

Learning from failure: Research initiatives towards improving resilience of the Swedish railway system

Alexander Wilhelmsson¹
LUCRAM, Lund University, Sweden

Kurt Petersen²
LUCRAM, Lund University, Sweden

Abstract

This paper includes a brief description of some closely related ongoing research activities aiming at learning from failures in order to improve the resilience of the Swedish railway system. One of these activities includes the development of a method aiming at assessing the capability for restoring the service of the railway system after strains affecting its technical, and often highly interdependent, elements. In the event of incidents affecting these technical elements, adequate capability of those actors responsible for restoring the system is important. The method is based on a systems approach, and builds on evaluation of a number of incidents that have occurred on a section of the Swedish railway system in workshop sessions, involving persons with substantial knowledge and experience from recovery operations. By varying these incidents by so-called counterfactual scenarios the capability to return to normal operation after different types and magnitudes of strain can be demonstrated. Hence, the method is useful for evaluating the preparedness for future incidents affecting the railway system. Another study where a similar starting point is used, but where a wider spectrum of serious incidents and accidents form the basis for analysis, is a study focusing on the ability to learn from accidents that have stricken the railway system. Incidents and accidents, and in particular the subsequent accident investigation reports that are issued by the accident investigation boards in Sweden, Norway and Denmark, are studied in order to evaluate their potential for enhancing implementation of lessons learned. Although still in its initial stage, the preliminary results from the study indicate that problems for example stemming from the difficulties in knowledge transfer between different hierarchical levels in society influence the process of learning from accidents. The third study presented in this paper aims at describing the decision making process regarding investments in safety measures in railway tunnel projects. The study is based on interviews with persons involved in six Swedish railway tunnel projects comprising a total of 28 tunnels. The actors involved in the decision making process have considerably different points of departure, which at least in some of the studied projects has proven to be a reason for discussions and disagreements regarding the design of different safety measures. The results from this study show that substantial resources are invested in safety measures in all of the studied projects. However, the study also indicate that there is a need for increased coordination between the different authorities and organizational levels involved in the projects, and that the experience transfer between different projects can be improved. The three case studies are illustrated in an analytical framework that can be used as a basis for further studies, and it can be concluded that the different approaches are valuable in order to improve the resilience of the Swedish railway system.

Introduction

The railway system, and other complex socio-technical infrastructure systems, are characterised by a high degree of interdependencies, i.e. mutual dependencies between parts or subsystems. These dependencies make the systems more efficient under normal operation, but at the same time more

¹ Department of Fire Safety Engineering and Systems Safety
LTH, Box 118, SE-221 00 Lund, Sweden Tel: +46 (0)46 288 09 39
E-mail: alexander.wilhelmsson@brand.lth.se Fax: +46 (0)46 222 46 12

² Department of Fire Safety Engineering and Systems Safety
LTH, Box 118, SE-221 00 Lund, Sweden Tel: +46 (0)46 288 48 36
E-mail: kurt.petersen@brand.lth.se Fax: +46 (0)46 222 46 12

vulnerable to so-called cascading failures, i.e. failures spreading from one part of the system to another (Little, 2002; Rinaldi et al., 2001). According to Perrow (1984), failures are inevitable in systems that are characterised by a high degree of complexity and tight couplings between its parts, which is the meaning behind what he refers to as normal accidents. Similarly, Dekker (2006) argues that failures do not stem from the errors from human actions or technical malfunctions in an otherwise safe system, but rather failures should be seen as “structural by-products of a system’s normal functioning” (p. 17). Taking this somewhat pessimistic stance as a starting point, we need to realise that failures are an unavoidable side-effect of the normal operation of complex systems in a dynamic environment. However, this does not mean that actions to prevent future failures should not be taken. On the contrary, efforts should be made towards improving the railway system's ability to effectively “adjust its function *prior to* or *following* changes and disturbances so that it can continue its functioning after a disruption or a major mishap, and in the presence of continuous stresses”, which is an ability defining a resilient system according to Hollnagel (2008, p. xii). The aim of this paper is to present different approaches towards making use of the knowledge that can be gained from failures, in order to improve the resilience of the Swedish railway system. This is carried out by shedding light upon a number of aspects of the question that is forming the basis for this paper, namely; what can we learn from failures in the railway system?

Previous work on the topic has led to the categorisation of three levels of learning from failures suggested by Freitag and Hale (1997) reproduced here;

- 1st order learning: The first order learning corresponds to detection of a deviation and subsequent correction. This type of situation involves fixing parts that have failed and returning to normal operation using the original plans and goals.
- 2nd order learning: In the second order learning redesign of the system is necessary, and the plan for achieving the goal of the system needs to be changed.
- 3rd order learning: Finally, in the third order learning also changes of the goal of the system is required, e.g. the rejection of a whole technology.

This categorisation has been used as a starting point in a study by Hovden et al (in press), and will also be used as a basis for the case studies in this paper. Before presenting these research activities, it should be noted that, although the term failure will be used throughout this paper, this term may be somewhat misleading. As pointed out by Hollnagel (2006), events that we call failures most of the time actually stem from variations in our attempts to adjust in an unpredictable environment, and are therefore the flip side of success. In addition, when human actions are described as failures, it is often forgot that the actions taken by the human at the specific point in time, given the available information and other contextual factors, made perfect sense (which is the essence of the so-called local rationality principle, see Dekker (2006)). Therefore, the term failure in strict terms may be misleading and should here only be thought of as a term describing a surprise in relation to expected outcomes that lead to unwanted consequences.

Failures in the railway system give rise to consequences that can be described along two dimensions, both of which will be treated in this paper. First of all, failures from time to time result in incidents or accidents that have an impact on the safety of the people using or working in the system. It is therefore essential to be able to learn from these failures in order to prevent the same accident from happening again. Furthermore, as pointed out by several authors, it is not sufficient only to learn about how to prevent that same accident happening again, but about how to prevent as many other accidents as possible (Hale, 1997). Secondly, failures result in (small but rather frequent) disturbances to the functioning of the railway system, leading to delays and economic losses. This type of disturbances is the focus of the first of the three research activities that will be presented in this paper.

Case study 1 – The ability to recover from failures

Since our society is becoming more and more dependent upon the reliable function of a number of vital infrastructure systems, including the railway system, failures in these systems can result in large consequences for a nation's economy and social well-being (McDaniels et al, 2007). In order to maintain a reliable function of the railway system it is essential to develop strength to resist different types of failures combined with an ability to quickly recover from such failures. As described in the previous section, the ability of a system to return to normal function when affected by failure can be defined as its resilience (Hollnagel 2006). According to McDaniels et al (2008), two important aspects of a system's resilience are its robustness and rapidity, where the robustness refers to the ability to withstand a certain amount of strain, whereas the rapidity refers to the time required for the system to return to normal operation. See Figure 1.

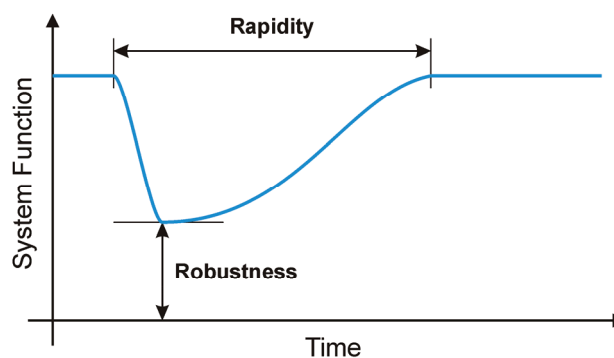


Figure 1: Schematic illustration of a system's ability to withstand strain (robustness) and time required to return to normal operation (rapidity). Figure based on McDaniels et al (2008)

From an analysis of the way previous failures in the railway system were handled we can learn important lessons about the capability for handling future ones. Knowledge of this capability is in many cases unknown or not explicitly expressed. Therefore, the aim of this study is to gain knowledge of the rapidity aspect (i.e. the time required for recovery), from previous failures affecting the technical, and often highly interdependent, subsystems constituting the railway system. Failures affecting the railway system are handled by a so-called response system, which refers to those actors that restore the system back to normal operation (see also Uhr (2007) for a more explicit definition). By studying the response system's capability for restoring the system valuable knowledge for preparedness planning can be gained, e.g. the maximum magnitude of strain the response system can handle.

For this purpose a method for assessing response system's capability has been developed, based on a systems approach. The method is based on table-top exercises in workshop sessions including persons with knowledge of the system function and experience from response operations. A first step of the method aims at creating a model of the system under study, which functions as a shared mental model for the participants of the workshop sessions. This model facilitates the identification of dependencies between the system elements and the identification of the response system.

The time required for restoring the railway system is assessed by using a number of incidents that have occurred in the railway system as a starting point, and by varying these incidents by so-called counterfactual scenarios (see Abrahamsson et al, 2008). A counterfactual scenario means variations of a real incident, i.e. if a real incident involved derailment of one car, a counterfactual scenario may be a derailment of two cars etc. Based on the assessment of recovery times, response curves are created. See Figure 2 for a schematic illustration of a response curve.

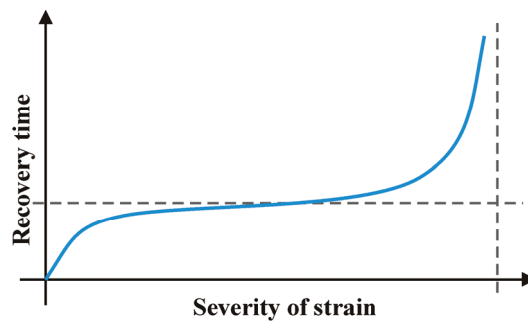


Figure 2: Schematic illustration of a response curve

Response curves are illustrations of the recovery time with respect to the magnitude of strain, and the shape of the response curves reveal a number of interesting characteristics that are valuable for preparedness planning in the face of future possible failures. For example, for some response operations an initial steep slope can be expected due to the need for specific resources etc. In addition, a region where sufficient capability for handling additional strains can be expected, which can be indicated by a rather constant or slightly increasing slope of the curve. Finally, at some point a dramatic change in slope of the curve may be found, which indicates where the limitation for handling additional strain is reached.

The method has been tested in an empirical study of a section of the Swedish railway system (between Stockholm and Gothenburg) with four persons from the Swedish Rail Administration participating in a workshop session. The study resulted in a model of the system that enabled the identification of those actors who restore the function of the railway system after strains, i.e. the response system. Assessment of the response system's capability for handling different incidents resulted in the creation of a response curve, see Figure 3.

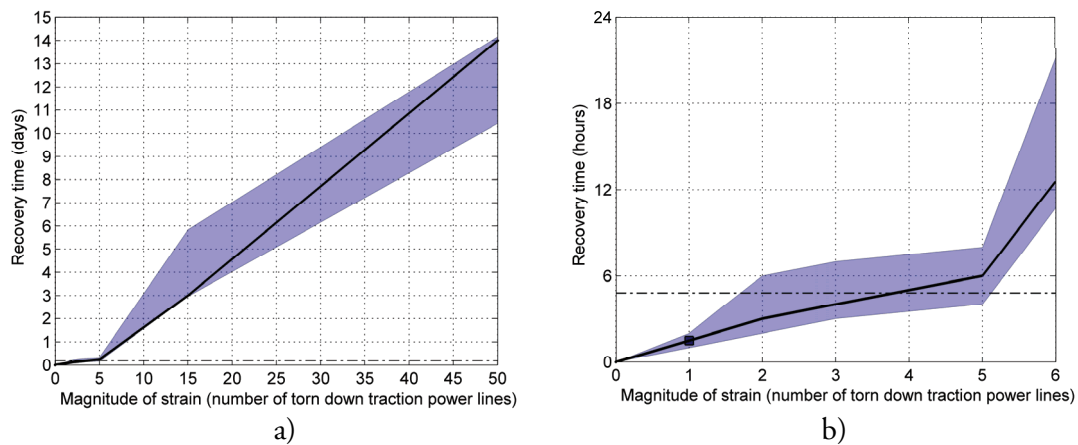


Figure 3: Response curve showing the recovery time with respect to increasing number of torn down traction power lines (Figure 3b is a close-up of Figure 3a)

The type of failures that the workshop session was based upon involved incidents where traction power lines were torn down. Two interesting regions can be identified in the response curve shown in Figure 3a; one between zero to five torn down traction power lines (see Figure 3b for a

close-up of this region of the curve) and one between five to fifty torn down traction power lines. The first region indicates where only the normal response teams for the given railway section is involved, and the second region where response teams from other railway sections are assisting in the recovery of the technical systems. Hence, the maximum capability of the local response system is reached at about five torn down traction power lines, but due to the ability to receive assistance from other response systems in the region no definite maximum capability in the form of a vertical slope of the response curve can be identified for this type of strains. However, the slope of the response curve is significantly steeper for strains above five traction power lines, which indicates that although capabilities for restoration above this point exists, the pace of recovery is slower due to the need for assistance from other response operators in the region.

In parallel ongoing work (see e.g. Johansson et al., 2008), the vulnerability of the interdependent technical subsystems constituting the railway system is studied. By systematically simulating failures in one or more technical systems simultaneously, the vulnerability of the railway system as a whole, due to dependencies between the subsystems, can be analysed. For this purpose, the use of recovery times identified in case study 1 is very important in achieving a realistic measure of the system's overall vulnerability. Consequently, the response curves can be used as a basis for decision-making regarding the adequate capability for restoring the technical system after different types and magnitudes of failures. In particular, by including counterfactual scenarios with magnitudes of strain that are above those of normal, well-known failures it is possible to identify the limits of the response system's capability.

So far, the method has only been tested for one type of scenario, which is failures that are affecting the traction power line. Although further empirical testing of the presented method is required, it can be concluded that the approach based on using previous incidents as a starting point results in valuable knowledge regarding the response system's capability. By systematically assessing the recovery time for a number of incidents and counterfactual scenarios knowledge from persons with experience from this type of recovery operations can be compiled and used for decision making and planning for future events.

Case study 2 – Obstacles for learning from failure

In addition to failures affecting the reliability of the railway system, which was emphasised in case study 1, failures sometimes result in severe damage both in terms of economic values and in terms of human lives. Although there is a strong desire in society to prevent these types of events as far as possible by a continuous emphasis on safety measures and prevention of accidents, all accidents cannot be prevented. Therefore, when accidents occur there is also a need for avoiding similar events taking place in the future, which is often expressed as a need for learning from accidents.

Similar to case study 1, failures that have occurred in the railway system are used as a starting point in this study, and as a basis for learning. Since incidents and accidents most often stem from a complex interplay between multiple factors, many of which are the result of normal variations in their everyday work context (Rasmussen, 1997), the elicitation of lessons and the subsequent implementation of these lessons is a difficult undertaking. The lessons learned often point at circumstances influencing the safety of a system that cannot be altered by single measures at one specific point of the system, since the causes of these events are theoretically infinite (Freitag & Hale, 1997). This is obviously making countermeasures difficult to achieve, and many obstacles to lessons learned can be identified.

Accident investigations constitute an important tool for learning from accidents, not only as a means for avoiding recurrence of similar events in the future but also for generally improving safety (Kjellén, 2000). In order to systematically and independently carry out accident investigations, permanent accident investigation boards are established in several countries, albeit with slightly different structures and responsibilities. Conclusions from accident investigations are conveyed via a number of different actors, all of which have different roles and perspectives. It is normally different

actors who are carrying out the accident investigation, deciding on suitable measures to be taken based on the recommendations in the investigation report, implementing these measures and following up and monitoring them. Hence, implementation of these lessons is usually not straightforward. Case study 2 constitutes the first step of a larger study aiming at improving the knowledge regarding what factors that are important for improving the implementation of lessons learned from accidents and incidents. Although still in its initial phase, the preliminary results from this study indicate that some of the factors that are influencing the ability to learn from accidents include:

- The structure of the accident investigation board, i.e. the number of investigators, their level and span of skills and competences
- The mandate of the investigation board, i.e. ability to influence the implementation of recommendations and follow-up activities
- The investigation method used by the investigators, i.e. what causes that are emphasized, the formulation of recommendations
- The processing of information between involved actors, i.e. the way that findings in the investigation is conveyed

In order to analyse the importance of these factors, an initial comparison between the formal structures of the accident investigation boards in Sweden, Norway and Denmark has been carried out. From this comparison it can be concluded that the Swedish board has the broadest responsibility in terms of what types of accidents that shall be investigated. Their responsibility encompasses all types of serious accidents, i.e. in addition to transport accidents (aviation, railway, maritime and road traffic accidents), the permanent Swedish investigation board also investigates other types of serious accidents including military accidents, mining accidents and accidents involving nuclear or chemical activities. In Norway the permanent investigation board investigates all transport accidents, i.e. aviation, railway, maritime and road traffic accidents, whereas in Denmark the permanent investigation board is restricted to only investigate aviation and railway accidents. In addition to the board investigating aviation and railway accidents, there is a separate permanent board in Denmark investigating road traffic accidents. However, this investigation board is different from the other boards since it is focusing on “themes” of accidents, i.e. investigation of a number of accidents within the same category at the time (e.g. bus accidents).

The initial studies indicate that this type of differences in structure and mandate are influencing the outcome of accident investigations, and consequently the potential for lessons to be learned. However, a closer look at accident investigation boards and their functioning is essential in order to study the impact of the different aspects described above. Therefore, future studies include more detailed analysis of a number of accident investigation reports issued by the accident investigation boards in Sweden, Norway and Denmark, which will be analysed regarding their influence on the potential for learning.

Case study 3 – Obstacles for implementation of lessons learned

Previously in this paper it was noted that the causes of an accident are theoretically infinite, which makes the explanation of the event and the subsequent lessons learned difficult. Lessons that are learned about safety (from previous failures, but also from safety analyses, technological development and more general experience) are in some cases eventually reflected in new or revised legislations. However, the co-existence of different views on safety and lessons learned from failures sometimes lead to difficulties in preventing future failures. One such situation is the decision making regarding safety measures in tunnel projects in Sweden, where different legislations are applicable, all of which reflect slightly different perspectives on safety.

The actors involved in the decision making process regarding safety investments in railway tunnels in Sweden have different governing legislations and points of departure. In 2003 this was acknowledged by the Swedish government, which led to the assignment of the four authorities involved in safety design of tunnels to provide a report on how to improve consensus regarding safety in tunnel projects. However, the main outcome from the assignment was that consensus is unattainable due to the incompatible legislations on the area. Therefore, given these incompatible views reflected in the different legislations, the aim of case study 3 is to investigate how decisions are made in practice. The study is based on interviews with 18 persons involved in six Swedish railway tunnel projects comprising a total of 28 tunnels. The interviews resulted in a description of the decision making process regarding railway tunnels in Sweden, which is schematically illustrated in Figure 4.

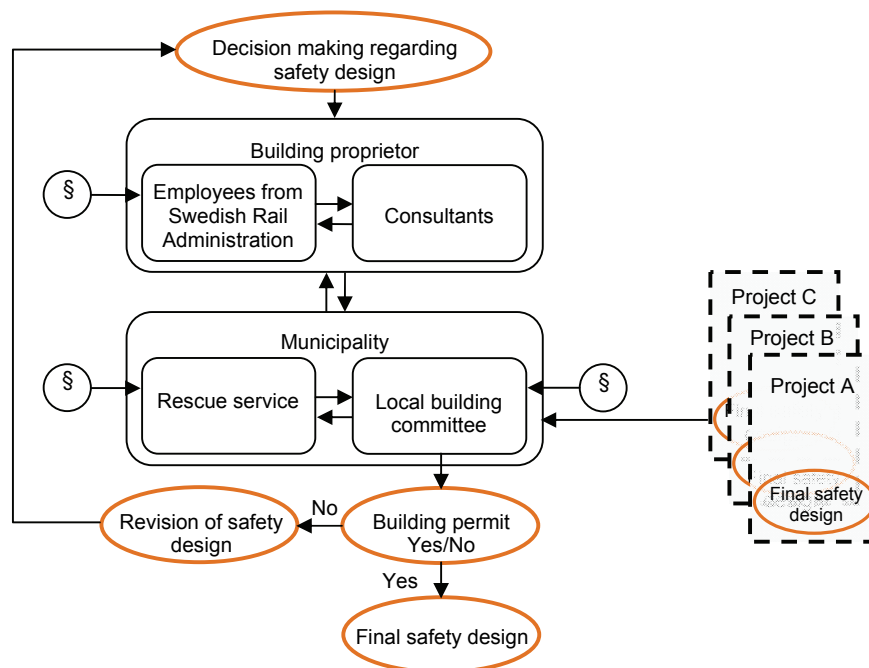


Figure 4: Schematic illustration of the decision making process regarding railway tunnel safety

As shown in Figure 4, the safety design of railway tunnels in Sweden is proposed by the Swedish Rail Administration (and their appointed consultants) in their role as the building proprietor. Safety measures are designed by the use of a risk-based approach according to a handbook issued by the Swedish Rail Administration. In addition, railway tunnels, like all other buildings in Sweden, require a building permit from the local building committee in the municipality where the tunnel will be built. This means that two different sets of guidelines and legislations, reflecting different views on risk and safety are applicable. However, since the local building committee generally does not have any experience from the building of railway tunnels, where the major issues of concern are safety and means of evacuation rather than architectural issues that is the case for other buildings, they seek advice from the local rescue service on these issues. In this way, the safety design proposed by the Swedish Rail Administration and their appointed consultants need to be approved by the local rescue service before the tunnel can be taken into operation. This means that decentralised decision making in questions that are considered to be of national interest put a lot of pressure on local decision makers. The interviews show that the municipality, and in particular the

rescue service, end up in having a central position in the decision making due to the need for a building permit.

In some of the studied projects the decision making process is characterised by disagreements and very long discussions between the involved actors, due to their different perspectives on risk and safety. In some of the tunnel projects the rescue service have required additional safety measures based on their governing legislations, i.e. a third set of legislations, which the building proprietor has not been willing to agree on. This study therefore shows that inability to solve a problem on a higher level in society (in this case among authorities) moves the problem to a lower level (in this case to the municipalities and local authorities). Clearly, this makes decision making difficult, since none of the involved actors want to deviate from their view of an appropriate safety design. It was also shown that the same problems regarding decision making were identified in several projects, and the interviews showed that transfer of experiences between projects was very limited, resulting in a feeling of “reinventing the wheel” among several of the interviewees.

Finally, the interviews showed that in several projects the rescue service and the building committee refer to other railway tunnel projects as a justification of their demands for additional safety measures, stating that the amount of safety measures in the tunnel in their municipality must not be less than in any other municipality, regardless the outcome of the risk-based approach and specific contextual factors behind the decisions in other tunnels. Therefore, this study shows that the decisions in one railway tunnel project affect the decisions in other projects, leading to what is here referred to as “precedents”, i.e. comparisons with other railway tunnel projects. From a comparison between the amount of safety measures between the studied tunnel projects no major differences can be identified, despite differences in length, traffic volume and other characteristics of the tunnels. This can be explained by a substantial influence from comparisons with other projects (“precedents”), levelling out differences in safety measures between the projects, which therefore is a very influential aspects of the decision making in the studied projects.

Results

The different approaches towards improving resilience of the railway system have resulted in the development of an analytical framework illustrated in Figure 5. The figure is based on Hovden et al (in press), with some modifications in order to capture the continuous nature of these processes.

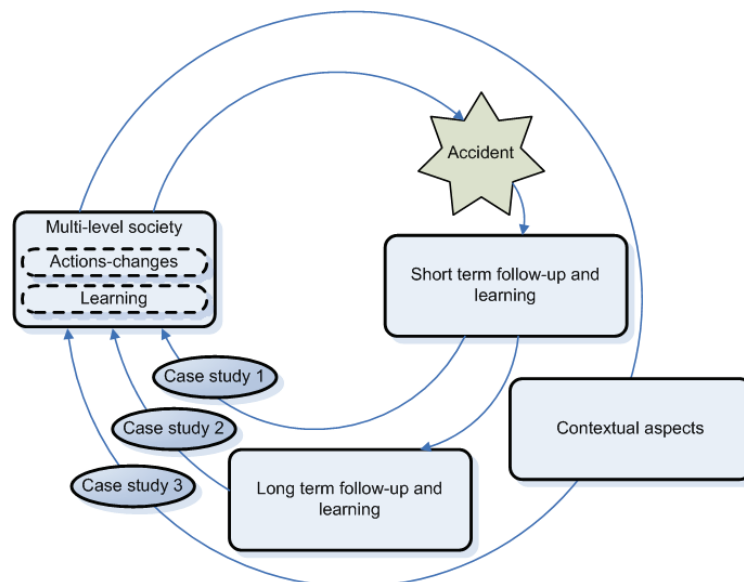


Figure 5: Analytical framework (based on Hovden et al (in press))

The framework is a schematic representation of the different processes identified in the three case studies described in this paper. Case study 1 was carried out as a table-top exercise, and therefore resulted in rather immediate internal changes, e.g. accumulated knowledge of the response system's capabilities, represented by the inner loop in Figure 5. Case study 2 was based on the study of accident investigations and how lessons learned from accidents are affected by numerous factors, e.g. the mandate and structure of the investigation boards. Although this study is still in its initial phase, it can be concluded that both short term follow-up and learning (e.g. immediate changes) and long term follow-up and learning can be identified. This latter process include accident investigations that are carried out in order to more thoroughly analyse the circumstances leading to the accident by external organisations, which is represented by the second loop in Figure 5. Finally, case study 3 illustrated a situation that was not directly related to failures in the railway system, but where different perspectives and the lack of experience transfer influenced the decision making in railway tunnel projects. This outer loop, which generally is slower than the other two, illustrates those contextual aspects that are gradually and continually taking place in society. For example, this loop includes technological and scientific progress, and changes in norms and values in society that influences the resilience of the system in a more continuous manner.

Discussion

Three parallel processes that together influence the ability to improve resilience of the railway system have been identified in this paper. These processes have been illustrated in Figure 5, based on Hovden et al (in press). The characteristics of these processes differ in several ways, e.g. in terms of the time scale between them, which is generally increasing for each outer loop in Figure 5. Moreover, the involvement of additional levels of society is increasing at the outer loops. The inner loop is mainly concerned with local changes and “quick fixes” close in time and location to the occurrence of a failure. This can be contrasted with the undertaking of investigations by national accident investigation boards, where substantial time is required, and where several levels of society are involved. Finally, the outer loop includes processes where norms and values are changed, technological and scientific developments are progressing, which is involving an even longer time scale and essentially all levels of society.

The identification of the different processes, and the representation of them in an analytical framework consists a first step towards gaining deeper understanding of multilevel learning from failures, and for improving the ability to handle future failures. However, the presented case studies and the framework only reveals *what* processes that can be identified, but not *how* these processes lead to learning and changes on different levels in society. Therefore, in order to gain deeper understanding of how learning from failure can be used to improve resilience of the railway system, additional studies in this area are required.

Conclusions

This paper summarises some ongoing research activities, all of which constitute an attempt towards exploring what can be learned from failures in the railway system. These research activities have lead to the development of an analytical framework that is useful for further studies. Although additional work is required, these different approaches provide valuable input in order to improve the resilience of the railway system.

References

- Abrahamsson, M., Hassel, H., & Tehler, H. (2008). A system-oriented framework for analysing and evaluating emergency response.
- Dekker, S. (2006). *The Field Guide to Understanding Human Error*. Aldershot: Ashgate Publishing Limited.
- Freitag, M., & Hale, A. (1997). Structure of Event Analysis. In A. Hale, B. Wilpert & M. Freitag (Eds.), *After the Event: From Accident to Organisational Learning* (pp. 11-22). Oxford: Pergamon.
- Hale, A. (1997). Introduction: The Goals of Event Analysis. In A. Hale, B. Wilpert & M. Freitag (Eds.), *After the Event: From Accident to Organisational Learning* (pp. 1-10). Oxford: Pergamon.
- Hollnagel, E. (2006). Resilience – The Challenge of the Unstable. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.), *Resilience Engineering: Concepts and precepts*. Aldershot: Ashgate Publishing Limited.
- Hollnagel, E. (2008). Preface: Resilience Engineering in a Nutshell. In E. Hollnagel, C. P. Nemeth & S. Dekker (Eds.), *Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure* (Vol. 1, pp. xi-xiv). Aldershot: Ashgate Publishing Limited.
- Hovden, J., Størseth, F., & Tinmannsvik, R. K. (in press). Multilevel learning from accidents – case studies in transport. Paper submitted to *Safety Science*.
- Johansson, J., & Jönsson, H. (2008). A model for vulnerability Analysis of Interdependent Infrastructure Networks. Paper presented at *The Joint Conference for European Safety and Reliability Association and Society for Risk Analysis Europe (ESREL2008 and 17thSRA-Europe)*.
- Kjellén, U. (2000). *Prevention of Accidents Through Experience Feedback*. New York: Taylor & Francis.
- Little, R. G. (2002). Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences 2003*, 58-66.
- McDaniels, T., Chang, S., Cole, D., Mikawoz, J., & Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change*, 18(2), 310-318.
- McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., & Reed, D. (2007). Empirical Framework for Characterizing Infrastructure Failure Interdependencies. *Journal of Infrastructure Systems*, 13(3), 175-184.
- Perrow, C. (1984). *Normal accidents: Living with High-Risk Technologies*. New Jersey: Princeton University Press.
- Rasmussen, J. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, 27(2/3), 183-213.

Rasmussen, J., & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Karlstad: Swedish Rescue Services Agency.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 21(6), 11-25.

Uhr, C. (2007). *Behind the Charts - Exploring Conditions for High Level Emergency Response Management in a Complex Environment*. Lund University, Lund.