment is larger than the variety of the operations which is larger than the variety of the management. Organisational design must include variety attenuation and variety amplification to provide requisite variety. Communication channels (reports, instructions, discussions etc.) must have a higher capacity to transmit information relevant to variety selection in a given time than the originating subsystem has to generate it in that time. If 'bandwidth' is not sufficient lagging control with its consequences will occur. Furthermore whenever the information on a channel capable of distinguishing a given variety crosses a boundary, it undergoes transduction; the variety of the transducer must be at least equivalent to the variety of the channel. Translation from one language to another is a form of transduction. Recognition of the channel requirements (Beer's (1979) principles of organization) allows effective organisational design.

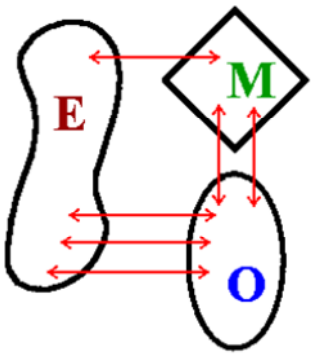


Fig. 1. Variety matching between environment, operations, and management

The VSM describes five organizational functions (Beer, 1979; 1981; 1985) which are *sufficient* and *required* to support viability, these are enumerated as system 1 to 5.

System 1 Primary activities, implementation
System 2 Conflict resolution, co-ordination, stability.
System 3 Internal regulation, monitoring, optimisation, synergy, **3*** Auditing.
System 4 Intelligence, adaptation, forward planning, strategy.
System 5 Policy, ultimate authority, identity

Systems 1,2,3 concern themselves with what is happening "inside and now". System 4 concerns itself with what might happen in the future, "outside and then". The rules of interaction between the two are determined by system 5.

An organisation, such as an airline company, can have viable parts such as passenger transport and aircraft maintenance. Each of these viable parts can have again viable parts in it such as Boeing 777 operations or engine maintenance. This demonstrates the concept of recursion, where viable systems are embedded in viable system and we can shift from one system-in-focus, to a higher or lower system-in-focus. In Fig. 2 two viable systems are embedded in the system 1 of the system-in-focus. The number of recursions to shift up or down depends on the goal of the analysis.

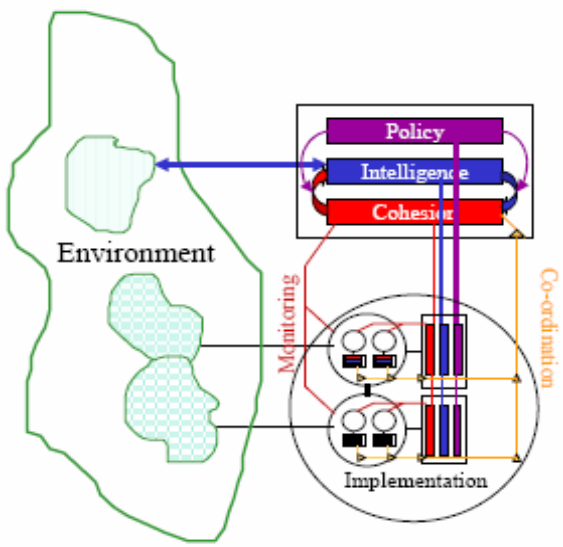


Fig. 2. The Viable System Model

The VSM is not an organizational chart but it models the structural communication channels and interactions between the different organizational functions. Therefore the VSM can be used as a diagnostic tool to evaluate the organizational fitness or viability.

4 RESILIENCE FROM A CYBERNETICS PERSPECTIVE?

I want to compare some quotes from the domain of RE with notions of cybernetics and VSM which may support further RE development.

1. Hollnagel & Woods (2006) state: "... resilience can be described as a *quality of functioning*. has two important consequences.
   A. "they must also be resilient and have the ability to recover from irregular variations, disruptions and degradation of expected working conditions..."
   B. ...Resilience engineering instead requires a continuous monitoring of system performance, of how things are done. In this respect resilience is tantamount to coping with complexity and to the ability to retain control..." (pp. 347-348)
2. "Resilience as form of control: ... In order to be in control it is necessary to know what has happened (the past), what happens (the present) and what may happen (the

future), as well as knowing what to do and having the required resources to do it..." (Hollnagel & Woods, 2006, p. 348)

Below are notions from cybernetics referencing to the two descriptions of RE aspects.

- Ref 1.A: Continuation of processes and ability to absorb perturbations and adaptation appear common in my understanding of resilience and viability. Cybernetics approaches on perturbations, even when originating from outside the design base, have been described by Ashby (1956) with *ultra-stable* homeostasis. Such a system is capable of resuming a steady state after it has been disturbed *in a way not envisioned* by its designer (Beer, 1966).
  Ref 1.B: An understanding of resilience engineering in terms of VSM would include adequacy of system functions to manage variety and the relationship between levels of recursion and requisite variety. Without adequate VSM system functions, e.g. system 4, an organisation might lack ability to respond to environmental changes such as market or technological changes. A underdeveloped function to scan the environment for threats and opportunities will most likely reduce viability and result in more surprises by unanticipated events thus increase demand for resilience.
  The ability to retain control is determined by "available" requisite variety. Leonard (2006), in her comparison of VSM and a risk model, refers to resilience as "*Resilience and survival choices* are the steps that are taken to prepare for the possibility of a catastrophe or sudden change such as cash reserves, computer back-up, security plans and developing robust, redundant communications channels and skill sets. Again, these choices are made by Systems Three, Four and Five but are implemented by System Two and the System One operations. System Three Star may periodically check that these provisions are being followed and are up to date."
  By increasing the level of recursion the organisation increases its variety handling capability. The different levels of recursion in the VSM are *not hierarchical* but more or less autonomous, connected by cohesion to the levels below and above, which increases responsiveness, which is critical aspect of resilience. It might be useful to analyse how the VSM can serve as a model to understand and recover from failure.
- Ref 2: Continuous system performance monitoring (failures and successes) to remain in control as in RE is also applicable to the concept of the VSM operations room or management cockpit for (almost) real-time control of the organisation. The question is of course what indicators or control variables should be used. VSM offers functional systems that can be monitored for their adequacy which brings us one step closer to developing metrics. Also the adequacy of the communications channels to transfer and transduce variety are sources for metrics. The framework of the VSM in combination with a compatible business model offer a way of assigning meaning to the metrics which are closely related to viability and therefore also to resilience.
  In the early 1970's Beer had almost completed an operations room to control the economy of Chile when the project was stopped by the military coup to replace president Allende. Currently a management cockpit, also based on cybernetic and VSM principles, is commercially available.

- Ref 2: Resilience as form of control is compatible with cybernetics the science of control and communication. Cybernetics has also been described as: A framework to make intentions happen" We know that predictions about the future are inadequate and this make it more relevant to have a control system when targets are set. With use of performance monitoring, deviations are recognised and control actions can be executed. VSM offers a structure for assigning control commands.
  The VSM explicitly has a functional description of dealing with the present, "inside and now" (system 1,2,3) and the future, "outside and then" (system 4). The sytem3 - 4 homeostat is the organ of adaptation for the organisation. The balancing of variety between the organisation and the environment is essential for maintaining requisite variety and thus staying in control. Comparison of the multi level Extended COntrol Model (ECOM, Hollnagel & Woods, 2005), which uses competence, control and constructs to model performance, and VSM could reveal interesting analogies.

5 CONCLUSION

Cybernetics and VSM appear, at least on first sight, to be closely related and therefore applications of cybernetics and VSM might be useful in applications of RE. This is not strange when considering the commonality in background of e.g. systems theory. Spare variety could be the expression for resilience in cybernetic language. This opens a whole arena of existing cybernetics scientific research that may be further developed for resilience specifics.

The maximal length of this paper limits the depth of the topic but in my PhD project on the development a Safety Management System I will further analyse the management of safety and resilience using cybernetics and the VSM.

REFERENCES

Ashby, W.R. (1956). *An introduction to cybernetics*. London: Methuen.

Beer, S. (1966). *Decision and control*. Chichester: Wiley.

Beer, S. (1979). *The heart of enterprise*. Chichester: Wiley.

Beer, S. (1981). *Brain of the firm*. Chichester: Wiley.

Beer, S. (1985). *Diagnosing the system for organisations*. Chichester: Wiley.

Conant, R. C. & Ashby, W. R. (1970). Every good regulator of a system must be a model of that system. *International Journal of System Science, 1* (2), 89-97.

Hollnagel, E. & Woods, D. D. (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. Boca Raton, FL: Taylor & Francis.

Hollnagel, E. & Woods, D. D. (2006). Epilogue: Resilience engineering precepts. In E. Hollnagel, D. D. Woods & N. Leveson (Eds), *Resilience engineering: Concepts and precepts* (pp. 347-358). Aldershot, UK: Ashgate.

Hollnagel E., Woods D. D. & Leveson N. (Eds). (2006). *Resilience engineering: Concepts and precepts.* Aldershot, UK: Ashgate.

Leonard, A. (2006). A comparison of the Viable System Model and seven models of risk with the effects of the Sarbanes-Oxley legislation. *Journal of Organisational Transformation and Social Changes, 3* (1), 85-93.

Wiener, N. (1948). *Cybernetics, or control and communication in the animal and the machine*. Cambridge, MA: The MIT Press, and Wiley.

Resilience in Usability Consultancy Practice: The Case for a Positive Resonance Model

Dominic Furniss[1], Ann Blandford[1] and Paul Curzon[2]

[1] UCLIC, 31/32 Alfred Place, London WC1E 7DP, UK
{d.furniss, a.blandford}@ucl.ac.uk
[2] Queen Mary, University of London, Dept. of Computer Science, Mile End, London, E1 4NS, UK
pc@dcs.qmul.ac.uk

Abstract. Usability evaluation methods (UEMs) play a central role in usability consultancy practice. Their adoption and adaptation plays an important part in making systems more resilient. There is a knowledge gap in how practitioners adopt and adapt UEMs. Wixon (2003) goes as far as to say that the current literature fails the practitioner. Work reported here builds on qualitative research on usability practice. The conceptual framework of resilience engineering can help bridge this gap. However, resilience engineering is typically focused on avoiding accidents at the lower end of performance: e.g. when system resources are too stretched or when system variability leads to failure. We argue that a better way of conceptualizing UEM use is for the maximization of impact on design at the high end of performance. Here practitioners adopt and adapt methods to resonate with the project, people and practices of the host company under constrained resources. This reasoning leads us to introduce and apply a positive resonance model to capture this perspective.

1 INTRODUCTION

Usability practice has a broad scope: encapsulating ergonomics and human factors work. Common to these practices is the motivation to make systems safer and more usable. A central part of this work is the employment of usability evaluation methods (UEMs) to test how safe and usable systems are, so results can be considered in the design process. Two related problems motivate our work. 1) Wixon (2003) argues that the literature fails the practitioner as academia evaluates UEMs on how many problems they find, while practitioners value methods by what can be done with constrained resources to maximize the beneficial impact on the product. 2) UEMs developed in academia are rarely adopted in practice (Bellotti, 1988; O'Neill, 1998). By understanding UEM adoption and adaptation by practitioners, in their terms, we hope to determine how the literature and UEM development can become more appropriate to practice.

Identifying what is important for the adoption and adaptation of UEMs from practitioners' perspectives has led us to analyse the wider context of usability practice. Furniss *et al.* (in press) report an earlier stage of this project that moved away from valuing methods for the number of problems found towards building a picture of the context in which UEM adoption and adaptation is embedded. Results were reported under four main themes: the methods and processes within the design and business context; the relationships between roles and people involved in the work; issues of communication and coordination of resources and information; and the psychology and expertise of

those involved. The analysis concluded that usability practice is usefully conceptualized from a system level where the goal is to coordinate resources to add value to design.

In this paper, we illustrate how resilience engineering concepts are reflected in the data and introduce the case for a positive resonance model. This builds on the work of Hollnagel (2004) who introduced the concept of how functional parts of a system can be considered to resonate together. This begins to address the need for a system level perspective of usability consultancy practice to understand UEM adoption and adaptation, which will contribute to the development of more resilient systems.

2 METHOD

The work reported here is an ongoing qualitative analysis based on interviewing usability practitioners about their work (the guiding topics of the semi-structured interviews can be found in Table 1). Usability practice in two contrasting contexts are being compared: website design, and safety-critical system development. Fourteen practitioners have been interviewed thus far (10 from the website design context and 4 from safety-critical systems development).

Table 1. Semi-structured interview topics used for usability practitioner interviews

Topic	Description
Background	Background of the person being interviewed. This aims to introduce the interviewee slowly and find out about their experience and perspective.
Work Organization	This includes how work is organized, the structure of the organization, whether there are teams, project lifecycle involvement, and what job challenges are faced.
Business: Client Relationships	This includes communicating with clients, both in attracting clients and handing work off to them. How do people communicate and what challenges do they face?
Practitioner skills	What do practitioners do, why are some better than others and how do they get better in their role? This could give an indication about what is important in their work.
Tools and techniques	What methods are used, how are they used, when are they used, what is valued in a good technique?

Grounded Theory (Strauss & Corbin, 1998) was used for the interviews and analysis: here the interviewees' perspective is put to the fore and theory is developed and tested through iterative interviews, transcribing, coding and analyzing by recognizing patterns in the data. The data builds from the practitioners' perspective and addresses the banality of their normal performances, both recognized as important by Dekker (2005). Resilience engineering presented itself as a potential lever for understanding the data since its conceptual ideas could be 'seen' in the data i.e. the theory captured and crystallized emerging insights.

3 RESILIENCE ENGINEERING LINKS

Five resilience engineering themes have been identified in the ongoing analysis of our data on usability consultancy practice. Each theme is discussed with relation to theory, supporting data and discussion.

1) Efficiency-thoroughness trade-off (ETTO). Theory: Hollnagel (2004, p. 152) and Dekker (2005, p. 144) both quote NASA's "Faster, Better, Cheaper" organizational philosophy to illustrate the problem of multiple competing goals in a system. **Support:** This is evident in usability consultancy practice. For example, one interviewee recognized that a previous company would overwork her to win contracts so she left. She is now in a company that project manages more fairly without staff having to stretch and stretch. It is also evident that usability practitioners want to use more UEMs but are restricted by client budgets and willingness. **Discussion:** This places the project design phase in a position of great importance as this is when options are discussed, plans made, and resources negotiated.

2) Loose coupling. Theory: Grote (2006, p. 116) states that "a core requirement for resilience is to achieve an adequate balance between stability and flexibility in the functioning of an organization." **Support:** This is evident in the labeling of techniques and methods that add stability to a design project, and where their practice can be adapted to suit the context. For example, Heuristic Evaluations (Nielsen, 1994) were reported to be used in an ad hoc manner to support design recommendations, explicitly used to evaluate and compare websites, implicitly used like an expert evaluation, and actual heuristics were sometimes adapted from "Nielsen's ten heuristics." **Discussion:** The loose coupling evident in labeling simplifies communication of project elements and structure to clients. According to our interviewees, novices (e.g. clients) are less able to cope with the details of potential project variances. Labels and prescriptions help overcome this.

3) Adaptability and Flexibility. Theory: This theme is reflected in Sundström and Hollnagel's (2006, p. 253) definition of resilience: to "adjust effectively to the multifaceted impact of internal and external events over a significant time period." **Support:** This was evident because practitioners would often say "it depends…" when questioned about their choice of methods. This alludes to the important contextual factors in UEM adoption and adaptation. **Discussion:** Furniss *et al.* (in press) state that usability consultancy can usefully be considered as a 'plug and play technology'. This is because services are flexible and adapt to the requirements of the project and the client. UEM adoption and adaptation is a negotiation between internal and external pressures.

4) Survivability and Different Dimensions of Resilience. Theory: A theme from the 2nd Resilience Engineering Symposium was that different dimensions of resilience should be considered e.g. survivability of an organization is a balance between not only resilience in safety, but also in economics so it can carry on as a business. **Support**: Respondent quotation: "one of the realities for commercial usability is that products that survive for a long time in a market place have to fulfil both the customers' needs and the business's[…]." **Discussion:** Survivability should consider the safety, usability, and business case. Too much of a focus on one of these could lead to a detriment of the system overall.

5) Local Rationality. Theory: Dekker (2005, p. 60) argues that context is central to the "local rationality principle (people's behaviour is rational when viewed from the inside of their situations)." **Support**: Valuing UEMs in practice has been found to rely on other factors other than the number of problems that can be found. **Discussion:** In a sense Wixon's (2003) argument concerning the lack of relevance of academic literature to practitioners is due to a lack of proper consideration of the practitioners' local rationality. This research aims to provide insight into the local rationality of usability practitioners in their adoption and adaptation of UEMs, and it is proposed that to do this adequately we need a positive resonance model.

4 THE CASE FOR A POSITIVE RESONANCE MODEL

Resonance plays a central part in the systemic Functional Resonance Accident Model (FRAM) (Hollnagel, 2004). An example of resonance common to most people's experiences is a playground swing (Hollnagel, 2004, p. 160). Children soon learn that they have to apply energy at the right moment in the swing to carry the energy through and amplify the swing. In this sense the applied energy 'resonates' with the swing. Children might also decrease the amplitude of the swing by applying energy against its natural frequency of oscillation. Hollnagel (2004, p. 165) then discusses stochastic resonance, which can be described as noise in a system that can be quite unpredictable and enhance or decrease signals depending on its variance; and functional resonance (Hollnagel, 2004, p. 170) which "does not depend on an unknown source but is a consequence of the functional couplings in the system." The FRAM model takes a systemic view of accident prevention by examining the functional resonance between different parts of a system, and looking for critical variances of that system that might resonate in unwanted ways. In this conception of functional resonance, the safe functioning of a system should lie within a certain threshold so it does not become uncontrollable. Some resonance may be beneficial in that the system can learn and adapt from the variance. Generally, however, if functional parts of the system have variance that resonate together then the activity can go over the threshold and the system can fail. Such resonance is therefore generally unwanted.

The conception of a plug and play usability component that adapts to fit the host company, people and project suggests that consultancy practices should aim to positively resonate with them. They should apply their resources at the time and place that maximizes the push on the project. By doing this usability consultancies have better survivability and resilience, and have a greater impact on making systems resilient themselves.

5 SUMMARY

We have created an interpretive bridge between the qualitative analysis of usability practitioners and the resilience engineering literature. This relates to Dekker's (2005, p. 192) statement that "Validation emerges from the literature (what others have said about

the same and similar contexts) and from interpretation (how theory and evidence make sense of this particular context)." We have shown how resilience engineering concepts are reflected in our data and proposed a positive resonance model. This captures the way usability consultancy services adapt and fit the host company, people and project to maximize their impact under constrained resources, therefore being more resilient themselves and creating a greater potential to make systems more resilient.

ACKNOWLEDGEMENTS

We are grateful for time that the interviewees contributed for this study. The work is funded by EPSRC Grants GR/S67494/01 and GR/S67500/01.

REFERENCES

Bellotti, V. (1988). Implications of Current Design Practice for the Use of HCI Techniques. In *Proc. BCS IV* (pp. 13-34).

Dekker, S. (2005). *Ten questions about human error: A new view of human factors and system safety*. London: Lawrence Erlbaum Associates.

Furniss, D., Blandford, A. & Curzon, P. (in press). Usability work in professional website design: Insights from practitioners' perspectives. In Law, E., Hvannberg, E., and Cockton, G. (Eds.). *Maturing usability: Quality in software, interaction and value*. Springer.

Grote, G. (2006). Rules management as source for loose coupling in high-risk systems. In *Proc. of the Second Resilience Engineering Symposium* (pp. 116-124).

Hollnagel, E. (2004). *Barriers and accident prevention*. Ashgate Publishing Company.

Nielsen, J. (1994). Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.), *Usability inspection methods*. John Wiley & Sons, New York, NY.

O'Neill, E. (1998). *User-developer cooperation in software development: building common ground and usable systems*. PhD Thesis. QMWC, University of London.

Strauss, A. & Corbin, J. (1998) *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2nd ed.). Sage Publications.

Sundström, G. & Hollnagel, E. (2006). Learning how to create resilience in business systems. In E. Hollnagel, D. Woods & N. Leveson (Eds.) Resilience engineering. Concepts and precepts. Cited in Sundström, G. & Hollnagel, E. (2006). On the art of creating and managing policies: Facilitating the emergence of resilience. In *Proc. of the Second Resilience Engineering Symposium* (pp. 304-312).

Wixon, D. (2003). Evaluating usability methods: Why the current literature fails the practitioner. *Interactions, 10* (4), 28-34.

Pragmatic Resilience

Jonas Lundberg and Björn Johansson

Department of Computer and Information Science, Linköpings universitet, Sweden
{jonlu, bjojo}@ida.liu.se

Abstract. There are different approaches to achieving persistence in system safety functions in the face of disturbances. Whereas some systems strive towards only maintaining stability of one stable state of maximum performance, other systems also rely on resilience, on the ability to make transitions to other stable states, of lower performance, when facing changes to driving variables or state variables. We discuss three kinds of systems, stable, bi-stable, and multi-stable systems, and their persistence when facing regular, irregular, and unexampled events.

1 INTRODUCTION

The aim of resilience engineering is to achieve persistence in systems functions in the face of disturbances. In particular, we are interested in persistence of the safety functions of the system. The focus thus lay on persistence of functions, rather than persistence of physical components that realize the functions. When engineering the resilience of a system, it is vital to balance the ability to achieve stability in the face of regular disturbances and threats, with the ability to achieve adaptive behavior when facing more irregular or unexampled events (Lundberg & Johansson, 2006). That can be summarized as

- The ability to respond, quickly and efficiently, to regular disturbances and threats.
- The ability continuously to monitor for irregular disturbances and threats, and to revise the basis for the monitoring when needed.
- The ability to anticipate future changes in the environment that may affect the system's ability to function, and the willingness to prepare against these changes even if the outcome is uncertain.

To engineer resilience, we need to know something about the variables we wish to control, and something about the variables that might be in flux. If these are well-known, the principal strategy may be increased stability. Physical barriers and safeguards are primary examples. If they are less well-known as in irregular events, the primary strategy may be to control the transitions between states of stability, to avoid both long periods of instability, and states of functional extinction. Examples of that may be to go from a stable up-time state of a nuclear facility, to a stable down-time state. Furthermore, the exact state to reach or how to manage the transition, may be partly unknown at the time of the event, and may have to be invented as the event unfolds, such as in the flooding of New Orleans. When ecologists use the term resilience, the variables that describe the system are called state variables, and those state variables that affect other variables, are called driving variables. For instance, economy and the acceptance of

risks are often seen as important driving variables for safety, affecting the states of many other variables, such as the existence of backup resources, or physical safeguards.

What we will discuss in this paper is different kinds of systems, and how they are characterized in terms of their ability to perform transitions between different functional states. We will also discuss some of the driving variables that affect the viability of safe transitions.

2 WHEN AND WHY IS A SYSTEM RESILIENT?

A system can be described in terms of functional states and state variables, together with state transitions (Ashby, 1960). State transitions can be described in terms of the variables that drive the system from one state to another between different stable states, or towards extinction (non-function in terms of functional states). Systems can also be described in relation to different event types in their environment that affect state variables or driving variables. This will be elaborated below.

2.1 Transitions between Functional States

A 'functional state' is a level of performance that a system can achieve under specific performance conditions. For example, an air traffic control center can, under normal operating conditions (equipment fully operational, normal weather, fully manned) handle a certain number of flights. In the case of a breakdown in for example a technical system needed for handling flights, performance will be hampered and this number will be reduced. The system will move from one functional state to another. However, as the observant reader notices, it is not self-evident that such a transition is possible. First of all, there has to be state to make a transition to. Secondly, some type of safe way to perform the transition must exist. A common approach to this is to keep an old technical system, with a certain performance level, operational when introducing a new one with a higher performance level. As long as the old system is operational and the personnel know how to use it, it will be possible to step back to it.

2.2 Driving Variables

The ability to make transitions between different functional states is essential for anyone that aim at creating a viable system. But the system characteristics promoting this ability must also be created and maintained. The driving force behind this, or the 'driving variable', is, in theory, safety. By creating barriers, redundancy and capacity for coping with different kinds of events, we improve stability and resilience. However, we must not forget that the driving variables in most real-world systems are not safety nor resilience, but rather other things such as profit, simplicity and complacency. When suggesting to a company CEO that safety should be improved, the first question is not likely to be "how?" but rather "how much will it cost?". When instructing a worker on the factory floor that he/she should check his/her equipment every day, he/she may firstly be enthusiastic, but when some time has passed, the checks are likely to become

more rare, or even stop completely. Although there are examples of highly reliable organizations, even those sometimes have accidents, and such accidents often have high consequences.

2.3 Stable, Bi-Stable, and Multi-Stable Systems

To exemplify the difference between stability and adaptivity through the transition between states, we can consider three kinds of systems, *stable, bi-stable* and *multi-stable systems*. These systems can in turn have control systems, which may be in need of protection, an issue that is termed the Matryoshka problem. That problem is discussed in detail in Lundberg and Johansson (2006). The state variables of a system, for instance the number of fire trucks in a fire brigade, are driving variables for the function of controlling fire, in a forest fire-fighting situation. The state variables of the system in turn have driving variables, such as economy. In the following three examples we describe the stable, bi-stable and multi-stable system types. We consider stable states to be states where the system has some level of functioning, whereas the alternative is states of functional extinction. The levels of performance may differ between stable states, and we assume that most systems strive towards states of as high performance as possible, while still being safe.

Firstly, we have the *stable system*. Here, stability is increased by defenses such as barriers that deflect damage, and by having spare resources, giving slack to the system. For instance, there might be resources for buying new kinds of equipment, or many spare parts for equipment. The idea here is to re-establish the previous control organization as soon as possible. This system does not adapt to unknown circumstances, only to the previously foreseen. The resources are driving variables, whereas items and people in the system are state variables. The key characteristic of a stable system is that is *stable in relation to one state*, to which it constantly tries to come back.

Second, we have the *bi-stable system*. This system may for instance be prepared for a loss of hierarchical control, where top level nodes are lost. The preparation could for instance consist of exercises in independent actions of remaining nodes, and establishment of cooperation between nodes. The state of instability is the transition stage, during which the functionality is not working as in the stable states. In this example, the state of instability might persist, if also one or more of the lower level nodes are damaged. The system can thus *strive towards a limited set of different states*, depending on damage to the state variables. Driving variables of the transitions are for instance resources and redundancy of skills to take up the roles needed for the alternative states.

Third, we have *multi-stable systems*. For instance, rescue services might need many different kinds of configurations, depending on the situation they face. Preparation is also in this case exercises in establishing different organizational setups, but it is done more thoroughly than in the preceding case. A multi-stable system can thus *adapt to a number of different states*. In this case, the driving variables are things like the economical resources for achieving more external resources, and the state variables are associated with the size of the event. If the size of the event surpasses the ability of the organiza-

tion, it might loose functionality, to the extent of complete loss of functionality (extinction). Another typical characteristic of multi-stable systems is the ability to reconfigure, or join up with other systems, forming an ad-hoc configuration with different capacities than the individual parts. The system might also be able to invent new ways of coping, increasing its performance.

2.4 Events

Systems may be subjected to events that affect the state variables or the driving variables. Ron Westrum describes three different types of events that can be related to resilience, *regular, irregular* and *unexampled* events (Westrum, 2006). The regular event is well-known, for example machine failure or bad weather. Irregular events are possible to imagine, but are normally so rare (or expensive to handle) that little specific preparation is taken. Earthquakes, large fires or chemical outlets are typically mentioned as examples of irregular events. Unexampled events are so rare that normally no organized mechanisms for coping with them exist. The 9/11 terrorist bombing or the flooding of New Orleans are often mentioned as examples of unexampled events. If a system is to be considered as 'safe', it needs to present stable characteristics in the face of regular events, a mixture of resilience and stability in the face of irregular events and finally high resilience when facing the unexampled.

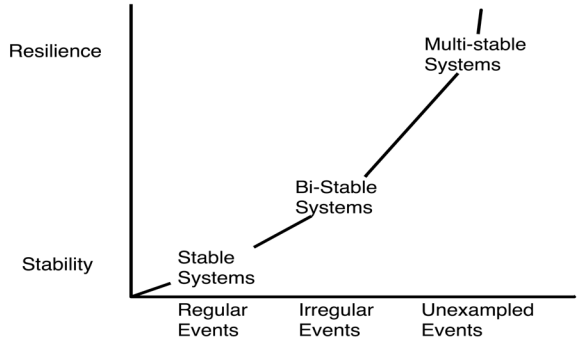


Figure 1. The relation between Westrum's event types and the different system types in relation to the stability-resilience continuum.

There is thus a connection between the stable, bi-stable and multi-stable systems and the event types (see figure 1.). In other terms, a 'safe' system must match the variety of its environment, as in the case of the law of requisite variety described by Ashby (1956). Different types of systems have different abilities to do this by practically coping with changes in the environment (McDonald, 2006).

3 DISCUSSION - PRAGMATIC RESILIENCE

To engineer resilient systems in the face of regular, irregular, and unexampled events, we need strategies for engineering state transitions, and for monitoring the driving variables that make safe state transitions possible. Due to the Matryoshka problem and the

occurrence of unexampled events, we can never be completely safe. However, we can strive towards maximizing the safety of each system that we in practice can affect. Epstein pointed out the logical problem that resilience is something that cannot be measured until the fact of impact (Epstein, 2006). This is true in one sense, but not very helpful from a resilience engineering perspective. Instead, we suggest another approach: on the one hand, we may be unable to foresee some kind of events, like unexampled ones. On the other hand, we can always ask our selves what will happen if a system is exposed to a disturbance or loose its intended functional state, regardless of the cause. Since we are aware that things that cannot be predicted are bound to happen it is far easier to simply try to describe what happens if one or more stable states are lost than to try to predict all possible disturbances and prepare for them. As long as some possible state to move to exists, the system at least has a theoretical possibility to survive.

A last important point is the fact that systems are vulnerable and low performing when they are in a state of transition between stable states. Transitions may also be characterized by uncertainty, especially in multi-stable systems if the system adaptively is searching for a stable state. The duration of the transition is another factor: if the time needed to make a transition is very long, the system may be of little or no use during that time. To promote the ability to make rapid transitions is thus essential if the system operates in a context where time is limited, as most safety-critical systems do.

REFERENCES

Ashby, W. R. (1956). *An introduction to cybernetics*. London: Chapman & Hall.

Ashby, W. R. (1960). *Design for a brain: The origin of adaptive behavior* (2nd ed.). London: Chapman & Hall.

Epstein, S. (2006). Unexampled events, resilience and PRA. In E. Hollnagel & E. Rigaud (Eds.). In E. Hollnagel & E. Rigaud (Eds.), *Proceedings of the Second Resilience Engineering Symposium* (pp. 105-116), Antibes, Juan-les-Pins, France, 8-10 Nov.

Lundberg, J. & Johansson, B. (2006). Resilience, stability and requisite interpretation in accident investigations. In E. Hollnagel & E. Rigaud (Eds.), *Proceedings of the Second Resilience Engineering Symposium* (pp. 191-198), Antibes, Juan-les-Pins, France, 8-10 Nov.

McDonald, N. (2006). Organizational resilience and industrial risk. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 155-179). Aldershot, UK: Ashgate.

Westrum, R. (2006). A typology of resilience situations. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (pp. 55-65). Aldershot, UK: Ashgate.

Trials and Tribulations: The Building of a Resilient Organization

Jan Skriver

Resilience AB, Knivsta, Sweden
jan.skriver@resilience.se

Abstract. Resilience engineering has emerged as a new approach to safety and risk management emphasizing the importance of proactive, anticipative and adaptive organizational behavior thereby distinguishing itself from the traditional approaches of PSA and accident analysis. In contrast to the traditional approaches that frequently artificially separate topics, the approach provides a theoretical synergy of safety and risk management principles that reflect the practitioner's everyday goals and challenges. This paper sets out to present a case study of the intricacies of building a resilient organization. Focus is on the challenges that may interfere with the creation of a resilient organization, e.g. power struggles, incompatible goals, competence, censorship, business culture, management fads, academic discussions, compromises, campaigns, failure to learn from near-misses and accidents, short term economical versus long term safety goals, and poor corrective actions. The challenges will be discussed and illustrated with examples. Based on the author's experience building a resilient organization is not easy despite the best intentions.

1 INTRODUCTION

Building a resilient organization is easier said than done. Safety goals frequently become entangled with other organizational goals and safety is gradually downgraded over time in a continual battle for supremacy. Why safety originally was seen as important and needing prioritization is soon forgotten amongst the need to earn money and desire to reach production targets. Even the experience of recent incidents and accidents can rapidly be forgotten. This is despite the prevalence of organizational visions of safety first or zero incidents and accidents.

A significant role is played by the organization's business culture. The organization's business culture provides the goals and boundaries to work within but is affected by external influences such as industry regulators, political decisions and particularly when it comes to safety, media interests and attention stirring popular opinion. This is often seen in the aftermath of large-scale incidents and accidents in which regular witch-hunts can result from the media's need to 'define and assign' responsibility and to identify scapegoats. Engineering resilience in such situations requires a systematic approach that emphasizes organizational foresight and adaptability (Hollnagel et al., 2006), which may be difficult when the consequences of the past looming in the background.

This paper presents the trials and tribulations of a practitioner attempting to engineer resilience in an organization in the aftermath of two large-scale accidents. It discusses issues that are inherent in almost every organization and which cannot be dismissed. No attempt has been made to refer to specific resilience engineering models rather to em-

phasis the challenges associated with applications in the practical environment. The list of challenges is far from exhaustive but reflect those of central relevance to the case in focus.

2 THE CHALLENGES

In the first quarter of 2000 a Scandinavian railway operator experienced two large-scale accidents: a collision between two passenger trains resulting in 19 fatalities, and a collision between two freight trains resulting in a long lasting gas fire and the risk of a BLEVE (Boiling Liquid Expanding Vapor Explosion). (This explosion could have potentially destroyed everything within a 500 meter radius, and occurred at the railway station of a town with a population of approximately 50 000.)

Despite having experience two large-scale accidents within a short time period, building a resilient organization soon became submerged under everyday preoccupations. This next section will describe some challenges the organization faced as it attempted to bounce back after the accidents as seen from the author's perspective.

2.1 Power Struggles

Despite what could be expected, experiencing large-scale accidents is unfortunately not always enough for organizations to show a willingness to lay aside existing internal conflicts (even at an individual level). In the aftermath of accidents, organizational changes are often one of the first steps to be taken to rectify the perceived causes. Frequently the CEO and her nearest colleagues will resign (voluntary or involuntary), leaving a void waiting to be filled. This unfortunately leads to a change of focus from correcting the causes of the accident and improving safety in the organization to individuals positioning themselves for managerial roles in the new hierarchy. Corrective actions become a task for lower and middle management, often in safety related positions, whereas top management change focus to the upcoming power struggles. Consequentially safety receives less attention than deserved and becomes less of a priority.

Power struggles can also take a different form. The strength of some trade unions can be of such dimensions that safety initiatives end up as compromises so that the balance between different trade unions and management remains the same. For example, following the train accidents, the railway operator decided to make changes to the departure procedure. The departure procedure had previously been changed to reflect the introduction of ATC (Automatic Train Control) on the lines. The conductor's role as a second barrier therefore became obsolete. Since ATC was only installed on the main lines, non-ATC lines relied on only one barrier for preventing accidents - the driver.

The organization conducted a risk analysis in which three alternatives were evaluated. The best solution was chosen and presented for the two trade unions (drivers and conductors). However, one problem arose. The suggested change to the procedure involved a change of power from the driver to the conductor. This was seen as unacceptable by the drivers union and in the end a compromise was reached, which involved selecting

the third safest procedure that maintained the prevailing power distribution. The procedure was still an improvement from the then present situation but power struggles clearly came in the way of safety.

2.2 Incompatible Goals

Incompatible goals exist in all organizations. Railways are customer-centered organizations and customer needs often take priority. Arriving and departing on time is central to a successful railway organization and reliability statistics are often presented at stations and on web pages as the first contact point between the customer and the organization.

The importance of time becomes an important signal the organization sends to both customers and personnel. Safety is rarely visible and is only mentioned in connection with accidents or incidents. For the driver this presents a problem, as delays are unwanted and create external (through traffic control centers communication) and internal (through a desire to run on time) pressures that ultimately create stress and increase the potential for SPAD (Signal Passed At Danger) incidents.

How priorities are communicated and followed-up in organizations is paramount. Communicating a safety first message will have limited success if managers and personnel are assessed on productivity. This requires awareness and attention from top management but is seldom understood or acted upon.

2.3 Competence

In many large organizations, safety departments consist of personnel who have worked their way up through the system. Their knowledge and skills are often unique but they frequently lack the safety science knowledge and skills required to work systematically with safety in order to build a strong and reliable organization. Hiring academically trained safety personnel is therefore often necessary to ensure that safety is managed systematically.

In the example referred to here, the organization improved the competence level of its safety organization and its place in the organization in the aftermath of the accidents. This was partly due to an internal awareness that improvements were required, but also externally by demands made by the regulator. The new safety department reported directly to the CEO and led to the safety department becoming a strong force in the organization. In the next two years the level of safety was improved significantly. However, internally many held the opinion that the safety department had became too dominant a force, which in turn created power struggles. Not everyone considered the increased competence and strength of the safety department as positive.

It took less than two years for the organization to forget the reasoning behind the need for a strong safety department. Internal disputes began to take priority over competence needs. The bigger picture was blurred and after two years (and two reorganizations later), the safety department was relegated in the hierarchy as a result of internal power struggles. Many of the higher qualified safety personnel employed after the accidents

left the organization, taking with them the competencies required to engineer a resilient organization.

2.4 Censorship

Censorship takes many shapes both voluntary and involuntary. Sometimes organizations do not wish to see the results of accident investigations because they point the finger at the higher echelons. At other times organizations seek scapegoats and wish to ignore the influence or failings of the system as a whole. Censorship may also be driven by the knowledge that the information will become available externally in the public domain.

Making the result of accident investigations public puts pressure on the organization both at individual (the people involved) and managerial levels (the people ultimately responsible). Willingness to learn is suddenly confronted by mass media criticism and its translation of events.

In 2002 the national Accident Investigation Board (AIB) was enlarged to include the railways. Operators and the infrastructure owner had to report and make their investigations accessible to the AIB to which the public had unlimited access. The result was that the operator decided to change the format of its accident reports so that these consisted primarily of a sequence of events description. Deeper analysis was kept as internal notes, however, it did not take long before the internal notes were perceived as superfluous by the management, as the criticisms included were seen as undesirable. Thus, a good accident investigation system faltered because the culture of the organization with respect to openness and willingness to face the facts did not match the good intention of the AIB to learn from accidents.

2.5 Business Culture

Organizations have cultures that reflect the primary goals to be attained whether financial, safety, environmental or quality. The business culture defines what is important in the organization and consequently how safety is prioritized. Separating safety from production is theoretically possible but practically impossible, as all decisions made in an organization in some way will reflect on safety. Working to improve safety must therefore be done in the light of the many internal and external influences affecting the organization. These are often not safety related and a first step to improve safety within a business culture is to make management understand that organizations work as complex systems where each decision impacts far beyond is direct target.

Selling the systemic perspective in an organization is not easy. Managers frequently see their roles as unique and independent of other functions in the organization and have problems accepting their direct or indirect influence on safety matters. If their decisions lead to success in the organization as a whole they happily take responsibility but if the decisions lead to failures or accidents they are less willing to accept responsibility.

In the aftermath of the accidents described, the safety department attempted to introduce a systemic perspective but found little acceptance in the organization. Not because of unwillingness amongst management to accept a systemic perspective but because of power struggles and territoriality. The resilience to change in the organization was far greater than the need for improved safety performance.

2.6 Management Fads

Campaigns, in particular poster campaigns are seen in most high reliability organizations as a tool to keep personnel informed and attentive to safety issues. As with most attitudinal campaigns the effects are short lived and rarely make a mark on behavior. In fact some organizations use too many poster campaigns and create a negative effect, as personnel do not see the point since the campaigns are rarely supported by any actions.

Behavioral intervention campaigns are stronger and will if supported over a longer time have an impact, e.g. Statoil's *Safe Behaviour Programme* (Statoil, 2007). This program was commenced in 2003 and has had to date more than 29.000 participants from the Statoil Group. Unfortunately many behavioral intervention programs are one offs and effects remain short term.

Other management fads e.g. organizational models, customer focus etc., can also impact on the organization in a negative way. In the last decade safety management theory has placed safety as part of the responsibility of line management. Whether this is right or wrong is difficult to say but the result has often been that line managers have been given increased responsibility but not adequate resources to take on this responsibility. At the same time safety departments have been reduced in size since there no longer is a need for the specialist in the organization, e.g. NASA (Rollenhagen, 2005). The drive to improve safety may also be used as a form of efficiency drive.

In the aftermath of the accidents the railway operator started a traffic safety campaign to improve understanding of behavioral issues. The campaign consisted of a single day's training and was to be available for the entire organization. The campaign was considered successful, however, the main group of personnel, the train drivers, only participated in limited numbers, as they could not be removed from other duties. The organizations priority was demonstrated very clearly through management's decision, which was observed and commented upon by many.

Following the employment of the new CEO the company was reorganized. This reorganization took place two and a half years after the accidents and a conscious decision was made to break up the safety department and delegate safety responsibility to line managers. The organization decided that specialists no longer were needed and the outcome was a 30% reduction of safety personnel including some of the most senior staff. The changes made to the safety organization were a reflection of the power struggles that had taken place and the consequences were never risk assessed by independent means. For management, a belief in modern safety management theory drove these changes, despite being based on limited scientific support.

2.7 Academic Discussions

Building a resilient organization often requires external input in the form of investigations, surveys or suggestions and suitable solutions to action. Organizations rarely want academic discussions about terms and vague or ambivalent definitions that make concepts difficult, if not impossible to apply.

The distance between academia and high reliability organizations frequently appears immense and the high level of abstraction used in academia is of limited or no use to an organization. For example, the culture/climate debate may be of high relevance to academics distinguishing between deeper and shallower characteristics of an organization but for most organizations this distinction has little value. What matters is a solution or solutions, to the problems encountered. Whether this is called safety culture or safety climate is irrelevant.

Following the accidents several surveys (culture/climate) were conducted. Statistical analysis identified a high number of interdependent characteristics, which were perceived to constitute the organization's safety culture. Complex models were presented to illustrate the significant result of the analysis but no concrete suggestions to corrective actions were made. The analyses also failed to link behavioral/attitudinal factors to structural aspects.

On the whole the safety culture focus disappeared in a statistical significance fog, which did not support the organization in developing suitable corrective measures. In the end the organization developed its own Simple Model of Safety Culture (Skriver, 2004) on which its corrective action plan was based. The model, containing three interdependent factors (risk control, attitudes and behavior), was utilized for developing and managing corrective actions both at concrete and more abstract levels in the organization from a systemic perspective and has since been applied successfully in other industries such as the nuclear and oil. For the practitioner keeping it simple is often the key to success.

2.8 Failure to Learn

In high reliability organizations accident investigations have a specific goal – to identify corrective actions that reduce the probability of the accident being repeated. Unfortunately most accident investigation methods pay little attention to this fact. Writing an accident investigation report often becomes an end rather than a means to an end and little consideration is given to how it shall be used. Poor corrective actions result and in the end the accident investigation fails to prevent further accidents as the organization fails to learn.

Systematic accident investigation is essential if an organization is to learn from what happened. However it is important that the focus is on accident prevention not on presenting a detailed description of an accident sequence, root causes, non-conformity or variability. This may be relevant for Accident Investigation Boards but for most organizations, where time limits may impact on the investigation it is important to keep the goal in mind.

When the accidents described occurred, it was apparent that the railway operator did not have an accident investigation method. One of the first actions was to develop an investigation method suited specifically to the needs of the railway. Essentially a railway operator employs two occupations that are most likely to be involved in accidents at the sharp end: train drivers and conductors, thus the method focused on their roles and potential actions in a systemic perspective. The method derived its structure from the STEP method (Hendrick & Benner, 1986) combined with the checklists of the Human Performance Investigation Method (Paradies *et al*., 1993). Due to its tight coupling train accidents are often predictable (design based) and it was therefore possible to include an element on generic corrective actions in the method thereby simplifying the task of seeking solutions for the line managers responsible.

The method was developed to account for the majority of accidents so that investigations could be conducted and documented in less than 10 working days. This was to satisfy management requirements and to ensure that media pressure did not interfere with the investigation process. The method was applied with success during the following years proving its value and also supported the improvement of an existing incident registration database. However, all investigation results are not always welcome (see 2.4) and the method died a slow death due to increased regulator attention and internal accident reports becoming accessible for the public.

2.9 Short-Term vs. Long-Term Goals

One of the biggest problems encountered in connection with engineering a resilient organization relates to the need for long term planning. This stands in strong contrast to most organization's short-term financial goals and managers' requirement to show instant results. Behavioral intervention programs in connection with changes to procedures or rules take time to have an impact. If, e.g. procedure violation has been the norm, it is insufficient to change the procedure and expect behavioral changes to follow. Organizations must work systematically with the changes as well as with behavior and attitudes to succeed. However, this type of work takes time, especially if many procedures have to be changed. Over time safety behavior will improve as a result of well-developed behavioral intervention programs.

Unfortunately the pressure put upon most managers to show results counteracts such a systematic approach. To show management abilities, campaigns and other changes are introduced often in rapid succession without further thought to the impact on safety as a whole. The end result is often poor despite high costs. It is important for organizations to understand that improving safety takes time and effort. A five-year plan provides the time span within which safety can be expected to improve.

3 CONCLUSIONS

Resilience engineering has been proposed as an approach that provides a theoretical synergy of safety and risk management principles that reflect the practitioner's everyday goals and challenges. This paper has outlined a number of the challenges associated

with the building of a resilient organization using examples from a practitioner's perspective. It is critical that the field takes such factors into account when new theories and models are produced. For the practitioner there is a need to keep things simple and to focus on solutions. If resilience engineering is to be an approach supporting the practitioner's goals and challenges it must reflect the goals and challenges of the practitioner and be aware that the needs often are different from the academic environment.

The difference between a resilient and a less resilient organization lies in how safety is managed on the whole. A resilient organization will focus on proactive safety management. Less resilient organizations will practice reactive safety management where savings from preventing accidents are rarely balanced with the costs of accidents. Essentially building a resilient organization is a question of systematic application of safety management principles, which in reality are always mediated by cost, prioritization and culture. Despite the best intentions engineering a resilient organization it not easy. Self-interest by managers and workers will often prevail and building a resilient organization may ultimately stand on the organization's resilience with respect to change.

REFERENCES

Hendrick, K. & Benner, L. (1986). *Investigating accidents with Step.* New York, USA: Marcel Dekker.

Hollnagel, E., Woods, D.D. & Leveson, N. (Eds.) (2006). *Resilience engineering: Concepts and precepts.* Burlington, USA: Ashgate.

Paradies, M., Unger, L., Haas, P. & Terranova, M. (1993). *Development of the NRC's human performance investigation process (HPIP).* NUREG/CR-5455.

Rollenhagen, C. (2005). *Säkerhetskultur.* Stockholm, S: RX Media.

Skriver, J. (2004). A simple model of safety culture. In D. de Waard, K.A. Brookhuis and C. M. Weikert (Eds.) (2004), *Human Factors in Design*. Maastricht, NL: Shaker Publishing.

Statoil (2007). *Safe behavior*. http://www.statoil.com/safebehaviourprogramme