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 systems 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 effect. 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 20\textsuperscript{th} century, the number of accidents has been reduced. Average time between them has increased to one in 100,000 flight hours [3].

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 17\textsuperscript{th} 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 19\textsuperscript{th} and early in 20\textsuperscript{th} 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 Jani\’ć 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 Jani\’ć 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 others 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]

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 e.g. TRIPOD DELTA [14] or HFACS [15]
dependencies such as feedback between model elements. Different model levels connected either directly or indirectly should be able to influence and exchange feedback between each other.

Problem analysis through systemic approach advocated by Rasmussen made Leveson conclude that understanding the intention, purpose and the decision for system design is crucial for successful accident prevention. Focusing on operator’s actions, system failures or technological flaws could lead to serious omissions in capturing some of most influential future accidents’ prevention factors. Risk modelling should address more than the accident mechanism only for more comprehensive investigation practice.

Fig. 3. Simplified Model of the Dynamics Behind the Shuttle Columbia Loss [21, p.100]

Generally applicable and widely applied two dimensional matrix risk assessment (Figure 4.) reduces the flexibility of the model and future improvements. Griffin agrees with Roelen related to more objective risk assessment when stating that SMS models for Safety Risk Assessment should influence the most important safety risks in the system. The probability of failures at “sharp end” and organisation structure at higher levels are interconnected. A stable state, input and output variables together with their functional relationship are crucial for assessing the level of management’s influence on risk. Finally, impartial risk assessment following modifications to system (either due to new technology or regulations) caters for more general application of new models.

<table>
<thead>
<tr>
<th>Risk probability</th>
<th>Risk severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic A</td>
<td>Hazardous B</td>
</tr>
<tr>
<td>Major C</td>
<td>Minor D</td>
</tr>
<tr>
<td>Negligible E</td>
<td></td>
</tr>
<tr>
<td>Frequent 5</td>
<td>5A 5B 5C 5D 5E</td>
</tr>
<tr>
<td>Occasional 4</td>
<td>4A 4B 4C 4D 4E</td>
</tr>
<tr>
<td>Remote 3</td>
<td>3A 3B 3C 3D 3E</td>
</tr>
<tr>
<td>Improbable 2</td>
<td>2A 2B 2C 2D 2E</td>
</tr>
<tr>
<td>Extremely improbable 1</td>
<td>1A 1B 1C 1D 2E</td>
</tr>
</tbody>
</table>

Netjasov and Janić state that the complexity of models that can cater for characteristics mentioned above require a modular approach that would simplify the process. Simplification is the reason for having models that can be used by general users. Replication of the calculation and results validation are next in line of the desired characteristics of the models. The representation of complex systems by models inadvertently results in their complexity and lengthy calculation process. Identified by Roelen that positions the usability of the model over the complexity of the same.

Fig. 4. ICAO Two Dimensional Risk Matrix [4]

According to Griffin the very exact and unforgiving nature of aviation as an industry drives requirements for replication of results and knowledge transfer from model designers to their users. They vary from “sharp end” operators across management and regulators to academia. As Stoop [24] states, different users require different information to be able to identify systemic challenges. Operators need information for safe operations. Management and regulators need indications and means for safety system design. Finally academia seek to understand system’s nature and the effect of suggested modifications or the need for different ones. Finally as Netjasov and Janić state, the effective and transparent use of module results would be possible only if their output is presented by units that can be validated objectively [8].
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