Knowledge management in the area of information security

Rui Fernando dos Santos Pereira Antunes Fernandes

Instituto Superior Técnico, Universidade de Lisboa, Portugal

ruiffernandes@tecnico.ulisboa.pt

Abstract.

The management of railway engineering, operational and organisational changes is composed of a set of activities including the recognition of alterations, the assessment of their impact, the gathering of dangers or hazards and the update of the organisation's risk profile, which poses security impacts. This is a recent process in many organisations and its effectiveness depends on careful application.

The goal of this study is to help understand the norms, context, limits, results and eventual improvements to the change management process in railroad organizations, studying its main elements and how they contribute to implementation.

The referential used on this study is Common Safety Method (CSM) in the context of the organisation's safety management system. This analysis was done through a case study of a Portuguese railroad operator collecting and analysing the perspective of relevant experts in different areas of the organisation.

We concluded that the improvements in the use of this method include technical aspects of application, the ability of raising awareness and involving key personnel with relevant and multidisciplinary skills, and the coordination and transfer of risk management information between companies. The improvements also include aspects of reorganization and rehabilitation of the sector essential to answer the high level of specialization demanded by the regulation and need for technical and organisational innovation.

Keywords – Management of Alterations, Risk Management, Risk Assessment, Safety Management, Change Management, Safety Management Systems, Common Safety Method.

1. Introduction

The concepts of risk management have been included in certification regulatory standards (e.g. in the new version of the NP ISO 9001:2015[1]) and in community and national legislation (e.g. Data Protection Regulations according to the EU Regulation N° 2016/678). Railway regulation has been also including requirements and concepts of risk management associated with the performance such as the Safety Management System (SMS), according to EU Regulation No 1148/2009. The management of changes with impact on security, consists of a set of activities including the recognition of these changes, the analysis of your impact, by survey of dangers and risk profile of the organization. It is, however, a recent process in large organizations with low effectiveness. The studies tend to focus on stable environments considered prevalent in the life of organizations. This situation does not match current reality of the railway industry. Changes generate operational impacts not negligible, altering the risk profile of the Organization in a relatively short space of time, consuming resources and management knowledge, hindering the preparation of effective responses to risk.

Research philosophy and perspective - The study follows a realistic epistemological approach under critical theory. It is required the observation of the phenomenon and the artefact, inserted in a specific context and organization. "...critical realism recognizes the importance of doing a study at multiple levels that have the ability to change the understanding that the investigator has over the object the study." Saunders, et al., (2009). The case study is supported by research based mainly on fieldwork, studying a program or institution in your reality, using interviews, observations, questionnaires, documents. Yin (2014).

2. Literature Review

2.1 Managing change

Change management is a critical task in any organization, the implementation of changes in the organization requires high levels of lead. Communication is one of the main aspects of managing change, Kotter (2012). The incorporation into the strategy of change, of vision and opinions of key stakeholders in the Organization, the higher levels, allows you to create a favourable climate to change, as facilitator of the implementation and change management. The sharing of the strategy and the decision allows to attract many ideas, ensuring progress in the right direction, Blokdijk (2008).

The authors Stink & Herold (2004); made a summary on development of initial steps in change management initiatives, in areas such as banking, engineering, health care, manufacturing, technological services and basic services; analysing in three studies, three basic aspects: the way in which organizational change affects the adjustment of workers with its tasks and organization; the tensions generated in workers; the impact of the change in the commitment of workers vis-à-vis the organization.

[1] ISO 9001: 2015 directs the organization's efforts towards sustainable development as a tool to improve overall performance. It encourages the focus of internal and external stakeholders in adopting a risk-based approach to quality management and emphasizes the importance of adopting a Quality Management System (QMS) as the organization's strategic decision.

Even less significant changes should be managed. Age is inversely proportional to acceptance requiring greater preparation and involvement of older workers. Personal tension increases with the impact of change in individual work of each worker, and also if the change has a high impact on the service/work unit and is not managed in an equitable manner. The largest commitment arises when the change is seen as advantageous for service, requires significant effort, but has little impact on daily tasks simultaneously.

Kyriakidis (2013) and Smith et al., (2013); consider that the rail system is a highly complex network that involves the continuous interaction between workers and technology, procedures and regulations to ensure the safety and efficiency of operations. From the architectural point of view, the complexity of these interactions presents a risk of failure associated and the consequences arise in the form of incidents and accidents.

2.2 The risk-based thinking

The risk-based thinking, constitutes one of the basic requirements of ISO 9001:2015 and aims to replace and improve the concept of prevention, which until here as a separate component of the QMS-quality management system. The risk-based thinking assumes that all aspects of the quality management system inherent in systems, processes and functions are analysed from the point of view of risk, especially with your identification, study and control from the design phase, in a proactive manner, making the prevention planning, operation, analysis and evaluation of the activities. It is considered that this approach helps to improve the governance of the Organization, to establish a proactive culture of improvement, statutory and regulatory compliance, consistency in quality of products and services, and to improve the confidence and satisfaction of customers.

2.3 Risk management

In a broad sense, risk is exposure to adversity. "a real-world condition where there is an exposure to adversity", Vaughan (1997). The risk situations may lead to different results of the intended towards positive or negative and are always characterized by uncertainty of these results. Risk is also defined as the influence of uncertainty about getting/reach of objectives/targets (ISO 31000:2009)[2], being inherent to the activities of man and of all companies. This effect can be a positive or negative deviation. The uncertainty stems from a deficiency of information, related to the understanding or knowledge of an event and its probability and consequence of occurrence. Risk is a combination of the probability and the consequences of the occurrence of a hazardous event (OHSAS 18001, 2007)[3]. For example, the risk in occupational safety and health (OSH) is a danger, in terms of likelihood and severity of an injury or disease that occurs as a result of the danger.

Risk management refers to the set of coordinates activities to direct and control an organization with regard to risk. It is considered the owner of the risk the entity with the responsibility and authority to manage the risk. It is considered the source of the risk an element that, by itself, or in combination with others, have intrinsic potential to give rise to a situation of risk. Among other events, with potential impact on the results of the Organization are: Internal interference factors: The Infrastructure and basic equipment, people, processes, technology, information systems, Government model of the Organization. External interference factors: The Natural, political, Economic, social, technological, Public Infrastructure, weather.

[2] Risk management: Principles and guidelines.

[3] Standard for the Occupational Health and Safety Assessment Series (OHSAS); OHSAS 18001 has been developed to be compatible with ISO 9001: 2015 (Quality) and ISO 14001: 2015 (Environment) management standards, facilitating the integration of occupational health and safety management systems, environmental management systems and quality management systems, should the organizations wish to do so.

Only the risks identified can be assessed and managed, the quality of the risk identification activities is crucial to the management process. Craighead, et al., (2007) say the severity of the problems is influenced by the time the company takes to understand the risks or predict their impact. Moosa (2007) addressed the subject of operational risk management. According to the Basel Committee on Banking Supervision (2001), operational risk is the risk of loss resulting from the inadequacy or failure of internal processes, people, systems or external events.

The risk management requirements from different norms (e.g. ISO 31000:2009 ISO 9001:2015; ISO 14001:2105, OHSAS18001; ISO 27001: ISO 22000, ISO 50001), are currently aligned in terms of concepts and structure. Those regulatory requirements include: the analysis of the internal and external context; the adoption of a risk-based management approach; the identification of the skills needed for staff perform your work and knowledge necessary to achieve compliance of products and services; the management of operational changes.

2.4 Safety management in railway enterprises

Jeffcott, et al., (2006) claims that the organizational safety culture, reflects the attitudes and behaviors that individuals share to consider and react to hazards and risks. They argue that trust is an underdeveloped concept and important in relation to theories of culture of safety and high reliability organizations. Their analysis suggests that the privatization of 1993 and the subsequent organizational restructuring of the rail sector in the United Kingdom, had important repercussions both in safety culture as in the trusts. The conclusions focus on three key elements in theories about "secure organizations" (flexibility, commitment and learning), discussing how the organization can be influenced by issues of trust.

A risk assessment system, can evaluate effectively and efficiently, the qualitative and quantitative risk data and the information associated with a rail system, which will provide rail risk analysts, managers and engineers a method and a tool for improving the safety management of railway systems and so set safety standards.

An, et al., (2011); conclude that risk management is becoming increasingly important for railway undertakings, in order to safeguard their passengers and employees, while improving security and reducing maintenance costs. However, in many circumstances, the application of probabilistic risk analysis tools may not give satisfactory results, because the data are incomplete or because there is a high level of uncertainty involved in risk data.

A risk assessment system, can evaluate effectively and efficiently, the qualitative and quantitative risk data and the information associated with a rail system, which will provide rail risk analysts, managers and engineers a method and a tool for improving the safety management of railway systems and so set safety standards. Hirsch (2006) summed up the experience of the meters in London and Paris in the monitoring of precursors of accidents over several years, as part of the Quantified Risk Analysis (QRA), model to reduce risk and improve safety. The precursors examined identified the areas or significant events most likely to cause casualties, allowing direct the investments for prevention of events and mitigate its consequences.

Kyriakidis, et al., (2012) claim that the assessment of the maturity of a security management system cannot be based only on the data analysis of precursors, main events, injuries and deaths that occur as a result of the provision of services, over a period of several years, (complete and reliable data available). The security maturity model which propose, based on a questionnaire of evaluation with different criteria, for each railway undertaking, with a numeric scale. The criteria include in particular the following aspects: Publication of safety reports; Periodicity of monitoring; The prioritization of security incidents; Efforts to mitigate the risks

and avoid incidents; Description of the security procedures, including the registration of dangers; Monitoring of residual risks.

Fleming (2001) says that; effective security management implies, among other things: The involvement of the management and supervision of operations; The interest and commitment to safety; Effective communication and consultation/participation of workers in the management of safety; the clear responsibility of security management; The integration of safety in different management functions; Systematic risk management processes; Regular audits, the registration systems of occurrences of OHS (occupational health and safety) and continuous improvement processes; Standardization of operational procedures; The training on safety; The hiring practices relevant to safety; The work environment; The use of technology compatible with safety; the organisation of work (e.g. the workload and pressure), consistent with the safety.

2.5 Preventing occurrences of accidents in railway transport

According to Kim, et al., (2010) human error, is considered as the most significant source of accidents or safety incidents in critical system. The study analysed statistics on rail accidents in South Korea between 1998 and 2007, concluding that 68% of train accidents involving collisions, derailments and fires were attributed to human error and 92% of level crossing accidents were caused by human error.

The author Svenson (1991) developed a model that describes the interaction between technical and organizational systems, which allow the occurrence of an accident, allowing the analysis by experts of accidents and the respective contribution of these factors. The model enables also the predictive analytics of security conditions, indicating leads to the introduction of improvements and raising questions about other elements, such as the cost, the feasibility and effectiveness of different means of increasing security. Gander, et al., (2011) studied the development of systems of management of fatigue in the railway sector, identifying the responsibility of management at three levels: Regulatory responsibility, associated with the regulatory and supervisory regime for each State and the international level; Responsibility of the industry/organisation, linked to the company's internal practices and regulatory; Individual responsibility, associated with the behaviour of individuals.

Newnam & Watson (2011) think the although the accident made records in databases can provide invaluable information about accident statistics, this information is usually insufficient to give a holistic view of the case of an accident. According to Davey, et al., (2008) the data collection methods are reactive instead of proactive.

Although the standards of design and technical solutions have improved, the major accidents continue to occur due to failures in the companies' Safety Management Systems (SMS). The main objectives of a good SMS shall ensure that: Risks are identified and assessed, and placed the appropriate controls in place to manage these risks; The responsibility and tasks that ensure checks are effective always. An SMS includes codes of practice for the safety management of the processes, principles, readiness in response to incidents/accidents and general risk management programs, including in environmental terms. There are three key features of the SMS (ICAO, 2006): Systematic safety management activities are carried out according to a predetermined plan, applied consistently throughout the Organization; proactive – emphasizing the prevention, through the identification of hazards and risk control and mitigation measures, anticipating the occurrence of events that affect safety; Explicit-all safety management activities are documented, visible and conducted independently of other activities.

The main reference to set the SMS in the railway's security policy-directive 2004/49/EC of 29 April, the European Parliament and of the Council, which was transposed to the Portuguese legal framework by Decree-Law No. 270/2003, as amended by Decree-Law No. 231/2007 of June 14.

The safety system principles emphasize a rigorous development of strategies for mitigating the security risks, through a complete risk assessment and your management in the long term. System security requires the application of technical and management skills in a systematic manner, with a proactive vision in terms of identification and control of hazards throughout the life cycles of the projects, programs and activities, as Roland & Moriarty (1990).

The systematic registration of safety occurrences allows the establishment of the Organization's risk profile and performance recommendations, being systematic risk assessment basis for the typification of the Organization's risk. The registration of all security data, is essential for daily monitoring of safety occurrences, the preparation of safety reports, indicators of safety and Security objectives definition. This SMS monitoring circuit is appropriate to the current operations of the rail system. There are, however, significant operating system changes that require a specialized approach for example: Use of a single agent on the train; Empowering the SMS of a part of the operation; Acquisition of new rolling stock; Amendment of technical systems of rolling stock with impact on safety; Placement of human resources in railway activity in new lines (e.g. international traffic); Reorganization of security support. These changes modify the risk profile of the Organization through the introduction/modification of activities, technologies, procedures, skills, among others aspects that will lead to new types of occurrences. The early definition of these new types of occurrences and their risk level is essential to implement preventive measures that minimize the risk introduced by these changes.

3. Change management by application of Common Safety Method

The European Railway Agency (2010), supports the implementation of the Common Safety Method (CSM) in the framework of the European rail system, as support for change management having promoted a broad explanation, those interested in the rail sector, the process of assessment and management of risks as defined by Commission Regulation (EC) no 352/2009, replaced by Regulation (EC) no 402/2013, April 30. The framework of the common security Method consists of six modules: Selection of significant changes; Hazards identification; Analysis and determination of risks, Registration of dangers; Demonstration of conformity with the safety requirements; Accreditation and independent assessment of the correct application of the CSM.

The nature of the amendment (significant/non-significant) is a sole responsibility of the proposer of the amendment (e.g. rail operator) and is based on the judgment of experts in the field in each organization. The identification of hazards assumes a prior definition of the scope of the system (functions and interfaces) analysing, defining the relevant contributions and the level of detail required. The hazards identification made by iterations until reaching the level of detail required, defines the acceptable risks (registration) and the unacceptable risks of each function and interface, sorting the estimated. The identification of hazards requires the preparation of a Checklist of undesirable events, their causes and consequences, with a frequency estimate and measures proposed. The analysis and estimation of the risk acceptable risks, considers three options (if not set national rules concerning this analysis): comparison with a reference System, so that the new system has the same level of safety; a code of practice that is widely recognized, appropriate to the type of danger analysed and publicly available to all actors; explicit Estimation and determination of Risk (e.g. ISO/IEC 73), towards the identification of new dangers and the explicit estimate risk, through the collection of quantitative information concerning the frequency and severity of incidents. The rregistration of dangers after change implementation. This record can be part of information

documenting the life cycle of the system. This record is a source of evidence to manage the safety management System and can be consulted by the National Safety Authority.

4. The management of changes in a Portuguese railway operator

The company carries out transportation of passengers, with a fleet of hundreds of vehicles that run through every day tens of thousands of km of infrastructure. The timetables are set for an annual time horizon/semi-annual, being complemented in weekly and daily terms depending on special requests. The availability of vehicles depends on service providers. The work is highly regulated and subject to very stringent security criteria that try to minimize occurrences of security (e.g., breakdowns, accidents, etc.).

The company applied CSM on several occasions. The increase in carriage commercial speed is one of those examples. The project was considered a significant change by entail the variation of the braking system of the carriage, one of the bodies with greatest impact on vehicle safety. The change was typified as operational in nature, consisting of technical modifications, considering that each modification technique adds eventually new risks.

For all the dangers identified it was possible to identify a code of practice and/or reference system. The deviations are non-existent in the implementation of codes of practice and the slippages identified relative to the reference system have been identified, having been considered irrelevant.

In the framework of risk analysis was provided for the monitoring/monitoring the in-service behaviour of the cars until two years after the start of your commercial operation at speeds greater than the previous one. After the closure of risk analysis of speed change of holding, a report was drawn up, by compiling occurrences that have occurred during this period, under the identified hazards.

5. Survey of aspects relevant to the management of changes

The views of the Organization were collected through document review, interviews and questionnaire to experts in the security management system, risk management, legal and normative regulations and operations, featuring the elements relevant to the activity of management changes and your interaction with the SMS. An identification of internal and external stakeholders more relevant and your selection has been trying to diversify the training base, the intervention area within the Organization and with high levels of experience and responsibility. The stakeholders were audit, namely personal working for the verification of conformity of the application of the procedures by the various organs of the company; operations, particularly personal working on planning, preparation, execution and evaluation of the service, as well as the preparation of resources in terms of personnel, vehicles, infrastructure and respective operating instructions; information systems, personal working for the definition of needs and implementation of information systems and technologies; certification, in particular personal working in the monitoring of business processes; safety, responsible for the management of the SMS; legal; maintenance and repair; and railway regulation.

The experts consider the management of unanimous changes an aspect critical to the organization. They point weaknesses of the regulatory process, the lack of and examples of application of the requirements and practice/general technical instructions that can be adapted to the specificity of the organization without use/reliance on consultants.

It is stated that the development of quality management systems and environment and safety management system made it possible to develop a more process-oriented and a greater understanding of the interdependencies between the company's activities. The safety management system is referred to as a critical element that comes to systematize the collection and processing of information, and change management as independent component and framed in the system. Prior to this change management approach just as situation and always linked to the acquisition or rehabilitation of rolling stock.

Experts state that CSM, allows them to address the emerging dangers/ risks more sooner and associated with the resources and practices that gave rise to them, anticipating that knowledge. Experts associate the current structure of national rail system to be the biggest problem on implementing and manage changes. The lack of integration between organizations responsible for different elements of the system, with lack of communication and coordination, makes it difficult to identify and manage the dangers related to changes that end up not being identified in a consolidated manner. This situation is particularly relevant because the system has a high technical and functional integration. The duplication of information systems is also referred as an element that limits the development of the organization's risk profile.

The main facilitator element mentioned by experts is the use of multidisciplinary teams in the change management process. The involvement of different valences of this analysis facilitates the recognition and acceptance of the results, leading also to proposals for feasible and effective mitigation measures.

There is a high level of agreement and consensus about the relevance of each CSM activity.

Changes with impact on security, may not be recognized as significant allowing less structured processes of analysis of the risk involved. Not understanding the significance of the changes invalidates the assumptions of the method and weakens the security management system.

Another very important step focuses on the aspect of the selection principle of risk acceptance. The use of the principles is limited to the use of codes of practice where there is great experience and the evaluation of similar systems, due to a history of great activity in the engineering development of organizational structures and operational processes in conjunction with other operators and manufacturers and that can be replicated. The implementation of risk control mechanisms and monitoring of hazards are equally important steps.

Technology related changes as the rolling stock have a registration system of occurrences and own and a monitoring team of engineering that makes them effective enough. The follow-up to the outcome of changes in organization, processes and activities is far more difficult, due to limitations on hazards monitoring.

6. Conclusions

The study concludes that the change management process helps the organization to plan, manage and implement critical changes to its operations and the subsequent monitoring of the risk profile. The management of changes is not always assumed as integrated process, whose result influences the performance of the areas covered by each change.

In addition to the aspects related to risk management culture that only recently that were formalized in terms of standards and national regulations, the application of this methodology implies the merging of technical skills about technologies, processes and railway activities.

The improvements in the application of this method include technical aspects of implementation, awareness capacity and involvement of key people with relevant and multidisciplinary skills, coordination and transfer of information between business partners.

The study looked at the reality of the change management according to the perspective of a particular area, focusing on the railway safety management system. In a future study, it will be interesting to see to what extent the issues affecting this reality will also be extended to other perspectives in the company particularly in emerging risk areas such as the protection of personal data, whose legal requirements require changes at the same time cultural, and technological procedures.

References

1. Agência Ferroviária Europeia. (2010). *Uma abordagem sistémica - Manual de aplicação para a conceção e aplicação de um Sistema de Gestão da Segurança ferroviária.*

2. An, M., Chen, Y., & Baker, C. J. (2011). A fuzzy reasoning and fuzzy-analytical hierarchy process based approach to the process of railway risk information: A railway risk management system. *Information Sciences, 181(18)*, 3946-3966.

3. Blokdijk, G. (2008). *Change Management 100 Success Secrets-The Complete Guide to Process, Tools, software and Training in Organizational Change Management.* Brisbane, Australia.: Emereo Pty Ltd.

4. Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: design characteristics and mitigation capabilities. *Decision Sciences,* 38(1), 131-156.

5. Davey, J. D., Freeman, J. E., Wishart, D. E., & Rowland, B. D. (2008). Developing and implementing fleet safety interventions to reduce harm: Where to from here? *Proceedings International Symposium on Safety Science and Technology VII.* Beijing, China: QUT Digital Repository: http://eprints.qut.edu.au/.

6. Fleming, M. (2001). *Safety Culture Maturity Model. Report 2000/049.* Colegate, Norwich: Health and Safety Executive.

7. Gander, P., Hartley, L., Powell, D., Cabon, P., Hitchcock, E., Mills, A., & Popkin, S. (2011). Fatigue risk management: Organizational factors at the regulatory and industry/company level. . *Accident Analysis & Prevention, 43(2)*, 573-590.

8. Hirsch, R. (2006). Reducing risk by probabilistic assessment, defence in depth and precursor monitoring. In: China International Railway and Metro Safety. *International Railway and Metro Safety Conference.* China: Imperial College, CoMET.

9. Jeffcott, S., Pidgeon, N., Weyman, A., & Walls, J. (2006). Risk, trust, and safety culture in UK train operating companies. *Risk analysis*, 26(5), 1105-1121.

10. Kim, D., Baek, D., & Yoon, W. (2010). Development and evaluation of a computeraided system for analyzing human error in railway operations. *Reliability Engineering & System Safety, vol. 95, nº2*, 87-98.

11. Kotter, J. (2012). How the most innovative companies capitalize on today's rapid-fire strategic challenges-and still make their numbers. *Harvard business review*, 90(11), 43-58.

12. Kyriakidis, M. (2013). *Developing a Human Performance Railway Operational Index to enhance safety of railway operations.* UK: Doctoral dissertation, Imperial College London.

13. Kyriakidis, M., Hirsch, R., & Majumdar, A. (2012). Metro railway safety: An analysis of accident precursors. . *Safety science, 50(7)*, 1535-1548.

14. Moosa, I. (2007). Operational risk: a survey. *Financial markets, institutions & instruments*, 16(4), 167-200.

15. Newnam, S., & Watson, B. (2011). Work-related driving safety in light vehicle fleets: A review of past research and the development of an intervention framework. *Safety Science, 49(3)*, 369-381.

16. Regulamento. (2013). *(CE) Nº 402/2013 DA COMISSÃO de 30 de abril de 2013, relativo a um método comum de segurança para a determinação e a avaliação dos riscos e que revoga o Regulamento (CE) n. o 352/2009.* Parlamento Europeu e do Conselho.

17. Roland, H. E., & Moriarty, B. (1990). *System safety engineering and management.* . John Wiley & Sons.

18. Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* UK: Pearson Education.

19. Smith, P., Kyriakidis, M., Majumdar, A., & Ochieng, W. (2013). Impact of European Railway Traffic Management System on Human Performance in Railway Operations: European Findings. *Transportation Research Record: Journal of the Transportation Research Board*, (2374), 83-92.

20. Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Anal,11* , 499–507.

21. Vaughan, D. (1997). *The Challenger launch decision: Risky technology, culture, and deviance at NASA.* U.S.A.: University of Chicago Press.

22. Yin, R. K. (2014). *Case study research: Design and methods (Fifth Edition).* USA: Sage publications.