# Risk Assessment of Critical Communication Infrastructure in Railways in Norway.

Stig O. Johnsen[1] and Mona Veen[2]
[1] Norwegian University of Science and Technology, Trondheim, Norway
Stig.O.Johnsen@gmail.com
[2] JBV, OPM, Trondheim, Norway

**Abstract.** This paper discusses the significant findings of a risk assessment of infrastructure used in emergency communication by railways in Norway. The initial risk assessment was performed in 2008 and we have reviewed the results in 2010, documenting mitigating actions and their effect. The development of safety and security culture has also been evaluated. The risk assessment was based on a socio-technical approach, which considers technical, organizational and human factors. Action research was used as a method to improve the risk assessment. Resilience is included, to improve safety, security and quality of service. It is suggested that collaboration supported by the action research approach, has aided in prioritizing key mitigating actions in the face of opposition. One of the identified unwanted incidents occurred in 2010, and this gave credibility to the risk assessment. The risk assessment seems to have sustained the safety and security culture and improved knowledge of emergency response. The resilience of the total system seems to have been improved. It is suggested that exploration of resilience and action research improves the quality and effect of the risk assessment.

## 1 BACKGROUND AND INTRODUCTION

This paper is discussing the significant findings of a risk assessment of infrastructure used in emergency communication in the Norwegian railway, the Global System for Mobile Communications in Railways (GSM-R). It is an international wireless communications standard for railway communication, see GSM(2010). We performed a risk assessment of the GSM-R system in 2008. Several technical challenges were the basis for our work. There was one central GSM-R switch without backup; this could be a single point of failure. Two central communication components managing most of the traffic was placed in the same room with a common power supply vulnerable of common cause failures. The GSM-R system was implemented in Norway in 2007 after the train accident at Åsta in 2000, where 19 people were killed, see NOU(2000). Prior to the Åsta accident, the train control identified two meeting trains on the same single track, but they did not manage to contact the train drivers in time.

The organization of rail traffic in Norway is divided between several different actors. In 2010 there are 13 different train operators. The Norwegian Railway Authority, SJT, is responsible for ensuring that rail operators meet the conditions and requirements set out in the railway legislation. The infrastructure operator, JBV, manages infrastructure - tracks and signaling equipment. We have based our risk assessment on the MTO concept (Man-Technology-Organization), for a broad socio-technical approach to safety that builds on different knowledge areas such as technology, psychology, organization knowledge, culture, human factors and safety, as described in Rollenhagen(2007). The risk assessment is based on a Preliminary Hazard Analysis (PHA), as described in Ericson(2005). Based on the vision to establish a "*secure and resilient transportation network*" from TSA(2007), we have also focused on resilience. When the GSM-R system fails, the failure should lead to a controlled degradation of the operation of train traffic, i.e. to resilience in operations. Resilience is defined as "*the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress*", from Hollnagel (2006). Safety is defined as: "*freedom from unacceptable risks*", and risk has been defined as "*Combination of the probability of occurrences of harm and the severity of that harm"*, both from ISO (1999). The focus of our risk assessment and discussion of security has been in the context of safety of train operations, to avoid major train accidents, incidents or disruption of traffic.

Safety culture has increasingly been explored in railways, as documented in the "state-of-the-art" review in Wilson(2006). Safety culture is an area with many different perspectives and opinions, as discussed in Yule(2003); one issue has been the possible relationship between safety surveys and safety outcomes. In Itoh(2004) there is documented a correlation between attitude factors such as the operators morale and motivation and the actual incident/accident rate of train operations. Based on the correlation of the past, it is suggested to assess attitudes in addition to incident/accident data to identify possible high risk or low risk units. Thus culture has been explored as an emergent property of the system, using a culture survey as a possible indicator of safety performance in the future. From Yule(2003); the most used definition is "*The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behavior that determine commitment to, and the style and proficiency of, an organization's safety management*". This definition is used by the International Union of Railways (UIC), see Johnsen(2005). Security has been included in the above definition of culture, i.e. looking at "safety and security culture". The key issues prior to starting the project were:

1. What are the major risks in a MTO perspective?
2. What are the main MTO mitigating actions, also improving resilience?
3. How can we assess and influence culture, to improve safety and resilience?
4. Can resilience be explored to mitigate security issues or challenges?

## 2 APPROACH

The activities in the project included standard steps from a preliminary hazard analysis (PHA). Different competencies and knowledge had to be included in the risk assessment in order to ensure a complete risk picture and to avoid simplification, an important issue in complex settings as discussed by Weick(2001). Key issues were prioritized in collaboration between different stakeholders and management in appropriate meeting arenas. These open collaborative meetings between stakeholders were called "search conferences". Assessment of safety and security culture was included in order to identify development of knowledge and awareness that could impact safety. The main activities were:

T1. Organize the project basded on collaboration across competencies.
T2. Identify major risks and major hazards in a MTO perspective.
T3. Prioritize risks in collaboration with stakeholders through search conferences.
T4. Prioritize mitigating actions based on MTO and improve resilience.
T5. Assess development of safety and security culture to identify areas of concern.

The risks and hazards were based on prior documented internal incidents in operations and based on selected issues from literature. Interviews and discussions were performed in eight expert groups from the operating organization. The major risks and mitigating actions were discussed based on a MTO perspective, exploring organizational and human factors issues during the intervews. The key findings were analyzed, documented and submitted to the interviewed persons, in order to verify and validate the results. The major risks and mitigating actions were summarized and presented to a search conference. The search conference were arranged to discuss major risks as presented through a risk matrix. The risk matrix and mitigating actions were displayed as large posters on the walls, in order to be able to change and prioritize the different elements in an open collaborative manner. Several suggested risks were changed based on the peer reviews, disagreements and discussions. The 40 employees were each given five "post-it notes" to prioritize mitigating actions. The participants increased their understanding by looking at how different personnel prioritized different mitigating actions. The safety and security culture was assessed through a questionnaire distributed in 2009, and in 2010. The questionnaire consisted of 30 questions, distributed to 37 employees. In 2009, 76% answered the questionnaire and in 2010, 78% answered the questionnaire.

### 2.1 Use of Action Research in the Project

Action research has been used to improve safety and security in complex organizations; this has been more fully documented in Johnsen(2009). Four important activities from action research has been explored and incorporated in the work plan are:

- Involving the different communities of practice who is working to ensure safety.
- Using workgroup meetings (search conferences) to increase workforce understanding.
- Using the workgroup meeting to prioritize risks and mitigating actions by bottom-up processes in addition to "top-down" decisions; and to increase ownership.

- Using the workgroup meeting to support a "proactive and informed" culture exploring the risk matrix as a communication tool across different organizational silos to improve risk understanding and risk communication.

### 2.2 Exploring Resilience in the Preliminary Hazard Analysis (PHA)

Resilience is suggested as an appropriate strategy to be used when we are faced with uncertainty induced risk problems, as described by Renn(2005). It is also suggested as an appropriate instrument to cope with surprises, and seems well suited to security issues. A detailed specification of resilience from Johnsen(2009) was used, describing resilience as the ability to be *redundant, to be able to perform controlled degradation and able to "rebound or recover", ability to be flexible, ability to manage margins and ability to sustain common mental models.* These resilient factors are listed in the following:

- *Redundancy* is defined as having several alternate and independent ways of performing a function. Redundancy was important in this project since there was only one central GSM-R switch and risks of common cause failures in the network. In our case redundancy was explored as a combination of technical and organizational actions when one key technical component fails.
- The ability to perform *controlled degradation and ability to "rebound or recover",* when system functions or barriers are failing. This is an important issue related to the GSM-R communication, the system is distributed and complex – key elements may fail and the organization and systems must be able to handle this without serious incidents and acceptable quality of service of train traffic.
- *Flexibility* in systems and organizations or diversity – having different ways of performing a function within a specific system. When there is a failure the total MTO system should be flexible. Examples could be the ability to handle loss of key components in the communication network, enabling messages to be distributed through different systems or through emergency procedures.
- *Managing margins* – ensure that safety boundaries are not crossed. Risk perceptions may indicate status at boundaries, and measurements of "safety and security culture" contain perceptions of risks, and are included in our approach.
- Establishment of some sort of *common mental models* – ensuring that communication and collaboration across organizations and systems are supported and based on common understanding of major risks, as documented in the risk matrix. In our context, the key issues are safety and security; especially common ability to know what to expect (anticipation), knowing what to look for (attention), knowing what to do (rational response) and having the ability to learn/reflect.

The railway industries, as other industries, have been fragmented between different operators and suppliers, with different risk perceptions and different learning arenas. Close collaboration may improve common risk perceptions as discussed in DeBruijne(2007) through "networked reliability" of skilled operators collaborating and learning. The Railway industry is focused on rules and regulation. By focusing on more than rules and regulation, there is an opportunity to move to a proactive and learning culture, as described in Westrum(1993). The assumption in this paper is that culture can be measured, managed, and manipulated as described in the functionalistic tradition Schein(1992). One method and questionnaire to explore and discuss culture is called CheckIT, and are described in Johnsen(2007).

## 3. RESULTS

In this section a description are given of unwanted incidents (U..) and mitigating actions (A..), final results and activities, results of survey of culture and subsequent unwanted incidents within the scope of the risk assessment. The key unwanted incidents are:

- (U1) Stop of central GSM-R communication, there is no backup of the GSM-R system; the system is a single point of failure. At present, organizational routines have not been established to enable the train traffic to function satisfactory with loss of GSM-R communication system. (Mitigation: A1 and A1.2, see next section).
- (U2) Stop of regional GSM-R communication, common failures in the infrastructure may lead to cascading errors and halt of communication. A fire at the Oslo S central station, removed power to much of the GSM-R communication equipment, halting all train traffic in Oslo during 20 hours, Utne(2009). (Mitigation: A2).
- (U6) Unanticipated human errors due to poor training of short-time contract employees and too few employees with experience. (Mitigation: A6).
- (U25) Poor resilience and MTO ability to handle crisis and recover, due to poor scenario training and poor crisis management. (Mitigation: A25).

All unwanted incidents were given a probability and consequence based on expert judgments and placed in a risk matrix. The risk matrix was used to prioritize unwanted incidents and mitigatig actions.The prioritized mitigating actions were:

- A1 – Duplicate the core GSM-R system via an independent backup system, in order to be able to sustain communication in the railway system, even if there are failures in the central GSM-R complex. Cost was estimated to be USD 30 Mill, (ref U1).
- A1.2 – Improve organizational resilience when GSM-R fails, to ensure some sort of "degraded" but safe train traffic and operation with reduced functionality. It is suggested to establish competencies, collaboration and manual procedures that can be used to manage the traffic when the systems malfunctions. (Ref U1).
- A2 – Improve technical resilience by redundancy i.e. duplicating and separating key distributed GSM-R components in different locations, as an example with different power supplies to avoid common cause failures. (Ref U2).
- A6 – Increase manning in safety critical areas and prioritize training, in order to increase knowledge, experience, flexibility and redundancy. This demands management actions to increase budgets and allocate increased manning. (Ref U6).
- A25 – Increase scenario training of a set of defined crises, such as loss of communication/ loss of power, loss of critical communication equipment such as BSC, in order to build resilience and be able to handle unwanted incidents with greater competence across different organizational silos. (Ref U25).

A suggestion from the safety staff was to not use the risk matrix. If a risk was positioned in the risk matrix in a "red" area then the action had to be implemented. The argument was that prioritizing of "must be done actions", should be the responsibility of line management. However, use of the risk matrix was accepted and the following mitigating activities have been prioritized and implemented:

- A1 – Duplicating the core GSM-R functionality at a cost of USD 30 Mill
- A2 – Duplicating local distributed components, to improve resilience.
- A6 – Increasing local manning of safety critical areas, to improve resilience.
- A25 – Increasing scenario training of defined crises, to improve resilience.

The culture survey was performed in 2009 and 2010. The assessment is subjective from the participants and thus relative. The "culture rating" in 2009 from the questionnaire was a subjective assessment of 3.7 and in 2010 it was 3.8 i.e. an assessment between a rule based culture (score 3) and a learning organization (score 5). The issue getting the highest evaluation was "*Knowledge of what may go wrong*", this could be interpreted as a positive ability to know the risks of operations in JBV, indicating that the stakeholders in JBV is moving towards an learning organization. Significant changes in the survey from 2009 is interesting. The "*planning and perception of ability to handle crisis*" improved from a score of 3.5 in 2009 to a score of 4.1 in 2010; this is an improvement of 0.6 – and documents that work with scenario analysis/crisis management has impacted the perceptions of the workforce in addition to establish routines to be used in crisis.

### 3.5 Actual Unwanted Incidents in the Period 2008 to 2010

The risk assessment focused on risks related to loss of communication and suggest that the resilience of the GSM-R system had to be improved. At 2010-03-29 the GSM-R system did fail and all the trains in Norway had to stop during three hours, due to the failure, ref NRK(2010). Luckily the top management could say to the critical media that they had decided to invest USD 30 Mill in a backup GSM-R central, to be used when the central GSM-R system failed, ref NRK(2010b).

## 4. CONCLUSION

The risk assessment, based on a broad socio-technical approach to safety, seems to have identified relevant major risks related to technology, organization and human factors, based on the incidents in 2010. The exploration of action research and collaboration through search conferences seems to have supported common understanding and common models of risks and mitigating actions across different stakeholders and competencies. The resilience of the system has been improved, due to improved scenario training, improved organizational redundancy (trough increased manning) and improvement in technical redundancy. Development of knowledge and risk awareness seems to have been improved through the risk assessment as documented by the CheckIT questionnaire. Resilience seems to be a useful strategy to mitigate security issues since it improves the capability to cope with surprises, it improves diversity and allows for flexible responses – all important issues related to security issues, thus resilience seems to be an important perspective when discussing security. The paper suggests extending the risk assessment process through exploration of resilience and action research to improve safety in complex settings.

## REFERENCES

De Bruijne, M., Van Eeten, M. (2007) “Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment”, *Journal of Contingencies and Crisis Management, Volume 15, Issue 1, pages 18–29.*

Ericson II C. A., (2005). "Hazard Analysis Techniques for System Safety", Wiley

GSM-R specification *from http://www.uic.org/spip.php?rubrique851* at 2010-01-11.

Hollnagel, E. Woods D., Leveson N. (2006) “Resilience Engineering” Ashgate

ISO Guide 51 (1999) "Safety Aspects–Guidelines for their Inclusion in Standards." ISO.

Itoh, Andersen, Seki (2004), “Track maintenance train operators’ attitudes to job, organisation and management and their correlation with accident/incident rate”, *Cognition, Technology and Work, Vol. 6(2), pp. 63-78*

Johnsen S.O., Herrera I.A., Vatn J, Rosness R. (2005) “Cross border railway operations: building safety at cultural interfaces”. In: *Wilson JR et al (eds) “Rail human factors: supporting the integrated railway”. Ashgate, pp 393–409*

Johnsen, S.O., Hansen, C.W., Line, M.B., Nordby, Y., Rich, E. and Qian, Y.: (2007) "CheckIT – A program to measure and improve information security and safety culture," *International Journal of Performability Engineering vol. 3(1 Part II), pp. 174-186.*

Johnsen, S.O., Skramstad T., Hagen J. (2009) “Enhancing the Safety, Security and Resilience of ICT and SCADA systems Using Action Research”, *Critical Infrastructure Protection III, eds Palmer C., Shenoi, S., (Berlin, Springer), pp 113-123,*

NOU 2000: 30 Åsta-ulykken, 4. januar 2000 Hovedrapport.

NRK (2010) “Train chaos” *nrk.no/nyheter/norge/1.7060731, retrieved 2010-03-29.*

NRK (2010b) “Train problems” *nrk.no/nyheter/norge/1.7063278, retrieved 2010-03-31.*

Renn, O. (2005) “Risk Governance, Towards an Integrative Approach” IRGC.

Rollenhagen, C., Evenéus, P., (2007) “Development of a systemic MTO perspective on dam safety management.” *The 4th EADAC Symposium, China, October 13–18, 2007.*

Schein E.H. (1992) “Organisational Culture and Leadership”, Jossey-Bass.

TSA (2007);Transportation Security Administration, “Transportation Systems: Critical Infrastructure and Key Resources”, US Department of Homeland Security.

Utne, I.B., Hokstad, P., Vatn, J.: “A structured approach to modeling interdependencies in risk analysis of critical infrastructures”, ESREL 2009.

Weick, K. & Sutcliffe K. (2001). “Managing the Unexpected: Assuring High Performance in an Age of Complexity”. San Francisco: Jossey-Bass.

Westrum R.J: (1993). “Cultures with Requisite Imagination”, *in: Wise, Stager and Hopkin (Eds.) Verification and Validation of Complex Systems:, Springer.*

Wilson J., Norris B., (2006) “Human factors in support of a successful railway: a review”, *Cognition, Technology and Work 8 (1) 4–14.*

Yule, S. (2003) “Safety culture and safety climate: a review of the literature” *Industrial Psychology Research centre 1 – 26.*