



City Research Online

City, University of London Institutional Repository

Citation: Sikora, I. (2015). Risk Assessment, Modelling And Proactive Safety Management System In Aviation: A Literature Review. Proceedings of Conference on Transportation Systems with International Participation,

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/16320/>

Link to published version:

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

RISK ASSESSMENT, MODELLING AND PROACTIVE SAFETY MANAGEMENT SYSTEM IN AVIATION: A LITERATURE REVIEW

Ivan Sikora
City University London,
Northampton Square, London, EC1V 0HB, United Kingdom

Summary

Safety and Risk are in the focus of the constant research ranging from strictly technical and technological to organisational influence. The increase of system's complexity and the shift of errors from purely mechanical to human and organisational has hampered the study and the prediction of accident probability. This paper reviews the literature for the Safety Management System (SMS) in aviation for their ability to account for the complex dynamics from which safety in these kinds of systems tends to emerge – or not. After this, it evaluates existing risk assessment modelling so as to assess the 'status' – or analytical strength – in this domain. The shortcomings of those models are presented to identify potential effective model's elements in relation to assessed the body of literature and current complex socio-technological systems present in air transportation system and other High Risk Organisation.

1. INTRODUCTION

High Reliability (Risk) Organisations (HRO) are usually complex technical systems¹ consisting of large numbers of components that operate in a coordinated manner with a potential of catastrophic effect to their operators as well as their environment in case of the failure. Despite only a few “sharp end” operators, the amount of energy involved and released in case of their mistake of oversight makes them comparable regardless of the fact whether they sail, fly or sit in their control rooms firmly on the ground.

The fact that HRO are highly regulated, and almost always failure free renders them even more difficult to analyse, let alone to study their potential failure promoting conditions or consequences. The increased complexity of the system together with the shift of the problems from technical towards organisational and human factors indicated the need for the modified approach in managing safety within HRO. SMS was one of the answers to this situation.

The structure of the SMS with approach to managing safety ranging from initially reactive to proactive and finally predictive is just one of the answers to this challenge. Human error is not

isolated from the system itself hence the proactive approach in this system with relevant Risk Assessment and Modelling practices are meant to cater for incidents even before they develop in fully developed accidents as stated by Lewis [1]. The complexity of the system and the interaction between its elements does not allow for comprehending all possible modes of failure. Therefore by effective observation and capturing error generating circumstances in the system one caters not for incidents and accidents that happened already but to attempt to indicate future ones.

It has been more than 120 years since the start of analysis of accident causation in order to prevent them or minimise their effect². The discovery of accident causes and circumstances enables their investigation, future accident prevention as well as the assessment of whether current systems are aligned with acceptable level of safety. The literature review presented in this paper serves the purpose of identifying Risk Modelling and safety data management approach appropriate for HRO organisations' nature.

¹ Aviation, Nuclear Energy, Military, Transport Systems, Healthcare

² Early research in accident causation and their investigation is attributed to Bortkiewicz in 1898.

1.1 The Evolution of Safety Thinking in Aviation

Incident and accident prevention in aviation was reactive before the introduction of SMS. Despite the fact that aviation safety level is better, compared to other modes of transportation, this approach was not good enough due to the nature of the industry. The apparent lack of incidents that had to be investigated as per national or international regulations [2] creates a difficult task when exploring trends or investigating circumstances that resulted in incident or accident. Having complex systems developed even more in the past 70 years made the task of accident prevention equally as challenging.

Initially early aviation development since the start of commercial flying has been hampered by technical flaws and problems. Figure 1. demonstrates that, since the introduction of jet engines by mid 20th century, the number of accidents has been reduced. Average time between them has increased to one in 100,000 flight hours [3].

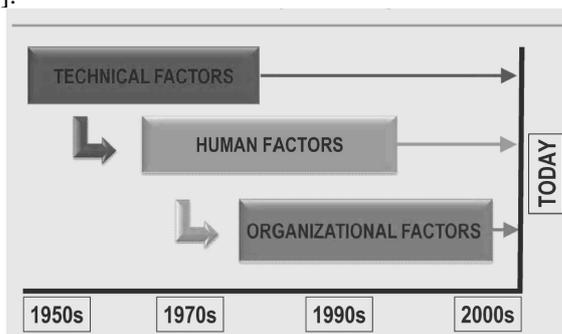


Fig. 1. The Evolution of Safety Thinking [4]

Having more reliable engines and components shifted the focus to other accident root causes. Improvements in Standard Operating Procedures (SOP) and Flight Crew training in addition to developments mentioned above have improved the ratio between accidents and the hours flown even more during 1960s and 1970s. Further discrepancy between highly developed and organised aviation regions continued for next two decades. Eventually there was a time when North American airlines would have expected an accident every two million flight hours while less sophisticated regions would have even 42 times less robust system [4]. That was the reason why aviation has started to apply systematic and regulated efforts to manage safety in all aspect of participating organisations.

2. A REVIEW OF EXISTING MODELS

2.1. Historical Review of Generic Accident Causation Models

Risk has been under scrutiny as early as the 17th century. Roelen makes the point that it was mainly the financial risk that has been studied and analysed [6]. Initial approach to accidents as sporadic events with “Act of God” nature has been modified so contemporary research about accident causation in industrialised society has been developed by end of 19th and early in 20th century.

Griffin states that the initial approach to explain accidents solely by the characteristics of their participants has changed by the introduction of the “Domino Theory” in early 1930s [7]. In his presentation of the same Heinrich has connected different elements in the chain of events that lead to an injury or accident. Among these were societal circumstances, human error, operator’s background as well as the accident trigger event.

The focus of all early models on accident circumstances originated from military and industrial organisations where they were developed and applied initially to reduce the number of injuries and financial losses generated by mishaps and unsafe acts. Towards the mid 20th century initial causation theories were enriched by new elements and some models for conflict predicting have been added to mainly reactive methods in use.

Netjasov and Janić stated that one of the first models that International Civil Aviation Organisation (ICAO) attempted to tackle safety and capacity over the North Atlantic was “Machol-Reich” in late 1960s [8]. Still the number of accident investigation models superseded the number of accident prediction (by risk assessment and management) until 1970s.

Improvements in systems safety due to the shift in understanding the influences on systems operations and safety from technological to human and organisational factors have gradually diminished. Hence, as Netjasov and Janić stated, new elements had to be introduced to develop more advanced models. For example, management and management related influences were introduced by Weaver [9] initially followed by Bird and Loftus [10]. The initial three elements from the “Domino Theory” have been linked when Adams [11] introduced organisational error as an element. Finally the 90s “Generic Error Modelling System” developed by James Reason [5] has been enabled through Johnson [12] and his barriers to error discussion.

James Reason’s widely accepted accident causation “Swiss Cheese” model is represented by

rotating cheese slices (Figure 2.). When the threat (represented by the arrow) makes it all the way from its origin through aligned “cheese” holes, it materialises and accident happens. Provided any of the slices blocks the path, the threat cannot develop further to a mishap.

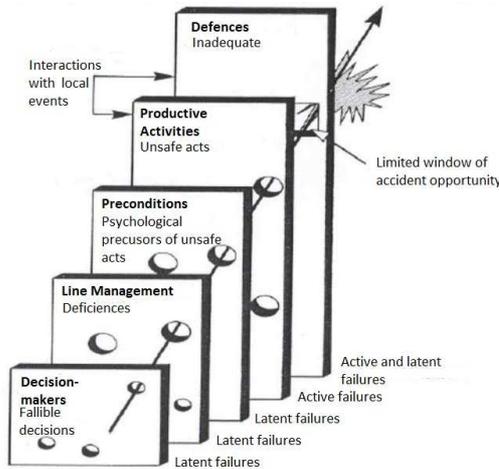


Fig. 2. Reason’s “Swiss Cheese” Model [5]

Despite the fact that this theory has helped to develop others³ it has not evolved so much from the initial “Domino Theory”. So the end of the 20th and early 21st centuries has brought new challenges in understanding accident causation in aviation. Contemporary systems have commanded the need to adjust our “common” modelling to their advanced and new logics.

Papers and books from the late 90s indicate several attempts to design over encompassing and comprehensive SMS models. Rasmussen’s [13] early overview of safety in complex socio technological systems established the basis of related research areas focused on factors contributing to an accident within those systems.

“Normal Accident” theory introduced by Perrow [16] explains system accident by complexity and interrelation between systems. This is reinforced by Reason’s [5] study of organisational factors and the structure that contributes to accidents. Following this approach the HRO name has been introduced to describe management of complex systems as in Rijpma [17]. Focused attention to organisational factors and conditions contributing to system safety resulted in Hollnagel et al. introducing the notion of resilience [18].

This has allowed for formal analysis of systems’ organisational structure, conditions and their response to developing safety issues. Alongside these developments aviation has addressed issues and adopted recommendations through SMS. [4, 19]

³ e.g. TRIPOD DELTA [14] or HFACS [15]

2.2. Complex Systems’ Safety Modelling Characteristics

In her work Leveson confirmed that models originating from the end of the 20th century did not reflect the complexity of accidents well enough [20]. This is very much so when they deal with systemic factors such as: limits in the organisational structure, inefficient management or limited safety culture of the company or the industry in general. Enhancing common sequential models is not enough and calls for the improvements have been made. In order to do that it would be of an utmost importance to understand how the system, with all relevant organisational and societal components, induces accidents (e.g. Figure 3.).

In addition to this Leveson makes a point about how, in systems managed by human as well as computer software, errors do not occur separately. They are even more affected by the management or flaws in safety culture that have not been taken into account in classical (i.e. existing) models. In cases where models have taken them into account, the effect was generally from experience or even random. Roelen [6] agrees and adds to that how the value of probability of the occurrence that works for technical components cannot be the same if a human component has been present in the event. Finally, reflecting on “The Event Analysis of Systemic Teamwork (EAST)” model characteristics, Griffin [7] concludes that new models should address the system in its entirety not as the sum of isolated events or participants [22].

The authors are in agreement that accident modelling should encourage a holistic view on accident causation even before the mishap. There are more than 22 threat assessing models and software packages as per FAA [23]. Focusing on operators, physical components failures or weak elements in technological procedures can potentially cause missing some of the vital factors in future accident prevention.

2.3. Some of the Desired Features of the Future Models as per Literature Review

Following the discussion about the nature and considerations, to be taken into account when analysing and modelling accidents the author will present critical desired features of the contemporary, and advanced, risk models.

According to Griffin future models should enable the study of the systems’ behaviour as a whole in both normal and out of normal state to be able to study their performance indicators. They should be based not only on linear dependency of the elements, but take into account other types of

3. CONCLUSION

A number of different literatures have been assessed here for their relations to previous and current practices to risk modelling and proactive safety management. This has been followed by the account of risk assessment model characteristics identified to be desired for contemporary and future models in relevant literature.

What this review suggests is that a modified approach to managing safety in aviation has been combined with enabling technological and organisational changes and formalised in an approach to cater for the nature of recent complex systems.

The formal requirement for data collection and analysis due to the nature of the operations and the interest of society has resulted in improving the level of safety in the aviation system. What this review further suggests is that the body of literature available for aviation could be applied to other HRO having in mind the advancement of formal research and regulatory initiatives in aviation domain itself.

4. REFERENCES

- [1] Lewis, C., Christopher, L.: A Brief Overview of Safety Management Systems (SMS), Flight Safety Information Journal, January 2008.
- [2] Aircraft Accident and Incident Investigation, Annex 13 to the Convention on International Civil Aviation, ICAO, Montreal, July 2010.
- [3] Wiener, E, L., Kanki, Barbara G., Helmreich, Robert L.: Cockpit Resource Management, Academic Press, San Diego, USA, 1993.
- [4] Safety Management Manual (SMM), (Doc 9859). International Civil Aviation Organisation, Second Edition, Montreal, 2009.
- [5] Reason, J.: Managing The Risk of Organizational Accidents, Ashgate Publishing Company, Burlington, USA, 1998.
- [6] Roelen, A.: Causal risk models of air transport, Comparison of user needs and model capabilities. PhD Thesis, Technische Universiteit Delft, The Netherlands, 10. November 2008., p. 21.-22.
- [7] Griffin, T.G.C.: The Flight of Information: New Approaches for Investigating Aviation Accident Causation. PhD Thesis, School of Engineering and Design, Brunel University, May 2010.
- [8] Netjasov, F., Janić, M.: A Review of the Research on Risk and Safety Modelling in Civil Aviation. Third International Conference on Research in Air Transportation, Fairfax, VA, Canada, 1. June 2008., p. 169.-176.
- [9] Weaver, D.: Symptoms of Operational Error. Professional Safety, Vol. 104, No. 2, October 1971., p.39-42.
- [10] Bird, F.E., Loftus, R.G.: Loss Control Management. Institute Press, Loganville, Georgia, USA, 1976.
- [11] Adams, E.: Accident Causation and the Management Systems. Professional Safety, October 1976., p.26-29.
- [12] Johnson, W.G.: MORT: The management oversight and risk tree. Journal of Safety Research, Vol. 7, No. 1, 1975., p.4-15.
- [13] Rasmussen, J.: Risk management in a dynamic society: a modelling problem. Safety Science, Vol. 27, No. 2-3, 1997., p.183-213.
- [14] Groeneweg, J., Roggeveen, V.: Tripod: Controlling the human error components in accidents. Safety and Reliability, Proceedings of the ESREL 2003 Conference, 1998., p.809-816.
- [15] Shappell, S.A., Wiegmann, D.A.: Applying Reason: The human factors analysis and classification system (HFACS). Human Factors and Aerospace Safety, Vol. 1, No. 1, 2001., p.59-86.
- [16] Perrow, C.: Normal Accidents: Living with High-risk Technologies. Princeton University Press, 1999.
- [17] Rijkman, J. A.: Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory. Journal of Contingencies and Crisis Management, Vol. 5, No. 1, March 1997., p.15-45.
- [18] Hollnagel, E., et al.: Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd., 2006.
- [19] Safety Management, Annex 19 to the Convention on International Civil Aviation, ICAO, Montreal, July 2013.
- [20] Leveson, N.: Engineering a Safer World. MIT, Aeronautics and Astronautics, Cambridge, MA, SAD, 2011.
- [21] Leveson, N, et al.: Risk Analysis of NASA Independent Technical Authority, MIT, Cambridge, MA, SAD, 2005.
- [22] Stanton, N.A., et. al.: Modelling Command and Control. Aldershot, UK, 2008.
- [23] Safety Management Systems for Airports. Volume 2: Guidebook. Transportation Research Board, Washington, DC, USA, 2009.
- [24] Stoop, J., Dekker, S.: Limitations of 'Swiss Cheese' Models And the Need for a Systems Approach., ISASI 2009., Proceedings, p. 52.-59