Toward an Epidemiology of Safety and Security Risks: An Organizational Vulnerability Assessment in International Airports

Ivano Bongiovanni[1,*] and Cameron Newton[2]

[1] Adam Smith Business School, University of Glasgow, Glasgow, UK

[2] School of Management, Queensland University of Technology, Brisbane, QLD, Australia

[*] Address correspondence to: Ivano Bongiovanni, Adam Smith Business School, East Quadrangle, Gilbert Scott Building, University of Glasgow, University Avenue, Glasgow G12 8QQ, UK; tel.: +44(0)141 330 1678; Ivano.Bongiovanni@glasgow.ac.uk

---

International airports are complex sociotechnical systems that have an intrinsic potential to develop safety and security disruptions. In the absence of appropriate defenses, and when the potential for disruption is neglected, organizational crises can occur and jeopardize aviation services. This investigation examines the ways in which modern international airports can be 'authors of their own misfortune' by adopting practices, attitudes, and behaviors that could increase their overall level of vulnerability. A sociotechnical perspective, the macroergonomic approach, is applied in this research to detect the potential organizational determinants of vulnerability in airport operations. Qualitative data nurture the case study on international airports produced by the present research. Findings from this study highlight that systemic weaknesses frequently reside in areas at the intersection of physical, organizational, and social spaces. Specific pathways of vulnerability can be drawn across these areas, involving the following systemic layers: individual, task, tools and technology, environment, and organization. This investigation expands the existing literature on the dynamics that characterize crisis incubation in multi-organization, multi-stakeholder systems such as international airports and provides practical recommendations for airport managers to improve their capabilities to early-detect symptoms of organizational vulnerability.

SOCIAL MEDIA SUMMARY:

Do we need a more holistic view on safety and security management in complex sociotechnical systems? This study paves the way to an epidemiology of safety and security risks in international airports.

KEY WORDS:

Organizational vulnerability; Airport risk management; Safety and security risks.

1. INTRODUCTION

In 2016, the International Air Transport Association projected that passengers worldwide will reach 7.2 billion by 2035, with an annual Compound Average Growth Rate of 3.7% (International Air Transport Association, 2014). Such demand for aviation services exerts remarkable pressure on the airport infrastructure, from a variety of stakeholders, whose interests often conflict. Indeed, compliance with safety and security regulations, economic goals, and time pressures coexist in the airport context and are managed by different actors, belonging to different organizations. Stemming from unintentional or intentional causes, safety and security risks have the potential to generate economic losses and, in the worst cases, human casualties in modern airports. The impact of disruptive safety and security occurrences is exacerbated by globalization, no-boundary attitudes, continuous flow of people and freight, and long-distance travel for leisure and work (Knox, O'Doherty, Vurdubakis, & Westrup, 2008). From a safety viewpoint, the complexity of air transport makes the provision of adequate levels of safety a difficult task (Netjasov & Janic, 2008). Similarly, from a security perspective, the features of modern airports make them particularly attractive target for terrorists (Stewart & Mueller, 2014), as well as an asset that requires expensive protection strategies from airport organizations (Shafieezadeh, Cha, & Ellingwood, 2015; Stewart & Mueller, 2013).

Airports can be described as large-scale sociotechnical systems made up of bounded work systems (e.g., arrival area, shops) acting as a unified whole (the airport infrastructure). Due to their complexity and size, modern airports can produce '*dysfunctionality'* (Lalonde & Roux-Dufort, 2010, p. 22) or errors that can manifest as risks, service disruptions and, potentially, larger crises. Indeed, airports have a particular potential for the generation of vulnerability, especially through their routine managerial processes (e.g., management of labor intensive operations; high integration and engagement with customers' groups; presence of

mixed components from both public and private sectors; increasing scale of operations over time; wide range of performed activities; etc.) (Smith, 2005).

Despite their potential relevance, holistic studies on safety and security risks in airports are missing in the literature, which seems more prone to providing case-specific guidelines and solutions for managing such risks, rather than focusing on understanding their complexity (Nash et al., 2012). Two components are missing from the scholarly literature: holistic taxonomy of safety and security risks and an associated epidemiological study.

The present study explores these caveats by attempting to establish a classification of safety and security risks and by laying the methodological foundations to investigate their epidemiology (Boyer & Pronovost, 2010), through the lens of pathways of vulnerability.

2. REVIEW OF THE RELEVANT LITERATURE

The conceptual framework adopted in the present paper sits at the intersection of four research areas: vulnerability, epidemiology of safety and security risks, vulnerability of airports to safety and security disruptions, and the macroergonomic approach (MeA) which looks at how systems work (or do not work) well together.

2.1. Vulnerability

Vulnerability was initially conceptualized in crisis and disaster management, with particular reference to social vulnerability of populations exposed to natural hazards (McEntire, 2001). Researchers started investigating the concept of vulnerability in an attempt to respond to the traditional *hazard-centric approach* to crises (White, 1974), which reflects the conventional view on the concept of risk. According to this perspective, in the dichotomy between *risk agent* (the source of risk) and *risk absorbing system* (the object of the risk), the traditional, predominant focus of analysis is on the former (McEntire, Gilmore Crocker, & Peters, 2010). Hazards are therefore considered the main focus of investigation to understand how potential risks turn into actual crises.

However, empirical observations of crises highlight that hazards are not the only element to take into account in the case of adverse events (England, Agarwal, & Blockley, 2008). Low intensity hazards have the potential to initiate a chain reaction leading to major consequences. Conversely, high intensity hazards can have negligible impacts. An explanation of such an apparent contradiction resides in the risk absorbing system. Indeed, the relevance of operational risks is *also* determined by inherent characteristics of the subject threatened by a specific hazard, in a word, by its *vulnerability* (McEntire, 2004).

Traditionally, three main stages characterize the theoretical development of vulnerability (Bouchon, 2006). First, vulnerability is considered from a technical perspective, as determined by the *degree of loss and damages* deriving from a hazard. Social dimensions of vulnerability are ignored. Second, vulnerability accounts for the *degree of exposure* to hazards, as reflected by loss and damages (Dow, 1992). Last, vulnerability refers to the *internal characteristics of the element at risk* (Lewis, 1999), where loss and damage become a function of the *resistance* capacity of the technical system. Similarly, from a social perspective, they become a function of the *resilience* capacity of the considered human system (Bouchon, 2006). This last stage adopts a *sociotechnical approach* in assessing vulnerability and accounts for social factors as well as more traditional technical factors.

The developmental notion of vulnerability can further be summarized in two main categories (Bouchon, 2006), which constitute its basic ontology. First, hazard-dependent vulnerability is determined by the amount of damage experienced by a system after being affected by a hazard. Vulnerability is mainly interpreted as an indicator of outcome. Second, hazard-independent vulnerability is determined by the internal state of a system, regardless of external hazards. Vulnerability is predominantly interpreted as an indicator of input.

From an epistemological perspective, vulnerability can be conceived as a *conceptual cluster* (Füssel, 2007, p. 156) and be investigated based on the specific context (e.g., economy,

ecology and sociology). According to this approach, knowledge of the concept of vulnerability is impossible if isolated from its specific context. Vulnerability can also be explored based on the *nature of the object of vulnerability*. This implies isolating vulnerability from its context and focusing on the characteristics of the vulnerable system (e.g., individual vulnerability, organizational vulnerability and infrastructural vulnerability). Knowledge of the concept of vulnerability is possible regardless of its context.

According to the adopted *ontological* and *epistemological* postures, research on vulnerability can be positioned in any of the quadrants of the following matrix (Fig. 1).

		Epistemological focus	
		Context	*Object of Vulnerability*
Ontological focus	*Hazard-Dependent*	Amount of physical damages caused by a coastal hurricane; Magnitude of financial losses deriving from economic turmoil; Extent of social damages produced by an epidemic on a given population; Etc.	Losses deriving from a terrorist attack in a major airport; Impact of stress agents on the performance of an individual; Lost reputation from sabotage perpetrated to an organisation; Etc.
	Hazard-Independent	Degree of sensitivity of a population to climate change-related issues; Resistance of a small economy subject to financial constraints; Capacity to internally develop conditions for political crisis; Etc.	Managerial factors increasing the chances for crises to occur; Technical faults in a power plant possibly leading to accidents; Individual ability to resist to, and recover from, conditions of physical incapacitation; Etc.

Fig. 1. Conceptual frameworks to investigate vulnerability with practical examples and focus of the present research (grey area)

The present research conducts a hazard-independent assessment of organizational vulnerability to safety and security risks, with international airports as object of vulnerability[1].

[1] As discussed, adopting a hazard-independent approach entails significant analytical benefits. However, we acknowledge its incongruity with traditional public response to hazards, which is mainly hazard-specific. Further research is needed in this area. We thank an anonymous reviewer for remarking this.

This means focusing on the airport as the risk absorbing system, regardless of the potential risk agents (e.g., a disgruntled operator or a violent storm). Vulnerability is considered as an input factor (e.g., as a function of the solidity of the external perimeter fence) and not as an outcome measure (e.g., as the economic loss deriving from weather-related flight cancellations). This study aims at expanding our understanding of determinants of safety and security risks, with a view to lay the foundations for their epidemiology (Boyer & Pronovost, 2010), in modern international airports.

2.2. Toward an epidemiology of safety and security risks: pathways of vulnerability

Prior research has highlighted that determinants of vulnerability rarely act in isolation (Turner, 1976; Turner & Pidgeon, 1978). The concept of *pathways of vulnerability* (Drennan, McConnell, & Stark, 2014; Kraemer, Carayon, & Clem, 2009; Smith, 2004, 2005) suggests that vulnerability develops through *corridors* that have the potential to lead to specific disruptions in normal business operations. Accordingly, in a study on the organizational determinants of vulnerability, the identification of such determinants (classification) is as important as the comprehension of the ways in which these determinants align and interact (analysis).

In pioneering work on the epidemiology of crises, Reason (1990) described the initial stages of crises as a set of latent conditions that develop through managerial practices. These conditions usually take the form of embedded *'failure pathways'* (Smith, 2005, p. 314), which reside in organizational processes and procedures. As such, managerial functions have a major role in crisis incubation, although this is often neglected in the literature (Smith, 2005). At an initial stage, decisions made at the managerial level can create the conditions for organizational controls to be by-passed (Carayon et al., 2006; Smith, 1990a, 1990b, 1995). In airports, an example of this can be the habit of staff members to leave security doors open behind them to

facilitate transit to, and from, the sterile area. This may constitute a latent antecedent for a potential risk to become an organizational crisis.

The literature presents a range of papers that explore the concept of pathways of vulnerability in various domains. In their work on food supply chains, Stave and Kopainsky (2015) adopt a system dynamics approach to unveil the mechanisms and pathways by which food systems can be affected by disturbances. Findings demonstrate that vulnerability of a national food system does not only result from external shocks, but also from the internal interaction of feedback loops in the food system. The authors recommend that future research be focused on exploring internal threats of food supply stability. Kraemer, Carayon and Clem (2009) assess the human and organizational factors that can be responsible for technical vulnerabilities in the field of Information and Communication Technologies. This study illustrates an original taxonomy of four different categories of vulnerability: design, implementation, configuration, and operational. Furthermore, it produces a classification of contributing human and organizational factors (e.g., external influences, human error, management, etc.). Through causal network analysis, the researchers associate the different categories of vulnerability with the identified factors. Findings underline that human and organizational factors contribute to the creation of a single pathway of vulnerability (Kraemer et al., 2009). Two pathways that have the potential to lead to organizational crises in public agencies have been identified by Drennan, McConnell, and Stark (2014). The first pathway is characterized by a slow incubation process, in which crises' determinants are internally developed. The second pathway, typical of events such as natural disasters, involves a sudden trigger that, by leveraging a pre-existing condition of vulnerability in the affected system, unleashes a crisis. Regardless of the typology of involved pathway, crises are mainly caused by failures in one or more of the following elements: human behavior, technology, management systems, and government behavior. Smith (2000, 2004, 2005) argues that vulnerability

develops in modern organizations throughout the crisis life-cycle. By conducting an external audit, pathways of vulnerability can be identified and used as the basis for crisis simulation exercises. The author recommends this procedure as a way to highlight the assumptions and beliefs that underlie the organizational life and as a first step towards the diffusion of a crisis-prepared organizational culture.

Several points are critical relating to pathways of vulnerability research. First, organizational disruptions are rarely the result of a unique determinant, often originating from the interplay of different co-factors. Second, regardless of the field of investigation, the concept of pathways of vulnerability provides an interpretation of the aforementioned interplay. Third, as the nature and number of co-determinants for organizational disruptions varies, a holistic perspective is deemed to be the most appropriate in order to gauge their origins. Last, the comprehension of pathways of vulnerability is deemed to constitute a crucial element in the diffusion of a crisis-prepared organizational culture.

2.3. Vulnerability of airports to safety and security disruptions

Research investigating airports' vulnerability to safety and security risks is scarce and mainly adopts a hazard-dependent approach (Fig. 1). This entails a focus on the triggering factors, for instance the patterns followed by extreme meteorological events around airports, (Lopez, 2016) or the behaviors enacted by Improvised Explosive Devices attackers (Lord, Nunes-Vaz, Filinkov, & Crane, 2010), rather than on the underlying organizational factors that contribute to the disruptive events. A notable exception to the prevalent hazard-dependent approach is represented by Pettersen and Bjornskau (2015), who investigate the organizational contradictions between aviation safety and airport security following the introduction, in Europe, of new security regulations. The misalignment between safety and security measures is indicated as a source of systemic vulnerability in aviation organizations. Admittedly:

> *Studies that address the relationship between flight safety and aviation security from an organizational perspective, focusing on […] organizational structure, culture, and power, seem to be lacking.* (Pettersen & Bjørnskau, 2015, p. 168).

The overwhelming majority of the literature on airport vulnerability reveals two distinct *foci*: safety or security issues. Among the most recent examples in the area of airport vulnerability to safety disruptions, the consequences of climate change (e.g., variation in wind directions, increase in temperatures, etc.) have been investigated by means of a hazard-dependent approach focused on the airport physical infrastructure (Lopez, 2016). An integrated hazard-dependent and hazard-independent approach is adopted by Li and Xu (2015), who propose a method to help air traffic administrations schedule airport maintenance to avoid safety concerns and service disruptions. Vulnerability is assessed based on the structural characteristics of the explored airports (nature of the object of vulnerability) and on the specific hazard (maintenance risks). However, no reference to managerial and organizational vulnerability factors is made. Similarly, Anh Tran and Namatame (2015) provide a model of the worldwide aviation network to illustrate its typical spatial characteristics. This allows the researchers to highlight the responses of the network to extreme events (hazard-dependent vulnerability analysis) and produce practical recommendations on how to improve such responses.

In general, the literature on models for airport security threat assessment adopts a combined hazard-dependent and hazard-independent perspective. Assessment of security risks (e.g., terrorism) is conducted considering both the characteristics of the airports (e.g., physical layout, security defenses, etc.) and the intentions or capabilities of the attackers. In their study on the sequential decision framework of attackers to a US airport, Shafieezadeh, Cha and Ellingwood (Shafieezadeh et al., 2015) assess the vulnerability of the airport's security systems based on the progressive decisions made by the attackers and calculate the likely losses for the airport according to whether the attack was successful, partially successful or unsuccessful.

However, an exploration of the intrinsic, organizational factors that impact the security performance of the airport lies outside the scope of the research.

The work by Lord et al. (2010) segments the airport in sub-components and elaborate a probabilistic model to assess the risks associated with an Improvised Explosive Device attack. This investigation considers vulnerability from a hazard-dependent perspective and revolves around the nature of the object of vulnerability. This study depicts a series of scenarios, in which the physical features of the front-of-house (e.g., size) and a number of mitigating factors (e.g., presence of threat detection systems) impact on the extent of the associated security risks.

Overall, there is a notable scarcity of studies adopting a hazard-independent approach to investigate vulnerability. The present paper is intended to fill this gap. The definition of vulnerability underlying this paper is borrowed from Kraemer, Carayon and Clem who consider vulnerability as the result of *'flawed organizational policies and individual practices whose origins are deeply rooted within early design assumptions and managerial decisions'* (2009, p. 510). This definition addresses a call in the literature that recommends assessing vulnerability based on the reality of human behavior within the organizational context of reference (management). According to the aforementioned definition, four elements are deemed to be key constituents of organizational vulnerability: organizational policies, individual practices, early design assumptions, and managerial decisions. These elements are mirrored in the Macroergonomic Approach (MeA) (Kraemer et al., 2009), which is a holistic framework for sociotechnical systems analysis that focuses on organizational characteristics and design of complex work systems (such as airports). As the sociotechnical framework that most closely explores the human-organization interface (Carayon & Smith, 2000; Hendrick & Kleiner, 2001; Kraemer et al., 2009), the MeA is utilized in the present research to investigate the vulnerability of airport operations.

2.4. Macroergonomic approach

Originating in the human factors and ergonomics mainframe, the MeA explores human performance and its limitations in the context of a specific sociotechnical system. In human factors and ergonomics, the relationship between human and system components occurs on five levels: human-machine (*hardware ergonomics)*; human-environment (*environmental ergonomics*); human-software (*cognitive ergonomics*); human-job (*work-design ergonomics*); and human-organization (*macroergonomics*) (Hendrick, 1998; Hendrick & Kleiner, 2001, 2002).

The MeA has been identified as a *'top-down sociotechnical systems approach to the design of work systems'* (Hendrick & Kleiner, 2002, p. 3). The MeA adopts a holistic approach in which the organizational design influences the human performance. Decisions made at the macro-level (the organization) are a pre-requisite for decisions made at the micro-level (the workstation). The perspective adopted by the MeA is *syncretic* in that it encompasses knowledge originating from a variety of research areas: sociotechnical systems, organizational psychology and human factors and ergonomics (Murphy, Robertson, & Carayon, 2014). The MeA elevates the traditional focus on work design and reaches out to higher systemic levels by describing sociotechnical systems as constituted by the sub-components depicted in Table I (Carayon & Smith, 2000; Kraemer et al., 2009).

Table I. Components of the MeA

MeA component	Examples
Individual	Physical status of operators, psychological conditions, skills
Task	Work pressure, job content, job control
Tools & Technology	Tools utilized during work duties
Environment	Workplace layout, noise levels, air quality
Organization: communication	Information-sharing arrangements
Organization: culture	Organizational values and behaviors
Organization: policy	Regulations, policies, guidelines
Organization: structure	Governance mechanisms
Organization: implementation	Application of organizational policies
Organization: strategy	Long-term organizational goals

Under certain conditions, the interplay among the aforementioned components can create systemic vulnerability. This interplay is shaped along specific patterns, or pathways of vulnerability (Kraemer et al., 2009).

3. RESEARCH METHODS

The present study, conducted in three airports in Australia, aimed at identifying potential organizational determinants of vulnerability to safety and security disruptions in international airports, by investigating the perceptions that airport actors have around safety and security risks. Due to the *exploratory* nature of the research (Babbie, 2013), we adopted a qualitative methodology (single case study). Despite the numerous organizations involved in airport operations, this research focused on the airport management functions executed by the airport operator. As an organization, airport management is the focal point of airports and sits at the intersection of the sociotechnical complexity of the airports.

We conducted 30 semi-structured interviews (12 in Airport A, 8 in Airport B and 10 in Airport C), analyzed 37 organizational documents (14 in Airport A, 16 in Airport B and 7 in Airport C) and spent around 21 hours in field observation (approx. 7 hours per airport). Data were predominantly drawn from the interviews (which revolved around participants' perceptions of safety and security risks), with document analysis and field observation as complementary methods.

3.1. Data collection methods

Key contacts in each airport identified interviewees who could provide insightful information. The selection of respondents followed a *purposeful sampling technique* (Patton, 2002) where the sample was categorized into four units of analysis: *leadership level* (LL) which included the general managers; *corporate management level* (CML) including the corporate managers reporting to the general managers; *operational management level* (OML) including operational managers reporting to the corporate managers; and managers from the *security screening providers* together with the Australian Federal Police (SSP/AFP), due to their

interconnectedness with airport security. The sample was further classified according to the areas of operations of the interviewees: landside managers (LS) responsible for terminals and annexes, airside (AS) managers predominantly dealing with tarmac operations, and landside/airside managers (LS/AS) with mixed functions. Table II illustrates the sample adopted for the semi-structured interviews.

Table II: Sample for the semi-structured interviews

Unit of Analysis	Area of Operations			
	Landside	**Landside/Airside**	**Airside**	**TOTAL**
Leadership Level	-	3	-	3
Corporate Management Level	3	4	3	10
Operational Management Level	2	7	3	12
SSP/AFP	5	-	-	5
TOTAL	10	14	6	**30**

Note: SSP/AFP = Security Service Providers/Australian Federal Police

Respondents agreed to have their interviews audio-recorded, except two cases where detailed notes were taken. Examples of questions asked during the interviews included: *'What are the most common safety and security risks to normal business operations that could manifest in your area of operations?'* and *'What factors could contribute in generating these safety and security risks, and how?'*

Document analysis included investigation of organizational documents (e.g., incident identification and investigation reports, risk assessment plans, etc.). Besides, field observation helped the researchers make sense of airport processes, practices, and structures (Knox et al., 2008), and was conducted in a *hanging around* form (Marshall & Rossman, 2011) in the three data collection sites. This included terminal walk-throughs and airside and security checkpoints inspections. Field notes were taken with a focus on impersonal elements such as airport layout, design, and organizational processes (Punch, 2012).

3.2. Data analysis

Data were coded using qualitative data analysis software (QSR International's NVivo 10). The first level of analysis of the organizational determinants of vulnerability was based on the categories proposed by the MeA. Recurring sub-themes were identified in the second level of data analysis.

An inter-rater test of reliability of the coding criteria was conducted on different excerpts of the semi-structured interviews. The resulting kappa coefficient was greater than 0.81 for all the coded excerpts (0.81 to 0.94), which indicates almost perfect agreement (Landis & Koch, 1977). Overall, 84 excerpts were compared, equally extracted from interviews in the three airports. These tests confirmed the reliability of the adopted frameworks for coding and data analysis.

4. RESULTS

In the interviews, the first set of questions revolved around the safety and security risks that respondents reputed the most relevant. This component of the study was intended to gain a better understanding of the perceptions existing among airport organizations with regards to their most significant risks. Saturation was achieved across the three aerodromes. Table III describes the safety and security risks indicated in the 30 semi-structured interviews, ranking them by frequency. It is worth further stressing that such risks are not actual events occurred in the airports, but potential instances whose frequency is calculated as percentage of participants referring to them in the interviews.

Table III: Safety and security risks

Disruption	Description	Freq. (%)
Landside security breaches	The integrity of the sterile area can potentially be compromised by access of unscreened individuals. Instances include: unscreened passengers, passengers in transit from unscreened airports, pass-back doors violations, etc.	63.3%
Congestion and queuing	Disturbances generated by reduced functionality in airport operations (e.g., check-in and security screening) which result in congestion at the airport facilities.	46.7%
Ramp safety issues	Workplace health and safety-related events (WHS) during airside operations in airports' ramp (*apron*), including:	40%

	mismanagement of ground service equipment, speed limit violations on the ramp, driving behind pushbacks, etc.	
Disruptive behaviors by passengers and general public	Passengers or members of the general public displaying disruptive behaviors. Instances include: refusal to undergo screening, hostile attitude, hoaxes, and criminal activity.	40%
Landside safety events	WHS occurrences affecting passengers, general public, or staff members in the landside area. Instances include: escalator falls, slips, trips and falls in the terminals, etc.	36.7%
Airside breaches	Security-related violations of the airside area. Instances include: access by wandering passengers, access control breaches by staff members, and external perimeter violations.	36.7%
Prohibited items violations	The intentional or unintentional introduction of items prohibited under current regulations into the sterile area of the airport.	36.7%
Technical failures	Disruptions in the functionality of technical assets in any of the airports' subsystems. Instances include failures to: IT systems, equipment, infrastructure, and aircrafts.	33.3%
Bird and wildlife management	Issues with the control of the wildlife living within and in the vicinity of the aerodromes. Bird-strikes represent the most significant of these instances.	26.7%
Natural hazards	These instances range from adverse weather conditions to calamitous natural events whose consequences can be minor or catastrophic.	26.7%
Unattended items	Personal items left unattended in the airport facilities. Instances include: unattended suitcases, working tools, boxes, etc.	26.7%
Fire alarms	Activation of fire alarms disrupting the normal airport operations (false alarms or fire events).	23.3%
Aircraft emergencies	Aircrafts experiencing issues when landing, parking, taxing or taking off.	20%
Maintenance, works and repairs	Extraordinary interventions on the airport infrastructure that have the potential to alter the normal flow of operations or entail safety issues.	20%
Traffic management front-of-house	Ancillary transportation services to and from the airport (parking, taxis, buses, trains) potentially jeopardized by service disturbances.	13.3%

Data revealed that safety and security risks escape strict classification. Each airport operator had a different methodology to collect, report and classify potential safety or security disturbances to their operations. One example was represented by the incident reporting systems utilized in the three airports, which ranged from statistical recollections of numerical values to detailed descriptions of events. Data revealed that these risks have different characteristics, according to their circumstances (e.g., the various types of potential aircraft emergencies); incubate and manifest in specific areas of operations; in extreme cases could

impact the whole airport or the national/global aviation network; could involve multiple actors from different organizations (public and private); and in cases of particular relevance, could affect the organization across the functional and hierarchical levels (e.g., units of analysis).

4.1. Macroergonomic factors of vulnerability

A total of 883 excerpts were coded around the 10 MeA categories. Table IV displays the MeA categories, sub-categories, their description and illustrative quotes from the interviews. Sub-categories constitute a novelty in the literature, as we elaborated them based on the most recurring themes that we identified within each MeA category.

Table IV. Macroergonomic factors, sub-categories and sample quotations

Macroergonomic factors	*Sub-categories*	*Description*	*Sample quotations*
Individual	**Complacency**	Sub-optimal level of attention in operators due to reduced activity	*'Are [the security screeners] feeling involved in what they're doing? Not always. Not so much out on the inspection points, where it's a bit monotonous.' (SSP/AFP-LS)*
	Stress	Psychological adverse state caused in operators by high levels of stress	*'"Look, I'm splitting up with my wife. My head isn't in the space." So, I go, "Okay, we're not gonna put you on operation screening. We're gonna put you somewhere else." So, in this way you're mitigating the risk by removing it.' (SSP/AFP-LS)*
	Lack of skills	Inadequate physical or psychological skills by operators in performing their duties	*'Sometimes some of the screening staff are not as skilled as they need to be in understanding the diversity of the people.' (OML-LS/AS)*
	Limited experience	Background experience of safety and security operators crucial in determining their performance	*'[Some ground handlers] are not quite getting the experience out there that they should. Some companies used to wait six months before they let some drive out there, whereas now, almost two weeks, they're trying to get them out there driving.' (CML-AS)*
Task	**Task repetitiveness**	Monotonous tasks following the same pattern may cause complacency in operators	*'Usually the reason why the guys miss [prohibited items during baggage screening], is because they're just tired, or they're looking at hundreds of bags every day. Not expecting it.' (CML-LS/AS)*
	Stressful tasks	Bounded by time constraints, operators may pay less attention to safety and security	*'[Ground handlers] need to rush, rush, rush. They'll run all over the place. […] On time performance sort of affects people's behavior, speeding and stuff like that.' (CML-AS)*
Tools and Technology	**Landside**	Non state-of-the-art equipment (hardware and software) affecting safety and security performance	*'I know at the domestic terminal they are looking at the [screening process] with the single view x-rays, but there's much better technology out there which we currently use at the international points transit.' (SSP/AFP-LS)*
	Airside	Need to constantly improve safety equipment to reduce risks Airside	*'We're currently looking at new equipment for bird dispersal and that sort of stuff. So yes, there's an area there where we're lacking because of the other side.' (OML-AS)*
Environment	**Landside**	Certain elements associated with the physical layout of terminals may produce sub-optimal safety and security	*'It's part of the whole design of where you've got departing and arriving mixing at those peak times. He's not the first person to have fallen over someone else's bag because of that interaction or that chaos that you sometimes...' (OML-LS/AS)*
	Landside/Airside	Sterile areas and transit points design have an impact on the performance at the screening points	*'[The separation between international and domestic terminals] makes it much more complex for the passenger in terms of transits, and also for levels of screening. So, we might have certain level of screening for one terminal that's not the same for the others.' (OML-LS/AS)*

Macroergonomic factors	*Sub-categories*	*Description*	*Sample quotations*
	Airside	Layout of external facilities may make Airside areas crowded	*'Aircraft parking restraints in terms of the amount of bays we've got and stuff like that. We'll have some squeezy times, so, our morning peak is the killer but I think it's a common problem around a lot of the airports around Australia.' (CML/AS)*
Organizational: Communication	**Internal**	Gap between the safety and security functional areas in terms of communication	*'I actually think that the Airside safety team is better linked into the business than the security team. The security team, sort of, sit out on their own, they're isolated. They're not integrated into the business, they think it's some secret stuff, but it's not a secret.' (CML-LS/AS)*
	Systemic	Some governmental agencies may be reticent in sharing information with airport management	*'The government agencies are a little bit different because of their clearances and because of our clearances. So, they're not allowed to share certain information to private industry. So, there's a bit of disconnect there. It's just an old methodology again.' (OML-LS)*
	External	Sub-optimal communication between airport organizations and passengers or general public	*'The public really even to this day, still don't know what they can and can't bring through, because nobody checks the government websites and you can put out as much information out at the front of the screen and point, nobody reads signs, nobody listens to videos.' (SSP/AFP-LS)*
Organizational: Culture	**Culture**	Organizational cultures may diffuse complacency, inadequate information sharing and gaps between safety and security functions	*'The guys doing safety on the apron, they are very aware of the arena they are working on, which is very complex. Safety, safety, safety…excellent. Security guys, on the other hand, I sometimes wonder if they really know what their role is.' (LL-LS/AS)*
	Training	Training effectiveness may clash with cost savings by airport organizations	*'How do you ensure that airlines have got the right training, processes, and procedures in place? You're dealing with the low cost model and their contractors and that can be difficult.' (CML-LS/AS)*
Organizational: Policy	**Safety**	Due to its nature, safety may be difficult to regiment and open to interpretation	*'Because here, you know, in some areas the Manual of Standards will say aerodrome operators "should" do this. Well, that's not a "must" or "shouldn't" and then you'd find a paragraph here that says do this, but this other paragraph completely opposite.' (CML-AS)*
	Security	Security can be perceived as a non-natural process, which may lead to sub-optimal performance	*'Security's not a natural process. If I said to you "Don't leave your bag unattended and remove all your wooden artefacts and don't have a plastic knife." You'd go, "Really?" So, it's not ingrained process. It's not a process that everyone does through life.' (OML-LS)*
Organizational: Structure	**Rostering**	Under-staffing caused by the low cost business model may impact the safety and security performance	*'Staffing level is probably a lot less. The ground handling companies probably don't have as many staff as they could. I mean they got minimal staff. You often have issues when you wanna move aircrafts at night because they haven't got staff around or available. So, they're not rostered on.' (CML-AS)*

Macroergonomic factors	*Sub-categories*	*Description*	*Sample quotations*
	Contracts	Complex contractual arrangements may reduce the effectiveness of controls by airport management on other organizations	*'Especially in the case of low cost carriers, they are under contractors. To me, that adds another barrier or ownership of the issue. My hands are tied. It doesn't help facilitate that ownership of the customer service issue. I believe there is more of a discharge of responsibility.' (CML-LS)*
Organizational: Implementation	**Security screening**	Security operators may inadequately implement screening procedures	*'It comes back to an appreciation of the behaviors of people and not putting everybody into one box and understanding the diversity of the makeup of your travelling public.' (OML-LS/AS)*
	Training	During training, excessive focus on screening procedures than on reasons for screening	*'Sometimes we train too much on the procedures but then, when I ask the guys "Why are you screening?", they don't know, so I would like to have more training on why we do screening in airports.' (SSP/AFP)*
	Cost reduction	Implementation of a real low cost model may impact the performance of operators	*'Whereas, I guess five years ago, the low cost carriers weren't really low cost, I guess that they weren't really operating that true low cost model. They'd say: "We just waiver the excess baggage fee and that's okay", or whatever that be. It's a change in their operating models of the airlines that's kind of having a follow on to airports as such.' (CML-LS/AS)*
Organizational: Strategy	**Low cost business model**	Pressure on the achievement of economic goals may be detrimental to safety and security	*'You know, airlines are all about on time performance, so that puts pressure on their staff straightaway. They just want passengers on the seats. As long as they can get their seats, they're happy.' (OML-LS)*
	Competition	Economic competition may suggest airport organizations to put in place strategic behaviors potentially detrimental to safety and security	*'So, at the moment, the decision to cease operations in case of natural hazards has to be through consultation, negotiation and that can sometimes be difficult, because airlines are competitive by nature. Neither one of them wants to stop operating before the other one does and that will put…their risk cap type is a lot different.' (CML-LS)*
	Stakeholder networks	Airport management may be *caught in the middle* in the airport's stakeholder network	*'The airports are the ones that I guess are in a really quite precarious situation, because they have to go back to the regulators. Then you've got your airlines that, as we said, they all do things slightly differently, but then how as an airport can you manage that?' (OML-LS)*

Note: CML = Corporate Management Level; OML = Operational Management Level; SSP/AFP = Security Service Providers/Australian Federal Police; LS = Landside; As = Airside.

The four units of analysis (LL, CML, OML, and SSP/AFP) were expected to enable identification of recurring nodes within the *hierarchical level* of the respondents. Results demonstrated that no significant trend could be singled out by analyzing the units of analysis as a mediator of the organizational factors for vulnerability. Nonetheless, some patterns seemed to emerge by looking at the areas of operation where the data originated (landside, airside and landside/airside). Interviewees mainly involved in LS operations underlined the importance of security-related factors; managers primarily operating AS emphasized the importance of safety-related factors; and a mixed perspective was provided by data drawn from the combined LS/AS areas of operation.

Data also revealed that the factors of vulnerability do not act in isolation, but constantly interact and influence each other, as multiple layers potentially producing pathways of vulnerability. This supports existing literature on this topic (Kraemer et al., 2009; Smith, 2004, 2005). We drew these mutual connections as they were emphasized by the respondents in the semi-structured interviews, and linked them with the safety and security risks that we had previously underlined.

An example of this were the Airside security breaches (Fig. 2), a category of security disruptions potentially deriving from a combination of individual (complacency by operators), task (task repetitiveness), environmental (design of LS/AS transit points), and cultural factors (an organizational culture of complacency towards, for instance, security doors left open by staff members).

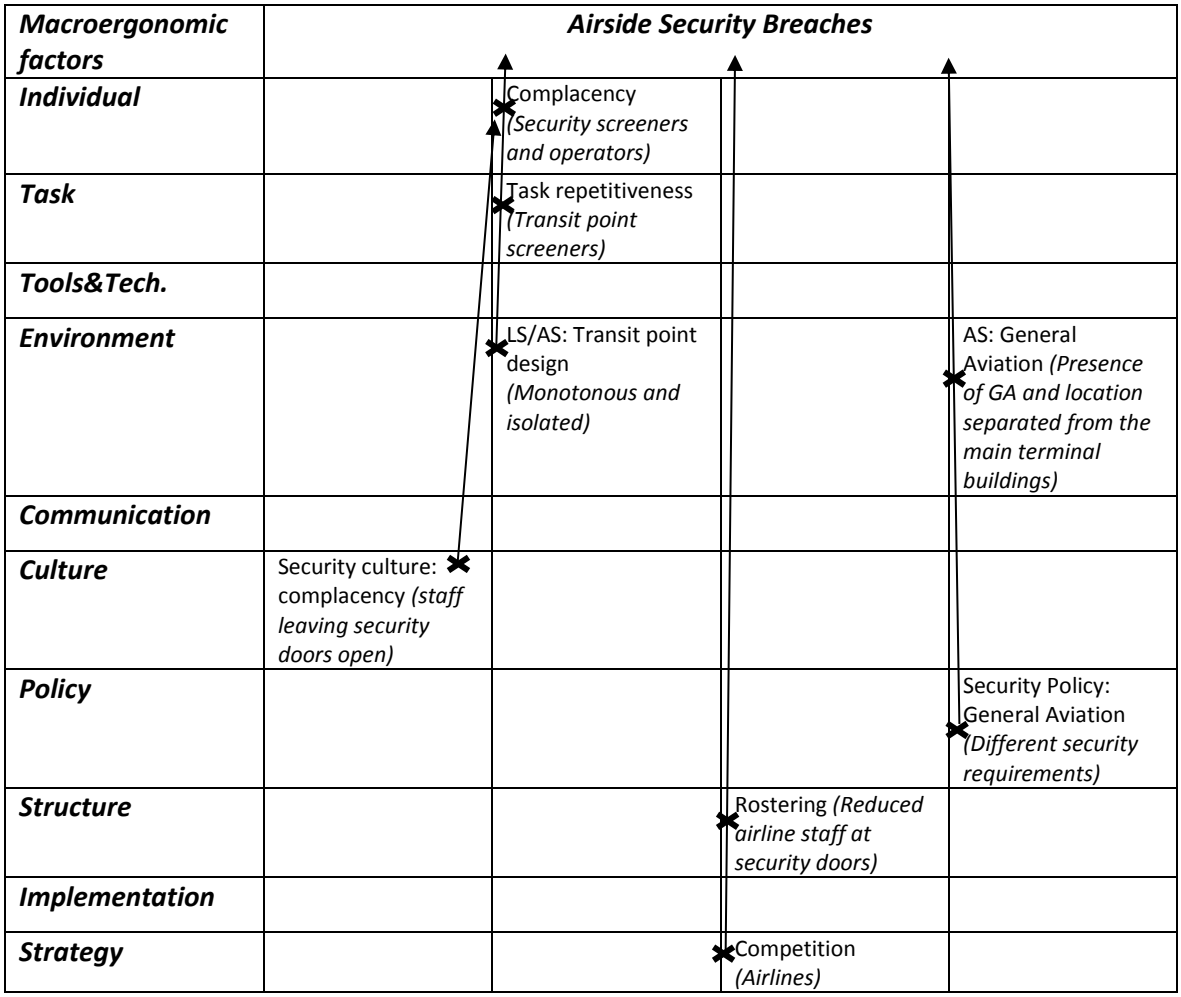

Fig. 2. An example of a potential pathway of vulnerability

Our findings demonstrate that the concept of pathways of vulnerability can be fruitfully applied to different sociotechnical systems, in order to provide insights on how specific safety and security risks may incubate and manifest. After further research in this field of study, theoretical frameworks for a diagnostic assessment of pathways of vulnerability can be elaborated.

4.2. Risk assessment frameworks in the three airports

During document analysis, we reviewed the risk assessment documents of the three airports. The review highlighted that in the three aerodromes safety and security risks are identified, assessed and treated in different ways based on their *likelihood* (ranging from 1, the lowest, to 5, the highest) and *consequences* (from E, the lowest, to A, the highest).

As an example, in Airport X[2], a *rare event* was considered to occur *once in 10 years;* in Airport Y, *less than once in 100 years;* and in Airport Z, *once in 20 or more years.* Similarly, in Airport X, a *major event* was classified as causing *major impact on operations;* in Airport Y, *economic loss between $4.5M and $18M;* and in Airport Z, *economic loss between $10M and $30M.* Furthermore, Airport X had three categories of *risk rating* (and, consequentially, of strategies for intervention), while Airport Y and Airport Z had four (with different definitions). In addition, the examined risk entries had different names and definitions in the three airports and several risks were classified in certain airports, and not in others. The risk assessment matrices originating from this taxonomy of operational risks were in turn different and entailed a non-harmonized classification of risk ratings, as depicted in Fig. 3.

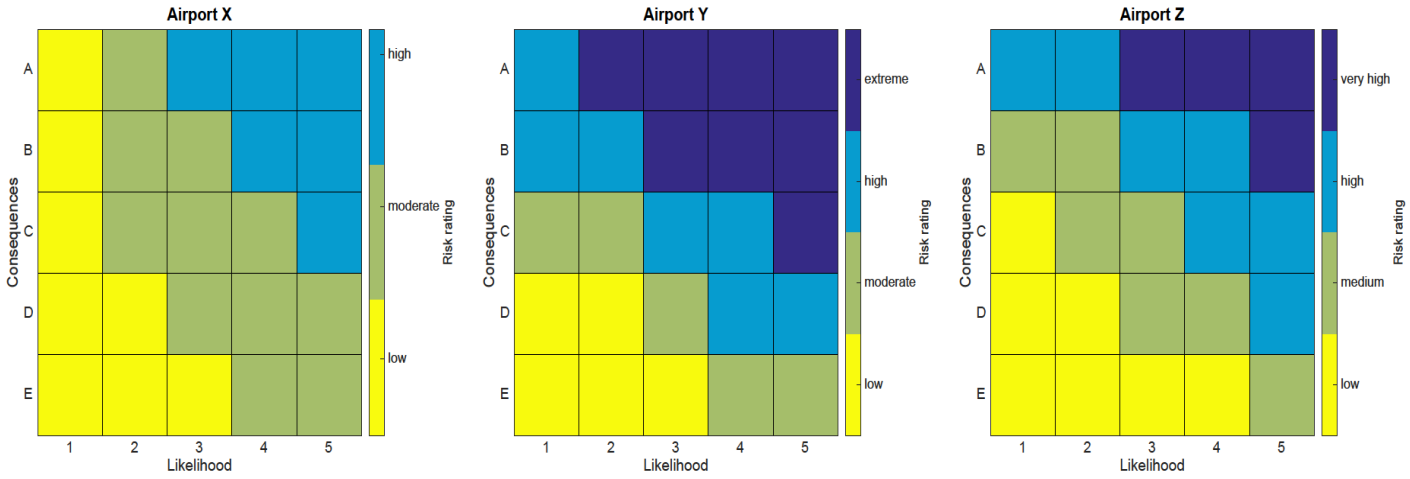

Fig. 3. Risk assessment matrices in the three airports

[2] The three airports are randomly indicated as X, Y, and Z to further protect their identity.

5. DISCUSSION

This research has adopted a hazard-independent approach to organizational vulnerability, encompassing safety as well as security risks as potentially originating from airport operations. This expands the existing literature, which mainly adopts a hazard-dependent approach. Our focus was on the characteristics of the object of vulnerability (the airports), regardless of the context, a perspective rarely adopted in the literature. In defining the overall level of vulnerability, we considered the crucial role of the interaction between the human (individual level) and the systemic features (organizational level) of airports.

This study has emphasized that multiple triggers of vulnerability stem from the 10 MeA categories: individual, task, tools and technology, environment, and organization (communication, culture, policy, structure, implementation, and strategy). Supporting existing studies (Drennan et al., 2014; Smith, 2004, 2005), our results revealed the potential for these factors to converge along preferential development corridors, where one or more features can generate another one (or others) until impacting individuals' performance and ultimately creating conditions for safety and security risks to materialize. An example of this were the airside breaches – representing a type of security risk potentially deriving from a combination of *individual factors* (complacency by operators), *task factors* (task repetitiveness), *environment factors* (design of landside/airside transit points), and *culture factors* (an organizational culture potentially complacent towards security doors left open). The present research expands the existing literature on pathways of vulnerability by exploring the most relevant pathways in an international airport environment. Our investigation has also supported Kraemer and Carayon's illustration of the individual factors as the closest determinants for human error potentially leading to disruptions (2007).

The results of this study have significant implications for the management of safe and secure operations in modern airports. Our findings highlight the potential impact that the airport (in terms of infrastructure and *ensemble* of organizations) can have on safety and security risks,

as indicated in the literature. Scholarly examples include in particular geographical location of airports (Jaques, 2010), infrastructural features that influence the presence of safety risks (Wilke, Majumdar, & Ochieng, 2015), company management and regulations (Johnson & Holloway, 2004; Pettersen & Bjørnskau, 2015), organizational change and structure (e.g., the role of sub-contracts in maintenance operations) (de Gramatica, Massacci, Shim, Turhan, & Williams, 2016; Herrera, Nordskag, Myhre, & Halvorsen, 2009), and others.

Besides an original recollection of pathways for safety and security risks, our investigation identified some transversal, recurring themes worth further exploration (the sub-categories of the MeA factors). An example is the implementation of a low-cost business model by some traditional airlines, besides the low-cost carriers. The case study revealed several potentially pertinent safety and security performance issues related to this business model. For example, from the data emerged themes related to tight or under-staffing and the use of complex contractual arrangements in outsourcing various functions to contractors. While common, these actions potentially expose airports to vulnerability as it becomes more difficult to ensure tight controls across the functions. As identified in a separate theme, these structural or resource-based issues potentially have a flow-on effect reflected by concern in ensuring that contractors had received the required and adequate training. Analysis of the data further revealed a theme related to time pressure and efficiency reflecting the cost of operations in airports. Indeed, high levels of pressure and time constraints are consistently demonstrated antecedents of accidents and errors in the workplace and airports via increased stress and frustration (Janic, 2000). Overall, these findings highlight the need for airport operators to develop protocols and systems that take account of the way airlines are increasingly organizing their business. Airport management is clearly required to balance multiple sources of vulnerability as it seeks to ensure compliance with safety and security regulations.

Understanding the dynamics that characterize the incubation, development and manifestation of organizational vulnerability is the basis for producing diagnostic frameworks for assessment of pathways of vulnerability in airports. Such frameworks can be used to conduct audits on airport operations. For training purposes, the contents of these audits can be shared within airport organizations. This is expected to raise operators and supervisors' awareness around the potential consequences that their actions, as well as the practices, attitudes, and behaviors executed in their organizations, can have in terms of safe and secure operations. The graphic representation in which the pathways of vulnerability have been depicted (Fig. 2) was inspired by the *accident causation models* present in the literature (Salmon, Cornelissen, & Trotter, 2012; Underwood & Waterson, 2014). Grid-type of representations of accident causation can be fruitfully utilized to map the MeA factors for organizational vulnerability in sociotechnical systems.

The present research has also highlighted that the pathways themselves are not a condition sufficient to make safety and security risks real. Triggering events such as human errors or criminal intentions have to occur in order to lead to an actual disturbance in the airport system. In this last case, latent pathways are exposed after the event has occurred, making prevention efforts useless. In order to further investigate the dynamics of pathways of vulnerability, we recommend complementing our approach with a hazard-dependent perspective which focuses on the nature of triggering events.

This study suggests that the MeA could be an appropriate model to use at international airports when conducting internal audits aimed at improving their safety and security systems as it could provide a/another useful lens from which to understand vulnerability. By so doing, airport organizations may be better able to proactively tackle the weaknesses that exist in their individual and managerial practices, attitudes, and behaviors. An assessment of the airports' environment against the 10 MeA categories could enable safety and security managers in

airports to more holistically scan their work systems without neglecting any sub-system. This could eventually allow the adoption of proactive measures to prevent or mitigate safety and security risks.

The absence of specific patterns in the identification of safety or security risks within the four units of analysis (LL, CML, OML, and SSP/AFP) supports the notion that the interviewed airport managers had a systemic vision of their working environment in terms of safety and security performance. Regardless of their hierarchical level, they displayed knowledge of the airport system and avoided focusing exclusively on their area of competence. A general manager could discuss very operational events and *vice versa* an operational manager could perceive very systemic disturbances to be relevant. Further research is suggested in this area, but a preliminary consideration can be drawn from the present research: airport management in Australia enforces a culture of engagement to safety and security at all hierarchical levels of the explored airport organizations.

The present paper has emphasized that a common framework to conduct risk assessment is not applied in the explored airports. In aviation, dissimilarities in the assessment of *risk likelihood* and *risk consequences* (and therefore also in the resulting *risk rating*) are expected and understandable. One could question that the different categories of likelihood and consequences have different definitions due to the diverse size of the airports, in terms of passengers, aircraft movements, revenues, etc. Based on this, in larger airports risks could be more likely, due to the increased number of movements and passengers[3]. At the same time, their consequences could be more relevant due to the higher economic value. Thus, a *major event* in Airport X may correspond to a *minor event* in Airport Z, and so on. For example, an airport surrounded by forests or other natural features is expected to have a different assessment

[3] Yet, this argument is true only in theory. Findings from this study highlight that the classification of *likelihood* does not follow this pattern and the very same event is not considered more likely in the biggest airport than in the smallest one.

of bird strike risks than an urban airport. Similarly, estimated consequences of a runway incursion in a busy international airport are supposed to be *naturally* different from those in a small regional aerodrome.

However, differences in risk assessment should be limited to estimates of likelihood and consequences and not also include the criteria against which this assessment is conducted. The introduction in the definition of likelihood and consequences of a weighting coefficient based on the airport category would maintain the individual characteristics of airports (size, revenues, movements, etc.) by nonetheless preserving comparability of risk assessment frameworks among the different airports. In general, the limitations of risk assessment frameworks (e.g., matrices, landscapes) have been discussed in the literature, to the point that Aven and Cox (2016) suggest that these tools should not be used for risk policy planning and resource allocation. Our study confirms this stance. However, we consider common risk assessment frameworks as the starting point to at least facilitate the sharing of best practices among airports. Airports need to come to agreed definitions of *risk likelihood* and *risk consequences*¸ so that *risk ratings* and intervention strategies are consistent throughout a country. A second, more ambitious step would be the elaboration of common risk entries organized around similar macro-categories of risks. In this way, a specific risk would have the same name and characteristics in all airports, which would improve comparability and information sharing.

5.1. Synthesis of practical contributions of the study

While in its infancy, the framework proposed in the present paper can be further tested (e.g., with quantitative methods or in other countries than Australia), with a view to being applied in airports. Despite this infancy, the findings of this paper have potential for practical application in a number of ways. First, the results promote the need to classify the most relevant safety and security risks for airports, and provide guidance to do so. Second, this paper supports

the utilization of the MeA as a blueprint to scan the organizational environment and flag, from the safety and security risks, the potential determinants of vulnerability across the 10 MeA categories. This approach can be utilized to conduct internal and/or external safety and security audits, possibly involving staff from different airports to leverage outsiders' perspective. Third, this method facilitates the development of hypotheses relating to pathways of vulnerability, by establishing connections among the identified determinants (e.g., if it is proved that *task repetitiveness* is a determinant of *complacency* in safety and security operators, the former can be associated with an increased potential for *airside breaches*). Furthermore, strategies and interventions to mitigate vulnerability can be developed by prioritizing the pathways of vulnerability that seem more likely and potentially more impactful.

As a final caveat, an agreed risk assessment framework across airports is a fundamental condition for testing the proposed framework across multiple airports. This requires establishment of common definitions of likelihood and consequences, common numerical standards for assessment, common definitions of risks, and common risk categories (see Section 4.2), as suggested in prior literature (Aven & Cox, 2016).

5.2. Limitations and future research

This research has some methodological limitations. As a qualitative study on safety and security risk perceptions, our research investigated airport risks as perceived, and described, by interviewees. This was necessary as Australian aviation has yet to record significant safety and security events, which is undeniably positive from an operational perspective, but also dramatically reduces available data to build a standardised method for the analysis of sociotechnical risk factors. Our study constitutes an *exploratory* attempt (Babbie, 2013) to cast light on the determinants of organizational vulnerability, towards establishing an epidemiology of safety and security risks in airports. We recommend therefore further sociotechnical investigation to further validate the findings from our investigation. Furthermore, our scope of

investigation was limited to organizational factors internal to the explored airports, with environmental factors only marginally assessed by the adopted framework. This last point does not diminish the relevance that surrounding economic, social, legal and political influences can have on the formation of pathways of vulnerability. An additional limitation of this exploration resides in the confidential nature of the collected data. This circumscribed the amount of information that could be used, namely respondents' personal data (e.g., job title, degree of experience, etc.). Lastly, our exploration focused on the perspective of airport management, a limitation in our study. Further research is necessary to gauge risk perceptions from the viewpoint of other fundamental players in the airport environment: airlines, retailers, travelers and general public.

The present research builds on the scarce academic literature on the vulnerability of modern airports. We believe that further studies are necessary in this area. A plausible avenue for investigation is an integrated approach between vulnerability assessment and resilience building. The ultimate goal of the present, and other, studies on sociotechnical systems is the reduction of their vulnerability to service disruptions. Vulnerability reduction leads to reduced likelihood and/or consequences of disruptions and increased resilience (Sheffi & Rice Jr, 2005). This integrated vulnerability-resilience field of research has been extensively investigated in the domain of supply chain management (Kim, Chen, & Linderman, 2015; Sheffi, 2015; Sheffi & Rice Jr, 2005; Speier, Whipple, Closs, & Voss, 2011) which can teach significant lessons to aviation management. The concept of *detection lead time* (the latency between the acknowledgement of a disruptive event and its first impact; (Sheffi, 2015)) suggests aviation risk managers to not focus only on mitigating the consequences of an event or operating to reduce its probability, but also to improve organizational capabilities to *'sense'* early warnings of an impending disruption. Digital technologies are indicated as a powerful instrument to improve early detection of disruptive events, and reduce vulnerability together

with increasing resilience, by building organic capabilities to sense threats and respond quickly. This has been investigated in a range of domains and practical examples include financial risk (Koyuncugil & Ozgulbas, 2010), emergency management (Pohl, Bouchachia, & Hellwagner, 2015), terrorism (Drozdova & Samoilov, 2010), and natural hazards (Asimakopoulou, 2010).

Despite their role, digital technologies should not be regarded as the ultimate solution to anticipate crises in airports. Adopting this stance would entail supporting the classic aviation safety and security models which consider airports as mass production organizations where human behaviors follow rational and logical pathways (Kirschenbaum, 2015). Technology and logistics are the crucial components of aviation facilities designed based on the aforementioned approach, a mass processing engineering perspective (Horonjeff, 2010), which neglects that airports are made of complex and interdependent groups of decision-makers (Remawi, Bates, & Dix, 2011).

The reality of human behavior indicates that safety and security decision-making in airports must take into account the human factor. This supports the argument that airport decision-making cannot be reduced to a *'simple-man-machine single-individual interaction'* (Kirschenbaum, 2015, p. 35).

6. CONCLUSION

Despite its relevance, the field of vulnerability of global aviation networks to safety and security risks lacks a structured, holistic body of knowledge that goes beyond *ad hoc* studies conducted in the aftermath of extreme events. The present investigation on the pathways of vulnerability that have the potential, in international airports, to generate safety and security risks is one of the first attempts to build such body of knowledge. We adopted a hazard-independent perspective that allowed us to focus on the organizational features of the explored airports and assess potential determinants for both safety and security disruptions. Our research supports and expands the theory on pathways of vulnerability and provides practical suggestions for aviation practitioners to improve their early detection capabilities.

ACKNOWLEDGMENTS

This research was a part of the work undertaken by the project "Airports of the Future" (LP0990135), a multi-disciplinary international collaborative research project exploring the complexity of modern airports and addressing conflicts between aviation security and the passenger experience, funded by the Australian Research Council Linkage Project scheme. The project was carried out during Ivano Bongiovanni's appointment with the School of Management, Queensland University of Technology (Brisbane, QLD, Australia). The authors would like to thank two anonymous reviewers for their precious feedback on the paper.

REFERENCES

Asimakopoulou, E. (2010). *Advanced ICTs for Disaster Management and Threat Detection: Collaborative and Distributed Frameworks: Collaborative and Distributed Frameworks*. Hershey, NY: IGI Global.

Aven, T., & Cox, L. A. (2016). National and Global Risk Studies: How Can the Field of Risk Analysis Contribute? *Risk Analysis, 36*(2), 186-190. doi: 10.1111/risa.12584

Babbie, E. R. (2013). *The practice of social research* (13th ed.). Belmont, Cal: Wadsworth - Cengage Learning.

Bouchon, S. (2006). *The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of the Art* (pp. 99). Retrieved from http://bookshop.europa.eu/en/the-vulnerability-of-interdependent-critical-infrastructures-systems-pbLBNA22205/

Boyer, K. K., & Pronovost, P. (2010). What medicine can teach operations: What operations can teach medicine. *Journal of Operations Management, 28*(5), 367-371. doi: http://dx.doi.org/10.1016/j.jom.2010.08.002

Carayon, P., Schoofs Hundt, A., Karsh, B. T., Gurses, A. P., Alvarado, C. J., Smith, M. J., & Flatley Brennan, P. (2006). Work system design for patient safety: the SEIPS model. *Quality and Safety in Health Care, 15*(suppl 1), i50-i58. doi: 10.1136/qshc.2005.015842

Carayon, P., & Smith, M. J. (2000). Work organization and ergonomics. *Applied Ergonomics, 31*(6), 649-662. doi: http://dx.doi.org/10.1016/S0003-6870(00)00040-5

de Gramatica, M., Massacci, F., Shim, W., Turhan, U., & Williams, J. (2016). Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training: Agency Problems and Airport Security. *Risk Analysis*, n/a-n/a. doi: 10.1111/risa.12607

Dow, K. (1992). Exploring Differences in Our Common Future(S) - the Meaning of Vulnerability to Global Environmental-Change. *Geoforum, 23*(3), 417-436. doi: 10.1016/0016-7185(92)90052-6

Drennan, L. T., McConnell, A., & Stark, A. (2014). *Risk and crisis management in the public sector*: Routledge.

Drozdova, K., & Samoilov, M. (2010). Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations. *Computational and Mathematical Organization Theory, 16*(1), 61-88.

England, J., Agarwal, J., & Blockley, D. (2008). The vulnerability of structures to unforeseen events. *Computers & Structures, 86*(10), 1042-1051. doi: http://dx.doi.org/10.1016/j.compstruc.2007.05.039

Füssel, H.-M. (2007). Vulnerability: a generally applicable conceptual framework for climate change research. *Global Environmental Change, 17*(2), 155-167.

Hendrick, H. W. (1998). *Macroergonomics: A Systems Approach for Dramatically Improving Occupational Health, Safety and Productivity.* Paper presented at the Advances in Occupational Ergonomics and Safety: Proceedings of the XIIIth Annual International Occupational Ergonomics and Safety Conference 1998.

Hendrick, H. W., & Kleiner, B. M. (2001). *Macroergonomics: an introduction to work system design*. Santa Monica, CA: Human Factors and Ergonomics Society.

Hendrick, H. W., & Kleiner, B. M. (2002). *Macroergonomics: theory, methods, and applications*. Mahwah, NJ: Lawrence Erlbaum Associates.

Herrera, I. A., Nordskag, A. O., Myhre, G., & Halvorsen, K. (2009). Aviation safety and maintenance under major organizational changes, investigating non-existing accidents. *Accident Analysis and Prevention, 41*(6), 1155-1163. doi: 10.1016/j.aap.2008.06.007

Horonjeff, R. (2010). *Planning and design of airports* (Vol. 5th). New York: McGraw-Hill.

International Air Transport Association. (2014). New IATA Passenger Forecast Reveals Fast-Growing Markets of the Future. Retrieved September 6th, 2016, from http://www.iata.org/pressroom/pr/Pages/2014-10-16-01.aspx

Janic, M. (2000). An assessment of risk and safety in civil aviation. *Journal of Air Transport Management, 6*(1), 43-50. doi: 10.1016/S0969-6997(99)00021-6

Jaques, T. (2010). Embedding issue management as a strategic element of crisis prevention. *Disaster Prevention and Management, 19*(4), 469-482. doi: http://dx.doi.org/10.1108/09653561011070385

Johnson, C. W., & Holloway, C. M. (2004, 2004). *Distribution of Causes in Selected US Aviation Accident Reports Between 1996 and 2003.* Paper presented at the 22nd International System Safety Conference, Providence, RI.

Kim, Y., Chen, Y.-S., & Linderman, K. (2015). Supply network disruption and resilience: A network structural perspective. *Journal of Operations Management, 33*, 43-59.

Kirschenbaum, A. A. (2015). The social foundations of airport security. *Journal of Air Transport Management, 48*, 34-41.

Knox, H., O'Doherty, D., Vurdubakis, T., & Westrup, C. (2008). Enacting Airports: Space, Movement and Modes of Ordering. *Organization, 15*(6), 869-888. doi: 10.1177/1350508408095818

Koyuncugil, A. S., & Ozgulbas, N. (2010). *Surveillance Technologies and Early Warning Systems: Data Mining Applications for Risk Detection: Data Mining Applications for Risk Detection*. Hershey, NY: IGI Global.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154. doi: http://dx.doi.org/10.1016/j.apergo.2006.03.010

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520. doi: 10.1016/j.cose.2009.04.006

Lalonde, C., & Roux-Dufort, C. (2010). Crisis Management in Institutional Healthcare Settings: From punitive to emancipatory solutions. *Organization Development Journal, 28*(1), 19-36.

Landis, J. R., & Koch, G. G. (1977). An Application of Hierarchical Kappa-type Statistics in the Assessment of Majority Agreement among Multiple Observers. *Biometrics, 33*(2), 363-374. doi: 10.2307/2529786

Lewis, J. (1999). *Development in disaster-prone places: studies of vulnerability*. London: Intermediate Technology.

Li, S., & Xu, X. (2015). Vulnerability analysis for airport networks based on fuzzy soft sets: From the structural and functional perspective. *Chinese Journal of Aeronautics, 28*(3), 780-788. doi: http://dx.doi.org/10.1016/j.cja.2015.04.002

Lopez, A. (2016). Vulnerability of Airports on Climate Change: An Assessment Methodology. *Transportation Research Procedia, 14*, 24-31. doi: http://dx.doi.org/10.1016/j.trpro.2016.05.037

Lord, S., Nunes-Vaz, R., Filinkov, A., & Crane, G. (2010). Airport front-of-house vulnerabilities and mitigation options. *Journal of Transportation Security, 3*(3), 149-177.

Marshall, C., & Rossman, G. B. (2011). *Designing qualitative research* (5th ed.). Thousand Oaks, CA: Sage Publications.

McEntire, D. (2001). Triggering agents, vulnerabilities and disaster reduction: towards a holistic paradigm. *Disaster Prevention and Management, 10*(3), 189-196. doi: 10.1108/09653560110395359

McEntire, D. (2004). Tenets of vulnerability: an assessment of a fundamental disaster concept. *Journal of Emergency Management, 2*(2), 23-29.

McEntire, D., Gilmore Crocker, C., & Peters, E. (2010). Addressing vulnerability through an integrated approach. *International Journal of Disaster Resilience in the Built Environment, 1*(1), 50-64. doi: 10.1108/17595901011026472

Murphy, L. A., Robertson, M. M., & Carayon, P. (2014). The next generation of macroergonomics: Integrating safety climate. *Accident Analysis & Prevention, 68*, 16-24. doi: http://dx.doi.org/10.1016/j.aap.2013.11.011

Nash, J. M., Agnew, R., Ward, S., Massey, R., Callister, T., Mcneill, R., . . . Tolton, E. (2012). *Guidebook for Airport Irregular Operations (IROPS) Contingency Planning* (Vol. 65). Washington, DC: Airport Cooperative Research Program.

Netjasov, F., & Janic, M. (2008). A review of research on risk and safety modelling in civil aviation. *Journal of Air Transport Management, 14*(4), 213-220. doi: http://dx.doi.org/10.1016/j.jairtraman.2008.04.008

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Pettersen, K. A., & Bjørnskau, T. (2015). Organizational contradictions between safety and security – Perceived challenges and ways of integrating critical infrastructure protection in civil aviation. *Safety Science, 71*, 167-177. doi: https://doi.org/10.1016/j.ssci.2014.04.018

Pohl, D., Bouchachia, A., & Hellwagner, H. (2015). Social media for crisis management: clustering approaches for sub-event detection. *Multimedia Tools and Applications, 74*(11), 3901-3932.

Punch, S. (2012). Hidden struggles of fieldwork: Exploring the role and use of field diaries. *Emotion, Space and Society, 5*(2), 86-93. doi: 10.1016/j.emospa.2010.09.005

Reason, J. T. (1990). *Human error*. Cambridge: Cambridge University Press.

Remawi, H., Bates, P., & Dix, I. (2011). The relationship between the implementation of a Safety Management System and the attitudes of employees towards unsafe acts in aviation. *Safety Science, 49*(5), 625-632.

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science, 50*(4), 1158-1170. doi: http://dx.doi.org/10.1016/j.ssci.2011.11.009

Shafieezadeh, A., Cha, E., & Ellingwood, B. (2015). A Decision Framework for Managing Risk to Airports from Terrorist Attack. *Risk Analysis, 35*(2), 292-306. doi: 10.1111/risa.12266

Sheffi, Y. (2015). Preparing for disruptions through early detection. *MIT Sloan management review, 57*(1), 31.

Sheffi, Y., & Rice Jr, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan management review, 47*(1), 41.

Smith, D. (1990a). Beyond contingency planning: Towards a model of crisis management. *Organization & Environment, 4*(4), 263-275.

Smith, D. (1990b). Corporate power and the politics of uncertainty: risk management at the Canvey Island complex. *Industrial Crisis Quarterly, 4*(1), 1-26.

Smith, D. (1995). The dark side of excellence: managing strategic failures. In J. Thompson (Ed.), *Handbook of strategic management* (pp. 161-191). Oxford, UK: Butterworth-Heinemann.

Smith, D. (2000). On a wing and a prayer? Exploring the human components of technological failure. *Systems Research and Behavioral Science, 17*(6), 543-559.

Smith, D. (2004). For Whom the Bell Tolls: Imagining Accidents and the Development of Crisis Simulation in Organizations. *Simulation & Gaming, 35*(3), 347-362. doi: 10.1177/1046878104266295

Smith, D. (2005). Business (not) as usual: crisis management, service recovery and the vulnerability of organisations. *Journal of Services Marketing, 19*(5), 309-320. doi: 10.1108/08876040510609925

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations: Mitigating product safety and security risks. *Journal of Operations Management, 29*(7), 721-736.

Stave, K. A., & Kopainsky, B. (2015). A system dynamics approach for examining mechanisms and pathways of food supply vulnerability. *Journal of Environmental Studies and Sciences, 5*(3), 321-336. doi: 10.1007/s13412-015-0289-x

Stewart, M., & Mueller, J. (2013). Terrorism Risks and Cost-Benefit Analysis of Aviation Security. *Risk Analysis, 33*(5), 893-908. doi: 10.1111/j.1539-6924.2012.01905.x

Stewart, M., & Mueller, J. (2014). A risk and cost–benefit analysis of police counter-terrorism operations at Australian airports. *Journal of Policing, Intelligence and Counter Terrorism, 9*(2), 98-116. doi: 10.1080/18335330.2014.940816

Tran, Q. H. A., & Namatame, A. (2015). Worldwide aviation network vulnerability analysis: a complex network approach. *Evolutionary and Institutional Economics Review, 12*(2), 349-373. doi: 10.1007/s40844-015-0025-y

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly, 21*(3), 378. doi: 10.2307/2391850

Turner, B. A., & Pidgeon, N. F. (1978). *Man-made disasters*. London: Wykeham Publications.

Underwood, P., & Waterson, P. (2014). Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. *Accident Analysis & Prevention, 68*, 75-94. doi: http://dx.doi.org/10.1016/j.aap.2013.07.027

White, G. F. (1974). *Natural hazards, local, national, global*. New York: Oxford University Press.

Wilke, S., Majumdar, A., & Ochieng, W. Y. (2015). The impact of airport characteristics on airport surface accidents and incidents. *Journal of Safety Research, 53*, 63-75. doi: http://dx.doi.org/10.1016/j.jsr.2015.03.006