

IT Innovation and its Organizational Conditions in Safety Critical Domains

The Case of the Minimum Safe Altitude Warning system

Simone Rozzi*, Paola Amaldi[†]*, and Barry Kirwan*

*[†]EUROCONTROL Experimental Center, Bretigny-sur-Orge, France

[†]Interaction Design Center, School of Information and Engineering, Middlesex University, London, UK

Keywords: Organizational/Institutional Precursor, Innovation Induced Risk, Interaction Failure

Abstract. Safety critical organizations modernize routinely their infrastructures in order to improve safety and productivity. However, such improvement might be compromised if new tools are not delivered, or fail to be adopted by operators, or worst introduce safety critical conditions. This research investigated the interactions between innovation processes introducing new operators' tools and the underlying organizational conditions. An application from the ATC domain, the MSAW, is taken as a main case study. Its development and history have been investigated within four European Air Navigation Service Providers. Findings indicated that the ability to set up the tool correlates to the presence of a safety net governance by which the organization develops the expertise to set up the tool over successive development cycles – no service provider encountered immediate acceptance of the tool. On the other hand opportunistic decisions to adopt the tool, misconceptions about its rationale, transfer of control over requirements and their implementation to manufacturer, hampered access to system parameters by ANSP personnel and increasingly rigid manufacturer-ANSP relationship in the down stream contract phase appear to relate to poor implementation of the tool and prevent prompt improvements.

1 Introduction

Information Technology (IT) upgrade does not always lead to the successful adoption of the newly introduced operators' tools. These are often “misused” or “underused” [1], or worst they are known as interfering with operational practices by generating safety critical situations. Consistent with Lyytinen and Hirscheim [2] we term these situations as “*interaction failures*”.

This paper aims at advancing current understanding of how safety critical organizations organize in order to avoid the occurrence of interaction failures during the modernization of their infrastructures. This topic appears to have been touched

by three relevant areas of the literature, although none of them appears to have dealt with it specifically.

2 Motivations and Background

Notably poor automation design and its error inducing conditions have set the agenda within the areas of cognitive engineering [e.g. 3,4] the focus being on the dynamics embedded in the human-machine interface unit – also expressed with the notion of *joint cognitive system* [5]. Well-known contributory conditions to interaction failures are the poor consideration of human and safety requirements along the development process of new automation and late intervention of human factors and safety specialists [6,7,8]. However these conditions are often mentioned independently of the broader organizational/institutional context within which they occur. IT innovation is not an isolated process independent of the societal structure in which it takes place. In reality many trade off decisions affect the way safety is built throughout the innovation process.

Safety risk information although available may be exposed to distorting organizational influences [e.g. 9,10,11,12]. Clarke in the analysis of risk decisions associated to decision to build a trans Alaska pipeline, suggests that it is incorrect to think that considerations on safety and risk lead decision-making; often it is the opposite case: once decisions are made based on political and economic ground, then safety estimates are made to show how necessary and safe is the new system [13]. Similarly Vaughan's seminal investigation of the Challenger Space Shuttle disaster indicates that safety assessment reflects more the organizational structural context rather than statistical figures alone [14].

Safety theorists have extensively theorized around the organizational bias leading to safety critical conditions. These include for instance commonly held mis-beliefs about hazards, poor communication, inadequate information handling in complex situations, impaired decision-making, lack of regulatory as well as contractors' oversight [15]. Vaughan [16] notes how such precursors are systematically produced by traits of the higher social structure within which they are embedded. These include in particular the degree of

interdependency between regulatory and regulated organizations, and the presence of highly competitive environment and scarce resources, ultimately leading to the normalization of hampered risk assessment in everyday decision making. The idea that safety erodes in face of increasing productivity is a well-recognized accident-inducing pattern today among many safety theorists [e.g. 17,18,19,20,21]. The idea being that while several actors in the work system – from the operators to administrators, managers and regulators – take decisions that appear sound according to their local productivity and safety constraints, they might actually be adding some unsafe conditions for someone in the work process, so that the aggregated effect of those individual decisions push the work system to operate beyond its safety margins. It has to be noted that these views have developed to explain the organizational bias preceding accidents. Hence the focus is on how the organization might lose control of its safety critical processes during operation, rather than innovation processes, which notably relate more to the process of design and development.

Finally, literature from the diffusion of innovation (DOI) area has focused more directly on how the organizational context might affect the process of innovation [22]. Notably, DOI has been focused on a wide range of innovations – from weapon systems and medical devices to consumer electronics and policy programmes – and their innovation development process, this one including “all the decisions, activities, and their impact on a final innovation, that occur from recognition of a need or a problem, through research and development of an innovation, commercialization through diffusion and the adoption by users, to its consequences” [22]. According to Rogers, if on the one hand organizations are stable systems made of individual organized to achieve common goals through hierarchy of ranks and division of labour, innovation is a constant on going process within them. Here the adoption process is much more complex than in the case of individuals. For instance following the decision to adopt, implementation might not follow through, due to the high number of actors involved in the decision process. Most importantly the innovation process might be shaped by structural factors: for instance organizations presenting low centralization, high organizational complexity, and low formalization facilitate the development of new innovation although they might obstruct implementation [23]. Further internally generated innovations are more likely to be implemented since they are more likely to match the need of the organization, and because personnel identify the innovation as their. While one of the merits of DOI has been to shed light into organizational dynamics underlying innovation process, scholars in the area have not been concerned on how the same organizational context might induce safety critical conditions on the innovation process.

To summarize work from the automation arena have stressed the error inducing conditions of automation, but have not been concerned on how these are produced by the social system within which they are embedded. Safety theorists, despite having extensively theorized around the

organizational precursors to safety critical conditions, have focused primarily on understating how organizational bias might lead to accidents, but not on how these affect innovation processes. Finally literature from the DOI area has noted an interaction between the innovation development process and the underlying organizational conditions. However such link has not been analysed from a safety perspective.

3 Objective

This paper takes an application from the air traffic control domain, the Minimum Safe Altitude System (MSAW) to understand how four European Air Navigation Service Providers engaged on its implementation and avoided interaction failures related to the tool. The objective has been to reconstruct the development and the history of the tool within the organization from the perspective of those developers, engineers, managers, controllers and safety experts that were involved in its implementation, in order to understand in this case:

- How did ANSPs organized to avoid MSAW related interaction failures?
- How did they fail to do so? i.e. How did they organize to contribute unintentionally to the very phenomenon they should ideally avoid?

4 Methodology

The present research consists on an exploratory qualitative Case Study centred on a system (MSAW) as developed and operated by four European Air Navigation Service Providers. The Case Study Methodology as described by [24] is an appropriate methodology to explore novel areas of inquiry.

4.1 Data Collection

Data has been collected in 2010 over six Air Traffic Control Centres distributed over four European Air Traffic National Service Providers over a period of 10 months. During each visit, narrative interviews with R&D directors, safety managers, developers, and air traffic controllers, have been carried out on local development practices, the organizational context, as well as the use of the tool. Interviews have been carried out also with international standards and safety policy developers, as well as regulators.

Narrative interviews consist in an in depth unstructured interviews focusing on a particular experience – the development of the MSAW in this case – during which the interviewer minimizes his intervention, while encouraging the interviewee to expands on points that might be of interest for the understanding of the story. Narrative Interviews are an established research method in management, social, and information system failure research. Beyond interviews, a variety of documental evidence – including MSAW requirements, use procedures, national regulations, service notes, accident reports – have been collected.

4.2 Data Analysis

Firstly data have been analysed by a network analysis approach as developed in organizational [25,26] and public policy research [27]. As illustrated by Roe [27], the basic method proceeds as follows: If individual X argues that the problem statement 1 lead to problem statement 2 (1→2), and individual Y problem argues that problem statement 2 lead to problem statement 3 (2→3), then the aggregated network is 1→2→3. In our work data have been coded for causal claims and problems as mentioned by study participants. Subsequently these codes were aggregated on a single network charting chains of events, decisions and conditions influencing the development of MSAW. Such network stretched beyond the individual perception of the problem as experienced by individual participants. Most importantly it stretched beyond organizational boundaries of function and structure, ultimately allowing the researchers to make sense of a highly complex situation where several influence factors co exist.

This level description was based on categories mentioned by study participants, i.e. with no top down imposition of any theoretical framework. This maximized the chances of inductive theorizing – which instead would have been compromised by attempting to force evidence into existing theories on a top down fashion, as some data would have been inevitably lost. After this step the network has been checked for the presence of contradictory or circular arguments at individual and intergroup level. Also emerging dependencies were subject to confirmation by triangulation with other data sources, in order to increase the validity of the network.

The last step in the analysis made use of the analogical theorizing method [28,29] to convert the data in a more structured theoretical explanation. The dynamics emerging in the network were coded by some “larger” theoretical construct that appeared to best illustrate the phenomena under scrutiny. This phase involved cycles of systematic literature reviews – in areas such as organizational safety, organizational behaviour, political science, IT management – to identify, compare and import the theoretical construct that best described the phenomenon unveiled by the network. This process was repeated until a final explanation was achieved and reproduced on a final narrative.

5 The Application Case: MSAW system

The Minimum Safe Altitude Warning system or MSAW is a subsystem of the main radar system intended to alert air traffic controllers of aircraft close proximity to terrain. The system compares the current or projected aircraft altitude against a predefined terrain database. Whenever an aircraft descends or is about to descend below a predefined minimum altitude the system generates a visual and aural warning. Upon reception of the MSAW alerts, the controller has to inform the pilot of the imminent danger, so that he or she can take a resolving manoeuvre if necessary. MSAW is the

ground equivalent of the – perhaps more famous – Ground Proximity Warning System (GPWS) available in the cockpit.

The system was first developed in the 70ies as a protection against Controlled Flight into Terrain accidents (CFIT), i.e. accidents occurring whenever an aircraft is flew into terrain, obstacles, or water, without any technical failure and the crew being unaware of the imminent collision. CFIT are one of the leading categories of civil aviation accidents. The likelihood of CFIT is considered to be higher during the phases of landing and take off, especially in presence of high terrain, and/or man made obstacles, such as building or antennas.

The MSAW is member of a class of application called safety nets, intended to alert the controller of potential risks such as conflicts with other aircraft (Short Term Conflict Alert or STCA), infringement of protected airspace volumes (Area Proximity Warning System or APW), and deviations from final approach path (Approach Path Monitor or APM).

In the context of MSAW, one class of interaction failures are those nuisance alerts generated due to poor set up of the terrain database. In fact the higher the mismatch between the database and the underlying terrain, tall buildings, or other man made obstacles, e.g. antennas, the higher the number of nuisance alerts. Technically speaking, such matching requires fine-tuning of the terrain database, and is more difficult in presence of high and variable terrain – e.g. reef – where also the role of the alert is more critical. Operational evidence indicates that high number of nuisance alerts have resulted in the system being ignored, or intentionally inhibited by service personnel, so that the alerting capability was hampered during safety critical situations [e.g. 30, 31].

6. Tuning Process: What service providers do to avoid Interaction Failures

A main index of avoidance of interaction failures turned out to be a “mature tuning process”, whereby the tool was fitted to local terrain and traffic conditions. The mature tuning process presents at least three main traits:

1. Having access to records of real traffic data that can be used for testing purposes. Using real data is deemed a fundamental step in order to (i) make sure tuning is based on traffic patterns typical of a particular site, and (ii) minimize the risk of missing relevant (terrain and aircraft) conflict points, as in the case of artificially generated traffic data;
2. Having a test-bed able to replay traffic data in fast time simulations and to generate statistic about the performance of the tool;
3. Having expert (representative) controllers involved in the process since the very beginning. The role of these controllers is that of providing an operational interpretation on the generated statistics to help developers classifying necessary from unnecessary alerts. This decision, which ultimately is based on expert operational judgment, allows developers to modify the

system, for instance by modifying algorithm parameters or adding inhibited volumes. This process relies extensively on operational judgement and is repeated until the performances of the tool are considered acceptable.

In the cases where such process was being deployed the organization was able to specify the functionalities - including the dimensions of the grid, its inhibited areas, and volumes – to be implemented by the manufacturer, hence maximising the likelihood of acceptance of the tool by its intended users, i.e. the air traffic controllers.

6. Safety Net Governance: How do service providers organize to avoid Interaction Failures

Avoidance of interaction failures and consequent high acceptance of the tool seemed to be highly correlated to the presence of a “*Safety Net Governance*” framework. We borrowed the concept of governance from the domains of clinical practice and IT. In its original formulation the notion includes (i) building the organizational capabilities to oversight the continuous monitoring and improvement of the quality of service and safe guarding of high standards of care [32,33], and (ii) ensuring that decisions about management and use of IT are harmonized with the business need of the organization [34]. In both acceptations the idea of governance implies the ability to direct organizational processes, roles and expertise to the improvement of some concept of quality. In this study we adopted the term safety governance to denote the organizational capability to oversight the life cycle of MSAW and other safety nets as well as guaranteeing their continuous improvement to make sure these systems deliver the intended benefit.

This seemed to be guaranteed by a focus on a feedback-feed forward cycle of tool improvement centred on controllers. The tuning process described in the previous section appear to reflect a larger effort whereby the organization systematically collect feedback on the tool, and then feed it forward into improvement actions. The focus on such feed back-feed forward cycle does not halt when the tool goes operational, rather is in place through the entire system lifecycle.

Such process was found to be supported firstly by a dedicated organizational structure – usually known as “Safety Net Task Force” or “Safety Net Group” – dedicated specifically to develop expertise in the domain of safety net. This structure adds to traditional safety department. Its respective leaders could interact with senior managers and directors to report on state of safety nets and guarantee that competent and sufficient resources were allocated to safety nets definition and maintenance. Usually such structure presents a high degree of specialization, in that each safety net is associated to an engineer. In some case these were former engineers working previously for the manufacturer competent with MSAW installation. In fact cross transfer of personnel from manufacturer to service provider was reported to increase the

ability of the latter to specify requirements and oversight manufacturer practices, as opposed to situations where little expertise was available which as it will be described later are an important precursors to installation failure. Another important role of this dedicated structure was to guarantee compliance with safety regulations. It has to be noticed that in the present case no regulators was reported to have oversighted the development of safety case during the development and improvement of the MSAW system.

Finally, dedicated tools supported such organizational structure. For instance beyond the test bed needed for the tuning of the system, other tools were defined specifically for evaluating MSAW and safety net performances. This included dedicated data analysis for replaying MSAW and other safety net behaviour following the occurrence of incidents. This assessment occurred in addition to the regular monitoring – this one achieved for instance by e-mail reports on tool performance sent on a regular basis to the responsible engineer.

7. Failing to avoid MSAW Interaction Failures

It is useful to consider that all of the MSAW installed by the service providers included in this study encountered poor acceptance after their first respective implementation – due to the high number of nuisance alerts generated. Eventually three of our service providers removed the tool after the first implementation.

Also in all cases, this initial phase where the organization gain an awareness of the challenges related to the set up of the tool, was followed by an improvement phase, where resources have been allocated to transit to a state where the tool was deemed reliable by its users. Two service providers are in this situation today and are regarded as best class implementation in the industry, and present the process and organizational infrastructure described in the earlier sections. The other two are in the process of improving, for instance by entering contracts with different manufacturer, or with the help of external consultants able to bring into the company additional level of expertise.

8. How ANSP might unintentionally promote the very phenomenon they should avoid

This section describes how organizations have organized to promote unintentionally the occurrence of Interaction Design Failure. This pattern was shared by those providers implementing Costumer Off the Shelf (COTS) MSAW.

8.1 Decision to adopt the system not matched by awareness of rationale and challenge in implementation

A first common condition appear to be the decision to adopt the system without any rationale justifying the introduction of the tool and with no outline of the challenges related to the

fine tuning of MSAW. At least in two cases the decision to adopt the MSAW system was taken during a major re-modernization process of real estate and major software systems, i.e. radar and flight processing systems. The MSAW was proposed by the manufacturer as an additional feature within the larger COTS package that was under acquisition. However there was little awareness about the need to have the MSAW system implemented, as opposed for instance to awareness of the need to replace the major radar processing system. Some of our study participants reported that their knowledge of MSAW system was limited to awareness of the acronym when they committed to implementation. Further it was assumed that the acquired COTS MSAW system was virtually quite suitable to the needs of the specific Air Traffic Control Center, and all that was needed to get it going was the manufacturer expertise to set it up.

A contributory factor to this situation was the state of international regulation and standard material on the tool when the service providers committed to its implementation. For instance the relevant ICAO standard [35] although specifying the MSAW operational concept did not clarify the definition of the minimum safe altitude – the essential parameter in the definition of the tool. Personnel reported that in their view it was not clear the rationale for having safety nets implemented from international standards [36]. Furthermore the relevant safety policy [37], while advocating excluding safety nets from risk assessment, was interpreted as demanding to exclude MSAW from the safety case; hence no tool specific safety case was developed. In general study participants perceived the regulatory situation as obfuscated and messy, at least until 2005, since EUROCONTROL initiated the development of safety guidance material specific for safety nets [see e.g. 38].

8.2 Consequences: Requirements do not get specified, control over tuning transferred to software manufacturer

The situation described above contributed firstly to leave the system underspecified – in some cases no MSAW requirement was developed at all, and the tool appeared simply as a label in the contract. But most importantly, the control over tuning of the system was implicitly transferred to the software manufacturer; without any formal control mechanism over such transfer – neither contractual, as in the worst cases no MSAW requirement was present in the contract; nor regulatory, as ATC software manufacturers were not subject to the maintenance of a safety case related to the development of new systems available for regulatory inspection and monitoring.

With no rationale and requirements specified by the service providers, the MSAW installation reflected more the manufacturer's view on the set up of the tool. In some cases the terrain database instead of being defined according to the specific terrain conditions, was adapted from that used on the site of a previous manufacturer's client. As a result the new grid was poorly fitted to the terrains. In another instance the

manufacturer exploited a grid that was specified for a different weather related function, so while the grid served well the intended function, its units were far too large for MSAW, hence generating too many unnecessary alerts. Further issues related to traceability of rationale behind MSAW parameters were observed. In one case, after the organization entered an improvement cycle in order to make the alert more reliable, it appeared to be difficult for the manufacturer engineers to explain all of their MSAW parameters. As one consultant put it, it looked as if the manufacturer was not entirely aware of the effects of the parameters on the MSAW performance and the trade off involved.

But poor traceability might only part of the story. In fact an emerging deeper structural condition was the willingness of the manufacturer to retain exclusive control over the core software functionalities. So that minimal training can be provided to service personnel, which in turn find difficult to access and change software parameters.

Finally, it has to be noted that fundamental gate in the service provider-manufacturer relationship is the contract. The upstream contract phase is an open window to negotiate the requirements to be implemented – at least when expertise is available. However, after the contract is signed, such windows shrink dramatically; manufacturer's responsiveness to accommodate changes or new requirements was perceived to decrease. New request might take place at the cost of postponed deadlines or additional costs. This is particularly true if the manufacturer opt for aggressive service and maintenance marketing strategy. In this case the product has been offered at an advantageous price over competitors' products, implying that profits will arise from changes and upgrades to the system. When this strategy is particularly aggressive, even minor technical changes, not just to MSAW, might become the object for demanding and protracted dispute.

To summarize, with expertise and control over software parameters entirely on manufacturer side, and with revenue logic oriented to service and assistance resulting on protracted negotiations, it becomes obvious why system improvement cannot be addressed promptly. In the best case the tool has been removed from operation.

9. Summary and Conclusion

The objective of this work has been to explore the interaction between organizational conditions an innovation process on going in safety critical organizations. We have taken an application from the air traffic control domain, the MSAW, and reconstructed his history within four European ANSPs, from the first deployment until today; to understand how these providers organize in order to avoid a class of MSAW related interaction failures.

We noted that a condition indicative of the ability to avoid the interaction failures and achieve high acceptance of the tool

has been the presence of a mature tuning process. Such process allows the organization to specify the requirement of the tool to the manufacturers. A second condition was the presence of a Safety Net Governance, i.e. an organizational capability centred on MSAW and other safety nets and responsible for their set up and continuous improvement. Central in this governance is the focus on the controller feedback cycle, by which the organization systematically collect feedback from the controller that will feed forward into further improvement.

One interesting finding was that no organization encountered immediate acceptance of the tool, due the high number of nuisance. All organizations, even those that today are acknowledged as having mature tuning process in place and have organizational and technological resources allocated to the tool, encountered poor acceptance of the tool after their development. This evidence suggests that before the organization is able to get the tool accepted by its users it has to go through a learning path made of successive iterative development cycles, where it learns to organize, and develop the expertise needed to set up the tool. The occurrence of hindrances seems a necessary step in this process. Perhaps one reasons for tool withdrawal to occur might be that such learning process exceeds the schedule allocated to implementation – the latter being dictated more by regulatory pressures or the need to have the tool operational before major public events that could increase significantly air traffic.

Finally the structural conditions associated to a high number of nuisance alerts and poor acceptance of COTS MSAW were reported. These included:

- Mis-beliefs on the ANSP side about the difficulties associated to the implementation of the tool being purchased and the degree of operational expertise required. This condition was associated to opportunistic decision to adopt, and under specification of tool rationale and requirements. Ultimately it transferred control over requirements and their implementation to manufacturer, without any oversight mechanism;
- Progressive freezing of the ANSP-manufacturer relationships in the downstream contract phase, where the ANSP might find reduced its capability to demand system improvements, if not at the cost of renegotiated deadlines or extra costs;
- Manufacturer interest to keep control of its system core processing in order to preserve its competitive advantage. This resulted in limited access on ANSP engineers to software parameters, which were entirely dependent on manufacturer for system improvement.

Overall these conditions not only result on a poor implementation of the tool, but also may make it difficult to achieve quick improvement.

Acknowledgment

This study is part of an ongoing doctoral research programme sponsored by EUROCONTROL Experimental Centre, Brétigny-sur-Orge, France. We wish to express our gratitude to all the staff and study participants that took part into this study, and Mr Andy Kilner, from EUROCONTROL, for his generous support during site visits. The views expressed herein do not necessarily reflect the official views or policy of the agency.

REFERENCES

- [1] R. Parasuraman and V.A. Riley, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors*, vol. 39, 1997, pp. 230-253.
- [2] K. Lyytinen and R. Hirschheim, "Information Systems Failures: A Survey and Classification of the Empirical Literature," *Oxford Surveys in Information Technology*, vol. 4, 1988, pp. 257-309.
- [3] D.D. Woods, "Decomposing Automation : Apparent Simplicity , Real Complexity," *Automation and Human Performance: Theory and Applications*, R. Parasurman and M. Moulous, Erlbaum, 1996, pp. 3-17.
- [4] D.D. Woods, J. Flanagan, T. Huang, P. Jones, and S. Kasif, "Human Centered Software Agents: Lessons for Clumsy Automation," Washington, DC: National Science Foundation, 1997, pp. 288-293.
- [5] E. Hollnagel and D. Woods D., *Joint Cognitive System. Foundations of Cognitive Systems Engineering*, Boca Ranton, FL: CRC Press Taylor & Francis Group, 2005.
- [6] K. Cardosi, "Human factors Lessons Learned in the Design and Implementation of Air Traffic Control Systems," *The Controller, First quarter*, 1998, pp. 11-15.
- [7] C. Sandom and D. Fowler, *Hitting the Target - Realising Safety in Human Subsystems* , Ottawa, Canada: 2003.
- [8] N. Leveson G., *System Safety Engineering: Back To The Future*, Aeronautics and Astronautics. Massachusetts Institute of Technology, 2002.
- [9] H. Kendall and M. Shubick, "The failure of nuclear power," Kluwer, 1991.
- [10] L.L. Tascia, *The Social Construction of Human Error*, State University of New York at Stony Brook, 1990.
- [11] T. Dietz, R.S. Frey, E. Rosa, R.E. Dunlap, and W. Michelson, "Risk, technology, and society," Westport, CT: Greenwood, 1993.
- [12] K.J. Tierney, "Sociology's Unique Contributions to The Study of Risk," Bielefeld, Germany: 1994.

- [13] L. Clarke, "Oil spill fantasies," *Atlantic Monthly*, 1990, pp. 65-77.
- [14] D. Vaughan, "Regulating Risk: Implications of the Challenger Accident," *Law & Policy*, vol. 11, 1989.
- [15] B.A. Turner, *Man-Made disasters*, London: Wykeham Publications, 1978.
- [16] D. Vaughan, *The Challenger Launch Decision*, Chicago: University of Chicago Press, 1996.
- [17] D.D. Woods, B. Starbuck, and M. Farjoun, "Creating Foresight: Lessons for Enhancing Resilience from Columbia," Blackwell, 2005.
- [18] E. Hollnagel, *The ETTO Principle -- Efficiency-Thoroughness Trade-Off: why things that go right sometimes go wrong*, Ashgate, 2009.
- [19] J. Rasmussen, "Risk management in a dynamic society: A modelling problem," *Safety Science*, vol. 27, 1997, pp. 183-213.
- [20] N. Leveson, "A New Accident Model for Engineering Safer System," Boston, US: 2002.
- [21] J. Reason, *Managing the Risk of Organizational Accidents*, Ashgate, 1997.
- [22] E.M. Rogers, *Diffusion of Innovations*, New York, NY: Free Press, 2003.
- [23] G. Zaltman, R. Duncan, and J. Holbek, *Innovations and Organizations*, New York: John Wiley and Sons, 1973.
- [24] R.K. Yin, *Case Study Research, Design and Methods (4th Edition)*, US: Sage, 2009.
- [25] J. Porras, *Stream Analysis: A Powerful Way to Diagnose and Manage Organizational Change*, Reading, MA: Addison-Wesley OD Series, 1987.
- [26] D. Boje, *Narrative Methods for Organisational & Communication Research*, London: Sage, 2001.
- [27] E. Roe, *Narrative Policy Analysis, Theory and Practice*, Duke University Press, 1994.
- [28] D. Vaughan, "NASA Revisited: Theory, Analogy, and Public Sociology," *American Journal of Sociology*, vol. 112, 2006, pp. 353-393.
- [29] D. Vaughan, "Theorizing Disaster: Analogy, historical ethnography, and the Challenger accident," *Ethnography*, vol. 5, 2004, pp. 315-347.
- [30] NTSB, *National Transportation Safety Board Safety Recommendation A-06-44 through A-06-47*, Washington, D.C.: NTSB, 2006.
- [31] NTSB, *Controlled Flight into Terrain, Korean Air Flight 801, Boeing 747-300, HL, Nimitz Hill, Guam, August 6, 1997*, National Transportation Safety Board, 2000.
- [32] L. Donaldson, "Clinical Governance: A Quality Concept," *Clinical Governance in Primary Care*, T. van Zwanenberg and J. Harrison, Radcliffe Medical Press, pp. 3-13.
- [33] T. Swage, *Clinical Governance in Health Care Practice*, Reed Educational and Professional Publishing Ltd 2000.
- [34] M. Magee, P. Marounek, L. Mueller, and A. Phillipson, "IBM IT governance approach: business performance through IT execution," 2008.
- [35] ICAO, "Doc 4444, Chapter 15, Paragraph 15.7.4 – Minimum Safe Altitude Warning (MSAW) Procedures," International Civil Aviation Administration, 2001, pp. 14-15.
- [36] EUROCONTROL, "Operational Requirements Document for EATCHIP Phase III ATM Added Functions Volume 2 - Safety Nets," 1999.
- [37] EUROCONTROL, "SRC Policy Document 2. Use of Safety Nets in Risk Assessment & Mitigation in ATM," 2003.
- [38] EUROCONTROL, "Specifications and Guidance Materials for Ground Based Safety Nets," 2009, http://www.eurocontrol.int/safety-nets/public/standard_page/specifications.html, last retrieved 29 March 2010.