Journal of Transportation Security
https://doi.org/10.1007/s12198-020-00209-z

Linking aviation security failures to human-mediated error. A review of the related literatures with directions for policy and research

Paul McFarlane[1]

Received: 8 June 2019 / Accepted: 26 April 2020/Published online: 15 May 2020

Abstract

Given the continued growth of air traffic demand and the importance of preventing aviation security failures in this increasingly complex system, this paper offers a review of the relevant literatures relating to the linkages between aviation security failures and human-mediated error. It argues that academics, security professionals and policymakers have given very little consideration to the complexity of these linkages; understanding how human errors can create hidden modes of failure that can be exploited by terrorists and other threat groups. This paper discusses how the literatures in other related fields can be used to explain how human-mediated errors are created and incubated, and how these error types can evolve to become system vulnerabilities and exploitable modes of aviation security failure. The paper concludes by identifying a significant gap in the current theoretical discourse. Implications for actionable policy and research recommendations include taking a fresh approach to proactively mitigating risk; implementing an over-arching risk management strategy which includes analysing data relating to aviation security failures and developing predictive models to detect abnormal and sub-optimal security performance.

Keywords Aviation security · Human error · System failure · Literature review

Introduction

Important to both practice and theory—"approximately $50 billion […] is spent annually world-wide in the quest to deter or disrupt terrorist attacks to aviation" (Stewart and Mueller 2018). Nevertheless, the aviation industry has given very little consideration to the complexity of the linkages between aviation security failures and

✉ Paul McFarlane
p.mcfarlane@ucl.ac.uk

[1] Jill Dando Institute of Security and Crime Science, University College London, London, UK

human-mediated errors, and to understanding how these same connections can increase the risk of creating hidden modes of failure (i.e., opaque pathways through all of the security system layers) that can be exploited by terrorists and other threat groups (McFarlane 2017). Recognising this risk is essential because human error is now widely recognised as being causal to the creation of modes of failures in other—similar—types of systems (cf. Reason 1990, 2008). However, the extent to which failures in aviation security are related to human error, is not fully understood, because it has not yet been attributed an appropriate level of significance by researchers, security professionals and policymakers (McFarlane 2017).

There are, however, some studies which have considered these linkages more broadly (cf. McFadden and Towell 1999; Weigmann and Shappell 2001a, b; Liang et al. 2010; Chiu 2016 for discussions about human factors in aviation accidents, aviation safety and aviation maintenance failures). There are also a limited amount of studies which make more specific connections, for example, the effect of human error and organisational factors in transportation security screening processes and inspection systems (cf. Kraemer et al. 2009; Arcúrio et al. 2018). Given this current situation, this paper reviews the condition of the relevant academic and professional literatures relating specifically to aviation security and human error. It discusses how the literatures in other related fields can be used to explain how human-mediated errors are created and incubated, and how these errors may evolve to become hidden system vulnerabilities and exploitable modes of aviation security failure.

This review is organised into four further sections. The first section introduces the concept of human-mediated errors and connects aviation security to the broader field of socio-technical system failures; arguing the current system is not effectively optimised and continues to operate in a weakened state. By concentrating upon the vital work of Reason (1990), the second section, uses the established theoretical paradigm of human error to explain how human-mediated errors and modes of failure could be created in the aviation security system. The third section turns to explain how these errors incubate and remain concealed within the layers and vagaries of the system. Finally, the paper concludes by identifying a significant gap in the current theoretical discourse connecting failures in aviation security with human-mediated errors and recommends directions for further research and policy change in this area to mitigate the risk of future security failures.

Broadening socio-technical system theory to aviation security

On the 11th September 2001 (henceforth 9/11), the global commercial aviation security system failed. In their deliberate exploitation of one of the most highly defended security systems, al-Qaeda operatives "defeated all the security layers that America's civil aviation security system then had in place to prevent a hijacking" (National Commission on Terrorist Attacks upon the United States 2004 p. 4). In overcoming these security layers, the terrorists exploited and revealed for the first time, a multitude of unimagined modes of system failure. Although at the time they were unanticipated—to Reason (1990, 2008), a leading expert in the theory of human error and system failures, these modes were not something new; they were in fact a series of unforeseen error paths that were able to permeate through all of the layers relied upon to defend the system.

These unforeseen error paths are a combination of two specific types of human-mediated errors, which occur within socio-technical systems such as aviation security: active and latent (Reason 1990). Active human-mediated errors are those which have immediate consequences upon the operation of the system and are usually made by front-line workers. For instance (as was the case on 9/11), where security operators at airport passenger screening checkpoints do not comply with or deliberately violate operating procedures and processes. On the other hand, the effect of (hidden) latent errors is not so apparent to the system; they are concealed within complex interactions relating to high-level decision-making processes, poor system design, ineffective training programmes and inadequate supervision of personnel.

In the last sixty-five years, researchers (e.g., Trist and Bamforth 1951; Cherns 1976; Mumford 2006; Baxter and Sommerville 2011; Grant et al. 2011; Davis et al. 2014) have identified many successful examples of socio-technical theories being used in different types of operational settings to understand the complex interactions between system elements. Other literatures which report on these socio-technical systems and their failures (e.g., Turner 1976, 1978; Rasmussen 1982; Reason 1990, 2008; Redmill and Rajan 1997; Turner and Pidgeon 1997; Perrow 1984, 1994, 1999, 2007) are useful, and can also be used by security practitioners and researchers to: (1) identify linkages between system failures and human error, (2) explain how human-mediated errors are created, incubated and exploited, and (3) understand how others have conceptualised human errors being causal to creating exploitable modes of system failure.

In essence, a socio-technical approach is "about taking a holistic view" (Peltu et al. 2008 p. 21; Davis et al. 2014). It's about configuring systems in such a way that the component (human, technical and organisational) parts all work together (Mumford 2006); avoiding decision-making that impedes performance by placing emphasis on one part of the system, to the exclusion of another (Baxter and Sommerville 2011). In the case of aviation security, socio-technical theory can be used to explore the propostion that the current system is not configured very well; imbalanced by an emphasis placed on automated technological defences (e.g., x-ray machines, full body scanners and explosive detection devices). When viewed holistically, this reliance upon these complex technological solutions creates system asymmetry, which can impact on the long-term efficacy of the security system to detect or deter threats (Hofer and Wetter 2012).

The literatures relating to socio-technical systems theory surface an important issue for aviation security. Unless the wider industry embraces the socio-technical principle of joint optimisation, the system is at risk of operating in a weakened state; vulnerable to further exploitation. There have been many studies which, in isolation, have considered the individual performance of aviation security technologies (e.g., back-scatter and millimetre body scanners; automatic liquid explosive detection systems; high resolution imaging) used to defend the system (cf. Federici et al. 2005; Miles et al. 2007; Leo and Lawler 2007; Vogel and Haller 2007; Klitou 2008; Song et al. 2009; Frimpong 2011; Mitchener-Nissen et al. 2011; Orouji et al. 2011; Schauer 2011). Nonetheless, there remains a lack of research which evaluates the impact of how these technologies are optimised to interact and work together with other elements of the system. Add to that, policymakers should also consider that security at airports which is "based solely on technology is nearing its limits in thwarting the various physical threats to aviation" (Kirschenbaum et al. 2012a p. 374).

The human element: the creation of human-mediated errors

In socio-technical systems like aviation security, the human element has autonomy for decisions relating to the design, operation, management and maintenance. The human part of the system is also responsible for making mistakes (Weigmann and Shappell 2001a, b) that create modes of failure, exploitable errors and vulnerabilities. With this being the case, the established theoretical paradigm of human error can be used to understand how human-mediated errors can be causal to system failures. Reason (1987, 1990, 1997, 2000, 2008) has significantly contributed to the development of the widely accepted and frequently cited taxonomy of human error, which includes the Generic Error Modelling System, Swiss Cheese Model and Organisational Accident Model.

Despite some criticism which suggests that Reason's propositions are based upon empirical data lacking in strength (Gray et al. 1993), his theory, nevertheless, remains most authoritative in its explanation and description of human error, and provides an appropriate theoretical framework for the conceptual analysis and discussion of human-mediated errors in socio-technical systems.

According to Reason (1990, 2008), there is still no unified definition of human error, however, it is accepted by most that human error involves "some form of [unintentional or deliberate] deviation" (Reason 2008 p. 29) from what is perceived to be the correct path or course of action. In one of his many publications, Reason examines this idea of deviation from a cognitive psychologist's perspective and presents a set of definitions of the concepts and types of error which can be found in socio-technical and other types of organisational systems such as aviation security. To structure his taxonomy, he provides a working definition of human error as being:

> "Those occasions in which a planned sequence of mental or physical activities fails to achieve its intended outcome, and when these failures cannot be attributed to the intervention of some chance agency" (Reason 1990 p. 9).

Building upon this, and based upon Rasmussen's (1983) skill-rule and knowledge-based performance framework, Reason (1990 p. 53) specifies three different types of human error you can expect to see in a system: (i) skill-based slips and lapses; (ii) rule-based mistakes; and (iii) knowledge-based mistakes. In his conceptual framework of the Generic Error Modelling System (GEMS), he also distinguishes slips and lapses that can result from a:

> "Failure in the execution [...] of an action sequence, regardless of whether or not the plan which was guided them was adequate to achieve it's intended objective'—and mistakes that are' deficiencies or failures in the judgmental and/or inferential processes involved in the selection of an objective or in the specification of the means to achieve it" (Reason 1990 p. 9).

At first blush, it is clear to see how these three types of cognitive-based errors can be present in all forms of socio-technical systems. In real-world systems such as aviation security, there are many opportunities, at all levels of the system, for the development

of slips, lapses and mistakes. Slips and lapses can be thought of as those errors committed by human operators performing one of the many functions required for the system to reliably operate. Mistakes, on the other hand, are those that relate to the design of the system (i.e., operating rules and procedures), and those that are made in relation to defining the objective of the system (i.e., what it was set up to do). That is why, therefore, slips and lapses are more easily detected by the system and— mistakes, on the other hand, are more challenging to recognise and not so apparent to the system operator or producer of the error.

Unsafe acts: errors and deliberate violations

Unsafe acts provides a further level of categorisation to distinguish between: (i) errors which occur at an individual level; and (ii) violations which are required to be considered in a broader social context in which human performance, and performance of the system, is described by its relationship with the other elements and operating processes (Reason 1990 p. 195). In this case, errors (slips, lapses and mistakes) only part-fill the framework for abnormal behaviour because they are unintentional in their commission. By contrast, violations are:

> "Deliberate—but not necessarily reprehensible—deviations from those practices deemed necessary (by designers, managers and regulatory agencies) to maintain the safe operation of a … system" (Reason 1990 p. 195).

Violations are causal to system failure. Dependent upon the level of intent, violations can be further classified as being either: (i) routine, or (ii) exceptional. Although action, by its very name, is intended, the adverse outcome is not necessarily foreseen as a consequence at the time of the violation (Reason et al. 1998; Reason 2008). In the literature, there are many examples from other systems of the catastrophic effect of deviations from safe operating procedures. For instance, the study by Vaughan (1997) into the explosion of the Challenger space shuttle in 1986, illustrates the effect of internal rule-based violations and deviations that, after their occurrence, became normalised (i.e., unwittingly concealed and embedded) into the routine operation and performance of the system.

Active and latent errors

There is an agreement in the literature that Reason's (1990) theory and taxonomy can also be applied to explain how human-mediated modes of failure come to exist in the protective layers of socio-technical systems. Reason (1990 p. 173) explains these failures are a consequence of the random combination of active and latent errors. In contrast to latent errors, the malign effect of active errors (or unsafe acts) on system operation is almost immediate and are those associated with the front-end human operators (think airport security employees) who are at the interface between system processes and technologies. Interventions which are designed solely to reduce the occurrence of active errors will be limited in terms of what they can do to improve the overall reliability of the system because:

> "Rather than being the main instigators of an accident, [human] operators tend to be the inheritors of the system defects created by poor design, incorrect installation, faulty maintenance and bad management decisions. Their part is usually that of adding the final garnish to a lethal brew whose ingredients have already been long in the cooking" (Reason 1990 p. 173).

Kirschenbaum et al. (2012a, b, c), Kirschenbaum and Mariani (2012), Hofer and Wetter (2012) and Arcúrio et al. (2018) have published the first serious discussions of what the 'final garnish' might look like in aviation security operations. Kirschenbaum et al. (2012a) collected data, by making over 250 ethnographic observations, at many airports across Europe. The airport environment was selected because it is optimised towards determining whether decisions made about security comply with mandated rules and procedures. Their study encapsulated all aspects of airport security, including land-side, airside, shopping and cargo areas, and hypothesised that "the behaviour of employees dealing with security in airports is generally assumed to reflect the constraints imposed by the rules and procedures in place" (Kirschenbaum et al. 2012a p. 72). Concurring with Reason's general classification of unsafe acts, many of Kirschenbaum et al's observations provide direct evidence of deliberate rule-breaking (unsafe acts) and malevolent behaviour by security screeners during what appears to be routine but, because of human and social factors, are in fact complex situations. Importantly, the researchers observed many events where security screeners consciously made decisions to knowingly allow prohibited items to enter the airside of the airport (Kirschenbaum and Mariani 2012).

More recently, Arcúrio et al. (2018) conducted a similar study in eighteen Brazilian airports. They questioned 602 aviation security professionals to explore the cognitive processes and perceptions related to their actions and decision-making while working in the security screening process. Similar to findings reported by Liang et al. (2010), their study analyses the frequency and effect of human errors related to key factors such as repetition, complacency and not following work procedures. In this case, security processionals with more experience made more errors relating to being complacent and not following correct work procedures. Rather than complying with regulatory procedures, participants' experience was often used to make decisions while working at the security checkpoint (ibid.). These studies are important because the extent to which aviation security professionals—after 9/11—are still willing to break the rules should be a concern for aviation security industry and policymakers. Add to that, with the increasing reliance on more sophisticated technologies, a lack of operational testing and severe propensity for security employees to bend and break the rules, security systems at airports can be reasonably described as being a habitat ripe for the creation and mutation of system vulnerabilities.

Rules and regulations: an Achilles heel

The studies completed by Kirschenbaum et al. (2012a, b, c), Hofer and Wetter (2012) and Arcúrio et al. (2018) provide an additional and significant contribution to the literatures associated with aviation security. They offer the first real data and empirical analysis of the effect of regulations and procedures, which support and provide the structural framework for the efficient operation of aviation security systems. In a very

similar way, the conceptual analysis of security by Lennerman (2012) identifies that it is the rules and regulations that determine how the whole system will function, spanning the macro (national regulations) through to the micro (local procedures for the system operation). When examined through the lens of Reason, Kirschenbaum et al. and Arcúrio et al. these rules and regulations, rather than being considered by policymakers as the central support of the system, should be recognised as being an Achilles' heel—significantly crucial in contributing to the creation of human-mediated errors and exploitable system vulnerabilities.

This point is significant because the global aviation security system is built upon a framework that is held together by a multitude of complex and politically derived rules, regulations and operating procedures determining how the system should function. Feakin (2011), in a report for the Royal United Services Institute, critically analyses this point. In his study he argues convincingly and contends that the response to terrorist attacks on civil aviation has become a retrospective and politically-driven process, the roots of which can be traced back to 1947, with the formation of the International Civil Aviation Organisation (ICAO) after the Chicago Convention in 1944 (International Civil Aviation Organisation 2011).

ICAO is a policymaking entity that directs member nations to incorporate international Standards and Recommended Practices (SARPS) into their security operating procedures (Sweet 2003, 2009). SARPS for international aviation security were developed by ICAO in 1974 and are designated as Annex 17 to the Chicago Convention. Annex 17 is specific to international aviation security and has the primary objective of ensuring the safety and security of passengers, crew, ground personnel and the general public in all matters related to acts of unlawful interference with civil aviation. In terms of compliance, however, Annex 17 is analogous to that of a 'toothless tiger' because it does not provide a mandate to prosecute or otherwise sanction states that violate security recommendations.

Annex 17, and all the other regulations are operationally realised in the form of compulsive rules, regulations and procedures that are applied to control some (and prohibit other) human actions within the system (Reason 2008). Paradoxically, this itself creates another risk. If Annex 17 rules were to be perceived by the system to create an over-specification of permitted actions, then, this itself may generate "the conditions [...] necessary [...] [for further] violations" (Reason 2008 p. 53) [emphasis added]—given that there is consensus in the literature that the over-specification of regulatory restriction can create situations where the only option is to violate rules.

In systems analogous to aviation security, this specific risk has been known for some time. In earlier research, the limitations of this type of regulatory control in socio-technical systems were identified by Waring, who argues that "no organisation can really hope to manage its [... security] successfully by sole reference [...] to what [regulators] say or do" (1996 p. 28) [emphasis added). This is because, although rules and regulations are a useful:

> "[T]ool to attempt to get people to behave in a responsible way, unless ways are found to create a culture in which 'regulations' are readily accepted it is doubtful they will ever be effective as is intended" (Toft and Reynolds 2005 p. 83).

Latent errors and the resident pathogen metaphor

Latent conditions "pose the greatest threat to the safety of a complex system" (Reason 1990 p. 173) because they remain hidden and dormant. In contrast to active errors, latent error conditions are the consequence of actions of those "removed both in time and space" from the front-end of the system such as the "designers, high level decision makers, construction workers, managers and maintenance personnel" (Reason 1990 p. 173). The unforeseen and dormant status of latent errors is conceptually similar to "resident pathogen[s]" in a human body (Reason 1990 p. 197–198). The metaphor explains that some latent conditions will always exist within each socio-technical system, and it will be these conditions that generate unsafe acts and the final garnish to undermine the defence of the system. Analogous to real life pathogens:

> "Latent conditions—such as poor design, gaps in supervision, undetected manufacturing defects or maintenance failures, unworkable procedures, clumsy automation, shortfalls in training [...] may be present for many years before they combine with local circumstances and active failures to penetrate the system's many layers of defences. They arise from strategic and other top-level decisions made by governments, regulators, manufacturers, designers and organisational. […] Latent conditions [...] are spawned in the upper echelons of the organisation and within related manufacturing, contracting, regulatory and governmental agencies [... they] can increase the likelihood of active failures through the creation of local factors promoting errors and violations. They can also aggravate the consequences of unsafe acts by their effects upon the system's defences, barriers and safeguards" (Reason 1997 p. 11).

The incubation of human-mediated errors in socio-technical systems

Having established how active errors and latent conditions may be created in socio-technical systems, this section now considers how these same error types can incubate and conceal themselves and why they only become visible—in hindsight—after they are exploited. There have been many recent examples of errors remaining concealed in systems such as 9/11; American Airlines flight 63: Richard Reid – 'The Shoe Bomber', 2001; Bojinka II: 'Operation Overt', The Liquid Bomb Plot, 2006; Northwest Airlines flight 253: Umar Farouk Abdulmutallab – 'The Underpants Bomber', 2009; Operation Hemorrhage: 'The Printer Cartridge Plot', 2010; 'Yemen Plane Bomb Plot', 2012; and Metrojet flight 9268: 'Egypt Plane Crash', 2015. The literatures relating to man-made disaster theory can be used to understand why errors incubate and become concealed within socio-technical systems, and why they only become visible to systems in hindsight after they are exploited. In every practical and theoretical sense aviation security failures can be thought of as (hu)man-made disasters.

A considerable amount of interdisciplinary research has been published on human-made disasters or, as they are now more often referred to, as socio-technical disasters. The majority of the literature provides both rich and useful ex-post descriptions of

disaster aetiology. However, a similar problem to that explored in the previous section exists, where it is only in other fields that there has been an increasing amount of research which examines how human-mediated errors have contributed to large-scale failures in socio-technical systems. Take, for example, the cases of; Three Mile Island (1979), Bhopal (1984), Chernobyl (1986), Piper Alpha (1988), Challenger Space Shuttle (1986), Herald of Free Enterprise (1987), Kings Cross Underground Fire (1987), Clapham Junction (1988), Kegworth M1 Air Crash (1989) and the BP Deep-water Horizon Explosion (2010). In a very similar way to socio-technical system theory, there is also no reason why disaster theories cannot be applied to the analysis of aviation security failures like those mentioned above.

Socio-technical disaster models

The first serious discussions and analyses of socio-technical disasters emerged in the late 1970s with the publication of an original text by the late Barry Turner. Turner's work (1976, 1978) introduced the idea of an 'incubation' period—a stage in the timeline of a system where the conjunction of human-mediated errors goes unnoticed by it. This concept has now been adopted and extended by other scholars (cf. Fink 1986; Shrivastava et al. 1988; Silverstein 1992; Toft and Reynolds 1999; 2005; Ibrahim et al. 2002; Aini and Fakhru'l-Razi 2009, 2010) as a necessary and contributory pre-condition (Blockley 1998; Aini and Fakhru'l-Razi 2010) to all socio-technical disasters. For instance, Turner's (1976) model of unfolding disasters describes the incubation period as the second of six sequential phases, which include the:

1 normal stage;
2 incubation period;
3 precipitating event;
4 onset;
5 rescue and salvage; and.
6 cultural adjustment.

Socio-technical disaster theory can be synthesised into a collection of linear models with a series of sequential stages (Aini and Fakhru'l-Razi 2009). There is agreement that the length of the incubation period is important in (i) creating the conditions necessary to conceal errors in system (Grawbowski and Robert 1997), and (ii) in determining the impact of the event on the system and surrounding environment. For instance, in their research, Ibrahim et al. (2002) observed that in some cases, latent conditions and errors had remained undetected in socio-technical systems for up to thirty years. The length of this period was related in some way to the number of human casualties and damage to property that occurred at the onset of the disaster (i.e., the longer the errors had remained concealed was significant in the overall impact of the disaster).

Ibrahim et al. (2002) concur with Reason's theory that it is during the design stage that the system will generate operational, organisational and technical errors, and because of various organisational factors these errors will eventually aggregate and incubate within the system. What is also important is that at some point during the incubation period, the active and latent errors will combine and emit a series of warnings and signals (in the form of near misses, accidents and incidents) of the system being in a bad state. Also, if not

identified and mitigated against, these errors will morph the system towards a critical condition. In this condition, any further unsafe acts not mediated by system defences will trigger the onset of a full disaster (Ibrahim et al. 2002).

A sociological perspective of system failure

Equally, Ibrahim et al's. proposition that socio-technical systems will—in advance—provide warning of its drift towards an unsafe condition is a significant contribution and is also key to how we should, in the future, think, about failures in aviation security. Comprehending why warning signs and signals are not visible in foresight is critical to the development of conceptual interventions to mitigate or prevent the triggering of a system failure. From a sociological perspective, Turner and Pidgeon (1997) provide some understanding as to why it may be challenging to develop anticipatory interventions; explaining this relates to a disparity between how the world is believed to operate and how it actually does. Believing that the world operates in a way that is separated from reality allows for the aggregation of what Turner (1978) describes as 'discrepant events' (i.e., latent conditions)—to go unnoticed.

As far as the literature is concerned, and indeed as far as this review is concerned, Turner (1978) is again helpful and categorises the reasons why warning signals that relate to discrepant events remain concealed and are only visible after they system fails. He plots them into four broad groups:

1 unnoticed or misunderstood because of erroneous assumptions;
2 unnoticed or misunderstood because of difficulties in handling information in complex situations;
3 effective violations of precautions passing unnoticed because of cultural lag in existing precautions; and.
4 unnoticed or misunderstood because of a reluctance to fear the worst outcome (ibid..).

In each case, information relating to the presence of discrepant events already exists within the system, and it is just the case that the implications of the information are often not fully appreciated or understood as needing to be acted upon (ibid..). To overcome this problem, Pidgeon and O'Leary (2000 p. 22) suggest there needs to be an element of "safety imagination" to "at least consider the possibility of [discrepant events] … that have not been thought of in advance." This approach seeks to overcome the obstacles described by Turner, by interrupting or temporarily moving beyond pre-conceived cultural and institutional assumptions, and perceptions of risk events and hazards that will compromise the capability of the system to defend itself against threats.

Pidgeon and O'Leary's Bayesian type of approach (i.e., continually updating the probability of an event as more information becomes available) towards the identification of risk events and hazards does appear to have some merit and applicability to commercial aviation transportation security. In its report on 9/11, the National Commission on Terrorist Attacks upon the United States (2004) identified that a failure in imagination by the United States government and intelligence agencies was significant to the success of the attack. Also, commensurate with Turner's views, the security system at that time was constructed neither to hypothesise nor consider the probability that Islamist terrorists would crash civilian airliners into buildings, and the "warning

system [therefore] was not looking for [this] information [...] because the system was not tuned to comprehend […] [it's] potential significance" (ibid. p. 149) [emphasis added]. Had the system, through imagination, considered that the probability of such an attack was more (or even) likely, it could have correctly interpreted many of the warnings, including in August 2001, when Zacarias Moussaoui was arrested whilst learning to fly at a Minnesota flight school (ibid..) in preparation for the 9/11 attacks.

Since Turner's work on man-made disasters, the problem of warnings not being interpreted correctly, nor understood when the relevant information is available in the system, has been discussed further in the literatures. For instance, and comparable in many ways to the events of 9/11, Silver (2012) in his analysis of the attack on Pearl Harbor in 1941 identified that—in hindsight—many signals were indicating the possibility of an attack. Nevertheless—in foresight—it was a complete surprise to the military and intelligence agencies when the attack occurred. Wohlstetter writing on the events of Pearl Harbour explains that:

> "It is much easier after the event to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear; we can now see what disaster it was signalling since the disaster has occurred. However, before the event, it is obscure and pregnant with conflicting meanings. It comes to the observer embedded in an atmosphere of 'noise', i.e., in the company of all sorts of information that is useless and irrelevant for predicting the particular disaster" (1962 p. 1–2).

In this case, a signal is "an indication of the underlying truth" and noise is "random patterns that might easily be mistaken for signals" (Silver 2012 p. 416–417). Therefore, it is only post-event when the signal will be visible amongst the competing noise and fit complementarily into the event aetiology. The challenges for aviation security to correctly interpret warning signals from amongst noise is similar in comparison to the difficulty explained by Turner of socio-technical systems identifying discrepant events hidden amongst the formed beliefs held by the system. On this point, Thomas Schelling has argued that:

> "There is a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously" (cited in Wohlstetter 1962 p.vii).

There is little controversy about the importance (and difficulty) of imagining the likelihood of what is perceived to be improbable and finding "a way of routinising, even bureaucratizing, the exercise of imagination" (National Commission on Terrorist Attacks upon the United States 2004 p. 344). Nevertheless, academics and security practitioners should start to think of new ways to provide some form of foresight of the system, beginning to fail and breakdown.

Incubation and normalisation of latent conditions and errors

As introduced earlier, the literatures provide excellent real-world examples of how socio-technical systems can incubate latent conditions and move the

system towards a dangerous condition. Vaughan's (1997) study of the 1986 Challenger space shuttle disaster illustrates how operational managers deliberately violated their own safety rules and procedures to meet the unrelenting demand of production pressures and flight schedules. In this example, the assessment to launch the shuttle was fundamentally flawed. The decision makers were not aware of the real risk of failure of O-ring joints on the solid rocket booster. The real information relating to their ineffective seal had been incubated and concealed (over an extended time period) by the complex system and organisational processes, i.e., the positive feedback loop had moved the system away from a safe operating state to a dangerous condition. Although, Reason's Generic Error Modelling taxonomy would suggest that, in this case, there were intentional and routine violations of safety rules and procedures, Vaughan prefers an alternative theoretical perspective to explain that complex sociological influences that exist within socio-technical systems can 'normalise' deviant behaviour to the point where it is deemed acceptable (Vaughan 1997).

Vaughan (1997) argues that the ineffective seal on the O-ring joint was a potential latent incubating failure. Over the years before the disaster the system exhibited warnings of potential failure many times previously during the ignition cycle of the space shuttle. Despite this being known by system engineers and managers, the successful completion of previous launches and missions using the faulty O-ring influenced their perception of the risk, convincing them in some way that using the faulty O-ring seal was acceptable and that the shuttle was safe for flight. The first decision set a precedent; it became the normative standard for all future decisions relating to the continued use of the O-ring seal. This decision-making sequence, and the subsequent successful missions, had the outcome of "normalis[ing]" the rule violations relating to the use of the O-ring seal and contributed to the construction of a belief that it was an acceptable risk (Vaughan 1997 p. 112)—rather than acknowledging it as a fatal system error. In this case, normalisation had the consequence of morphing active errors to become deeply embedded latent conditions.

Layered security: defence in depth

Aviation security is a highly defended system. Similar to other hazardous industries, such as the mining industry, the Transportation Security Administration (TSA) has applied the philosophy of defence in depth using a multiplicity of layers and barriers to mitigate the initiation and escalation of adverse events (Saleh and Cummings 2011; Sorensen et al. 1999). The layering of protective measures is now an orthodox condition. The combination of multiple security layers, such as that found in the current TSA system, ranges from covertly using intelligence to profile risk through to passengers on the aircraft being the last line of defence and creates a fortified system with higher levels of security (Rekiel and de Wit 2013).

Despite there being some clear benefits of systems adopting defence-in-depth, Rasmussen (1988) and Rasmussen and Vicente (1989) are, to some extent, critical, and warn that the various layers of the system defences, in fact, create what Rasmussen aptly describes as:

> "The fallacy of defence in depth [...] where several independent events have to coincide before the system responds by visible changes in behaviour. Violation of safety pre-conditions during work on the system will probably not result in an immediate functional response, and latent effects of erroneous acts can therefore be left in the system. When such errors are allowed to be present over a longer period of time, the probability of coincidence of multiple faults necessary for the release of an accident is drastically increased" (1988 p. 3–4) [emphasis added].

Theoretically, the redundancy provided by defence-in-depth should ensure that critical security functions are unaffected by faults that occur in individual system elements. However, the very same procedures and work activities can reduce the sensitivity of the system to identify the accumulation of latent conditions (Rasmussen and Vicente 1989). The resultant effect of this fallacy, therefore, creates opacity, and those responsible for the management, operation and maintenance of the system may not, in the first instance, be able to identify, let alone resolve, any erroneous conditions (Reason 1990) that exist before a system failure. Rather than Turner's theoretical explanation, the fallacy of defence-in-depth provides a more practical explanation for aviation security, as to why warnings associated with the conjunction of latent conditions and errors remain hidden and go unnoticed during the incubation period.

The 'Swiss Cheese' metaphor

Being similar in many ways to the real-world TSA layers of aviation security, Reason (1997) also talks about the relationship between latent conditions and active errors using his Swiss Cheese model. As a general rule, the model helps to explain that the precise nature of the interactions between latent conditions and active errors are non-linear are highly unpredictable. There are many unknown factors involved when latent conditions and active errors combine to form an error pathway through the layered defences of the system (Reason 1990). In this case, the holes in the slices of cheese can be considered as being the latent conditions and active errors and the system, therefore, can be breached when the holes in all of the layers line up to create an error pathway. However, because this is reliant upon so many unknown variables, the likelihood, according to Reason (1990), of a trajectory path, or a human-mediated mode of failure, which penetrates the many layers of a system is very remote. The Swiss Cheese model:

> "Tries to capture some of the stochastic features involved in the unlikely coincidence of an unsafe act and a breach in the system defences. It shows a trajectory of opportunity originating in the higher levels of the system, passing via the precondition and unsafe act planes on then on through three successive layers of defence. Each of these planes has windows of opportunity, but they are in continual flux due to the largely unpredictable influences of both intrinsic and extrinsic factors. On each plane, the areas of permeability or windows vary over time in both their location and their size, and these changes have different time constants at different levels of the system" (Reason 1990 p. 209).

Even though the Swiss Cheese model leads one to perceive that the holes are fixed in time and space, they are "in reality […] shifting around, coming and going, shrinking and expanding in response to operator actions and local demands" (Reason 1997 p. 9). Although the formation of the holes appears to be unpredictable—terrorists, nevertheless, have with apparent ease, been able to overcome the system defences, suggesting the proposed occurrence of these probabilistic events is not as unlikely as initially posited by Reason, and could, therefore, be related to other types of system behaviour yet to be discovered.

The 'Organisational Accident' model

In a later publication, Reason (1997) develops his Swiss Cheese model by proposing the 'Organisational Accident' model as a further conceptual framework which can also be used by security professionals to understand how latent conditions and active errors contribute to the failure of highly defended and protected systems. This model differs from the earlier version in that his organisational accident theory takes a more holistic view to describe the complex aetiology that contributes to the breakdown of socio-technical systems. Using this model, he states there are logical explanations to system failures, even though they are "hard to predict or foresee" and involve "causal contributions [that are] distributed widely both throughout the system and over time" (Reason 1997 p. 1–8). In contrast to others, this model explains causation from the bottom-up. It starts with organisational factors, then local workplace conditions and, finally, the unsafe acts of the human operators (Reason 1997).

With this being the case, Reason's work is now better placed to substantiate the idea that failures in socio-technical systems can be connected to high-level organisational decision-making and processes such as forecasting, deployment of resources, planning and communication. The model suggests that:

> "[…] acts […] [s]pawned in the upper echelons of the organisation and within related manufacturing, contracting, regulatory and governmental agencies […that] can increase the likelihood of active failures […] promoting errors and [rule based] violations" (Reason 1997 p. 10–11) [emphasis added].

By necessity, these conditions, in some way or other, will always be found in socio-technical systems (ibid.. p. 36) and "will be present from the very beginnings of the system's productive life, or will develop unnoticed—or at least uncorrected—during its subsequent operations" (Reason 1997 p. 12). Although the literatures do not offer very much in terms of providing a solution to the problem, it is, however, consistent with the idea that human-mediated errors entering and incubating within systems such as aviation security, is inevitable.

Actionable policy implications and directions for future research

Mitigating human-mediated aviation security failures should be integral to an over-arching risk management strategy, which recognises, in a far greater way, these types of

occurrences. This review provides an evidence-base to recommend a fresh actionable approach to analysing aviation security data to proactively mitigate the risk of human-mediated errors and system failures. Taking action is critical because air traffic demand is forecast by the International Air Transport Association (IATA) to nearly double over the next two decades with 7.2 billion air passengers in 2035 (IATA 2016). This growth will add to existing pressures and stresses on the aviation security system, which is already operating in a weakened state. Such demand could contribute to increase the frequency (or potential) of human-mediated system failures. In just the same way that other security systems which we rely on have evolved, collecting data and researching human-mediated system failures needs to move towards the development of new ideas and models, which examine all the crucial variables in the causal equation.

To do so, aviation security professionals and policymakers can take action by reframing these types of failures as a predictive data problem. Similar to that purported by Zang and Mahadevian (2019) in their research about improving aviation safety, this reframing could use qualitative and quantitative data to develop predictive (machine learning) models to quantify risk and to detect abnormal and sub-optimal security behaviours occurring in the system. Practically, these data could be obtained from existing incident reporting systems such as the Confidential Human Incident Reporting System (CHIRP) in the United Kingdom and the Aviation Safety Reporting System (ASRS) in the United States (cf. Zang and Mahadevian 2019 for a more comprehensive discussion about their hybrid machine learning framework for risk prediction). While these systems may collect some data relating to aviation security, it is suggested that more bespoke metrics will be required to analyse aviation security failures. This review therefore also recommends action to evaluate current data collection capabilities and development of new qualitative and quantitative data discovery processes for human-mediated aviation security failures (the themes discussed in this review can be used as a useful starting point for a new discovery framework).

Policymakers should also consider the empirical research highlighted in this paper, which identifies the inherent risk of human security operators, deliberately or unwittingly, not complying with security procedures. This risk could, in the future, be mitigated by increasing the use of artificial intelligence (a.i.) and machine learning technologies and methods. For example, security operators manually viewing screening images to detect prohibited items is also hugely inefficient. At scale, this could be automated to reduce errors and improve passenger flow rates through security checkpoints. While European and US Governments have made significant investment into developing a.i. security technologies, there are, however, significant technical challenges for machine learning algorithms to perform these tasks reliably. For instance, the EU-funded iBrderCtrl project,[2] which uses a virtual border guard to ask questions and detect deception, has been criticised for its accuracy and risk of unintentional biases being incorporated in the system (Airport Technology 2019).

Importantly, in seeking to increase the use of a.i. technologies, the aviation industry should avoid commercial opaque off-the-shelf "black box" machine learning models that have not been properly tested in an operational setting. To optimise security performance, a better way forward would be for the aviation industry to work with (non- commercial) experts and research institutes to build machine learning models that make better use of data

[1] See: https://www.iborderctrl.eu for more information about this project.

to tackle problems, such as those inherent with aviation security. In this way, machine learning tools can be established on widely accepted scientific principles, also with a level of transparency that can be used to galvanise support for their use.

Conclusions

This paper set out to discuss the literatures that can be used to make useful linkages between human-mediated errors and aviation security failures. It considered prior research, theoretical perspectives and conceptual models that have been developed from other, but related system failures. Although these models are helpful, there are several limitations relating to their applicability aviation security. In particular, the limitations associated with the predictive capability of any of these conceptual models to identify warnings and signals and take mitigating action before the onset of human-mediated system failure. Nevertheless, analysing aviation security in this very abstract way may could be useful to identify a high-level and relevant theoretical framework that can be used to improve the operational efficacy of the system (Jenkins 2012).

Although this review is theoretical, it can also be used to recommend policy change. Future work can be carried out in the following direction. Policymakers and aviation security professionals should develop new strategies and methods to acknowledge the risk posed by latent conditions and active errors. Specifically, focusing on the premise that when latent incubating conditions combine randomly together with other errors, they produce warnings and signals of the onset of system failure. Presently, these warnings and signals are only visible in hindsight, and the current system does not have the predictive capability, in foresight, to detect changes in the system condition. Thus, future research needs to be oriented towards using available security system data to identify at what point these conditions produce warnings and signals; classifying the tell-tale indicators that can be used to mitigate the impact and return the system to a safe condition.

Finally, in the context of this paper's contribution, effective aviation security depends on identifying crucial contributing variables to mitigate human-mediated modes of system failure. It is critical that future research and policy programmes seek to identify lines of causation due to the complexity of the linkages between human-mediated errors and security failures. This problem should be considered in the context of how the broader security landscape is changing; using available data together with artificial and machine learning methods to be more predictive about the risk of failures. Although, as this paper points out, there has been a paucity of valid empirical research in these areas, it remains for researchers, aviation security professionals and policymaker to embrace the benefits of using existing theoretical frameworks and new predictive methodologies to proactively expose and understand how human-mediated vulnerabilities can freely exist and contribute to aviation security failures.

References

Aini MS, Fakhru'l-Razi A (2009) Issues and lessons from fire inquiry tribunals. Disaster Prev Manag 18(4): 434–442

Aini MS, Fakhrul-Razi A (2010) Development of socio-technical disaster model. Saf Sci 48:1286–1295

Arcúrio MS, Nakamura ES, Armborst T (2018) Human factors and errors in security aviation: An ergonomic perspective. J Adv Transp 2018:1–9

Baxter G, Sommerville I (2011) Socio-technical systems: From design methods to systems engineering. Interact Comput 23:4–17

Blockley D (1998) Managing proneness to failures. J Contingencies Crisis Manag 6:76–79

Cherns A (1976) The principles of socio-technical design. Hum Relat 29:783–792

Chiu MC, Hsieh MC (2016) Latent human error analysis and efficient improvement strategies by fuzzy TOPSIS in aviation maintenance tasks. Appl Ergon 54:36–147

Davis MC, Challenger R, Jayewardene DNW, Clegg C (2014) Advancing socio-technical systems thinking: a call for bravery. Appl Ergon 45:171–180

Feakin T (2011) Insecure skies? Challenges and options for change in aviation security. Royal United Services Institute for Defence and Security Studies, London

Federici JF, Schulkin B, Huang F, Gary D, Barat R, Oliveira F, Zimdars D (2005) THz imaging and sensing for security applications–explosives, weapons and drugs. Semiconducter Sci Technol 20:266–280

Fink S (1986) Crisis management: Planning for the inevitable. Amacom, New York

Frimpong A (2011) Introduction of full body image scanners at the airports: a delicate balance of protecting privacy and ensuring national security. J Transp Secur 4:221–225

Grabowski M, Roberts K (1997) Risk mitigation on large-scale systems: Lessons from high reliability organizations. Calif Manag Rev 39:152–162

Grant AM, Fried Y, Juillerat T (2011) Work matters: job design in classic and contemporary perspectives. In: Zedeck S (ed) APA handbook of industrial and organizational psychology, vol 1. Building and developing the organization. American Psychological Association, Washington, DC, pp 417–453

Gray WD, Sabnani H, Kirschenbaum S (1993) Review of the book human error. Int J Man Mach Stud 39: 1056–1057

Hofer F, Wetter OE (2012) Operational and human factors issues of new airport security technology—two case studies. J Transp Secur 5:277–291

IATA (2016) Forecasts passenger demand to double over 20 years. Available at: http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx. Accessed 1 Apr 2020

Ibrahim MS, Fakhru'l-Razi A, Sa'ari M, Aini MS, Rashid S (2002) Bright sparklers fire and explosions: The lessons learned. Int J Disaster Prev Manag 11:214–221

International Civil Aviation Organisation (2011) Security: Safeguarding international civil aviation against acts of unlawful interference. Annex 17 to the convention on international civil aviation. International Civil Aviation Organisation, Montreal

Jenkins B (2012) Aviation security: After four decades, it's time for a fundamental review. RAND Corporation, Santa Monica

Kirschenbaum A, Mariani M (2012) Trusting technology: Security decision making at airports. J Air Transp Manag 25:57–60

Kirschenbaum A, Mariani M, Van Gulijk C, Lubasz S, Rapoport C, Andriessen H (2012) Airport security: An ethnographic study. J Air Transp Manag 18:68–73

Kirschenbaum A, Mariani M, Van Gulijk C, Lubasz S, Rapoport C (2012) Airports at risk: The impact of information sources on security decisions. J Transp Secur 5:187–197

Kirschenbaum A, Rapaport C, Lubasz S, Mariani M, Van Gulijk C, Andriessen H (2012) Security profiling of airport employees: Complying with the rules. J Airport Manag 6:373–380

Klitou D (2008) Backscatter body scanner—a strip search by other means. Comput Law Secur Rev 24:316–325

Kraemer S, Carayon P, Sanquist TF (2009) Human and organizational factors in security screening and inspection systems: Conceptual framework and key research needs. Cogn Technol Work 11(11):29–24

Lennerman A (2012) Protecting the airport from an insider threat: A systematic approach to aviation security. J Airport Manag 6:225–230
Leo JG, Lawler JP (2007) A study of passenger perception and sensitivity to airport backscatter x-ray technologies. Int Bus Econ Res J 6:11–18
Liang GF, Lin JT, Hwang SL, Wang EMY, Patterson P (2010) Preventing human errors in aviation maintenance using an on-line maintenance assistance platform. Int J Ind Ergon 40(3):356–367
McFadden KL, Towell ER (1999) Aviation human factors: A framework for the new millennium. J Air Transp Manag 5(4):177–184
McFarlane P (2017) Aviation security as a self-organized critical phenomenon. Dissertation. University of Northampton, Northampton
Miles RE, Zhang XC, Eisele H, Krotkus A (2007) Terahertz frequency detection and identification of materials and objects. Springer, Dordrecht
Mitchener-Nissen T, Bowers K, Chetty K (2011) Public attitudes to airport security: the case of whole body scanners. Secur J 25:229–243
Mumford E (2006) The story of socio-technical design: reflections on its successes, failures and potential. Inf Syst J 16:317–342
National Commission on Terrorist Attacks upon the United States (2004) The 9/11 Commission Report. W.W. Norton & Company, New York
Orouji T, Hosseini Pooya SM, Jafarizadeh M, Khosravi HR, Rais Mohammad H (2011) Doses to the scanned individual and to the operator from an x-ray body scanner system. Radiat Prot Dosimimetry 147:227–229
Peltu M, Eason K, Clegg C (2008) How a socio technical approach can help NPfIT deliver better NHS patient care. Available at: http://www.bcs.org/upload/pdf/sociotechnical-approach-npfit.pdf. Accessed 28 June 2012
Perrow C (1984) Normal accidents: Living with high risk technologies. Princeton University Press, New Jersey
Perrow C (1994) The limits of safety: The enhancement of a theory of accidents. J Conting Crisis Manag 2: 212–220
Perrow C (1999) Normal accidents: Living with high risk technologies. Princeton University Press, New Jersey
Perrow C (2007) The next catastrophe: Reducing our vulnerabilities to natural, industrial and terrorist disasters. Princeton University Press, New Jersey
Pidgeon N, O'Leary M (2000) Man-made disasters: Why technology and organizations (sometimes) fail. Saf Sci 34:15–30
Rasmussen J (1982) Human errors: A taxonomy for describing human malfunction in industrial installations. J Occup Accid 4:31–33
Rasmussen J (1983) Skills, rules, knowledge: Signals, signs and symbols and other distinctions in human performance models. IEEE Trans Syst Man Cybern 13:257–267
Rasmussen J (1988) Interdisciplinary workshop to develop a multi-disciplinary research program based upon a holistic systems approach to safety and management of risk in large scale technological operations: In: proceedings of a conference, Washington D.C, 1988
Rasmussen J, Vicente K (1989) Coping with human errors through system design: Implications for ecological interface design. Int J Man Mach Stud 31:517–534
Reason J (1987) Generic error modelling system (GEMS): A cognitive framework for locating common human error forms. In: Rasmussen J, Duncan K, Leplat J (eds) New technology and human error. Wiley, London
Reason J (1990) Human error. Cambridge University Press, New York
Reason J (1997) Managing the risks of organisational accidents. Aldershot, Ashgate
Reason J (2000) Human error: Models and management. Br Med J 320:768–770
Reason J (2008) The human contribution: Unsafe acts, accidents and heroic recoveries. Ashgate Publishing Limited, Farnham
Reason J, Parker D, Lawton R (1998) Organisational controls and safety: the varieties of rule-related behaviour. J Occup Organ Psychol 71:289–304
Redmill F, Rajan J (1997) Human factors in safety critical systems. Butterworth-Heinmann, Oxford
Rekiel J, de Wit J (2013) The security system at European airports—Tour d'Horizon. J Transp Secur 6:89–102
Saleh J, Cummings A (2011) Safety in the mining industry and the unfinished legacy of mining accidents: Safety levers and defence in depth for addressing mining hazards. Saf Sci 49:767–777
Schauer DA (2011) Does security screening with backscatter x-rays do more good than harm? Radiology 259: 12–16

Shrivastava P, Mitroff II, Miller D, Miglani A (1988) Understanding industrial crisis. J Manag Stud 25:285–303
Silver N (2012) The signal and the noise: The art and science of prediction. Allen Lane, London
Silverstein ME (1992) Your right to survive. Potomac Books, Washington
Song Q, Zhao Y, Redo-Sanchez A, Zhang C, Liu X (2009) Fast continuous terahertz wave imaging system for security. Opt Commun 282:2019–2022
Sorensen JN, Apostolakis GE, Kress TS, Powers DA (1999) On the role of defense in depth in risk-informed regulation. In: International Topical Meeting on Probabilistic Safety Assessment: proceedings of a conference, Washington, DC, 1999
Stewart MG, Mueller J (2018) Are we safe enough? measuring and assessing aviation security. Elsevier, New York
Sweet K (2003) Aviation and airport security: Terrorism and safety concerns. Prentice Hall, New Jersey
Sweet K (2009) Aviation and airport security: Terrorism and safety concerns, 2nd edn. Prentice Hall, New Jersey
Airport Technology (2019) How can AI speed up airport security? Available at: https://www.airport-technology.com/features/ai-at-airports-security/. Accessed 1 Apr 2020
Toft B, Reynolds S (1999) Learning from disasters: A management approach. Perpetuity Press, London
Toft B, Reynolds S (2005) Learning from disasters: A management approach, 2 edn. Butterworth Heinemann, London
Trist EL, Bamforth KW (1951) Some social and psychological consequences of the Longwall Method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. Hum Relat 4:3–38
Turner BA (1976) The development of disasters: A sequence model for the analysis of the origin of disasters. Sociol Rev 24:753–775
Turner BA (1978) Man-made disasters. Wykeham Publications, London
Turner BA, Pidgeon NF (1997) Man-made disasters, 2 edn. Butterworth-Heinemann, London
Vaughan D (1997) The Challenger launch decision. Risky technology, culture and deviance at Nasa. University of Chicago Press, Chicago
Vogel H, Haller D (2007) Luggage and shipped goods. Eur J Radiol 63:242–253
Waring A (1996) Safety management systems. Chapman & Hall, London
Weigmann DA, Shappell SA (2001a) Applying the human factors analysis and classification system (HFACS) to the analysis of commercial aviation accident data: In: proceedings of the 11th International Symposium on Aviation Psychology. Columbus Ohio, 2001. The Ohio State University, Columbus
Wiegmann DA, Shappell SA (2001b) Human error analysis of commercial aviation accidents: Application of the Human Factors Analysis and Classification System (HFACS). Aviat Space Environ Med 72:1006–1016
Wohlstetter R (1962) Pearl Harbor: Warning and decision. Stanford University Press, Stanford
Zhang X, Mahadevan S (2019) Ensemble machine learning methods for aviation risk prediction. Decis Support Syst 116:48–63