Journal of Transportation Security (2023) 16:12
https://doi.org/10.1007/s12198-023-00257-1

A new inter-disciplinary relationship: introducing self-organized criticality to failures in aviation security

Paul McFarlane[1]

Received: 9 September 2022 / Accepted: 6 December 2022 / Published online: 16 November 2023

Abstract

This paper introduces the concept of self-organized criticality (SOC) to research on, and debates about, preventing the occurrence of human-mediated failures in aviation security. It aims to persuade readers (policymakers, security professionals, and academics) from different fields that this is a good topic for further research and one that is worth pursuing. This paper views aviation security as a complex system that produces risky behaviors because of chance interactions between many forms of human error. By rethinking the Bak-Tang-Wiesenfeld (BTW) sandpile model, the paper uses the explanatory nature of SOC to explore whether criticality may be viewed as a crucial component of aviation security. It elaborates on the effects of arbitrary interactions between various types of error using the BTW sandpile model's illustrative characteristics. The paper concludes by speculating that SOC can be used to generate new ways of thinking about interventions to mitigate failure and that academics and security professionals from various fields could collaborate to develop fresh ideas and integrated concepts to further our understanding of a crucial subject for the aviation industry.

Keywords Aviation security · Self-organized criticality · Complex systems · Human error · Risk management

Introduction

The concept of self-organized criticality (SOC), developed by Bak et al. (1987), is introduced to discussions on the occurrence of human-mediated failures in aviation security (e.g., McFarlane 2020a for a comprehensive review of the linkages between aviation security failures and human-mediated errors). This conceptual paper also suggests a number of new directions for further interdisciplinary study on this crucial subject. The aviation industry spends more than $50 billion

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

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

annually to improve the security system's capacity to prevent terrorist assaults (Stewart and Mueller 2018). Despite this investment, terrorists have continued to take advantage of weaknesses that are hidden in the different levels of the system. Finding and managing complex failure mechanisms remains a key goal for building a smarter system that is concerned with the recurring risk of failure. Thus, the goal of this paper is to persuade the reader that, despite some problems, this is a good area for research that policymakers, security professionals, and academics from many different fields should look further into.

A thorough conceptual analysis to increase the system's operational effectiveness has not yet been conducted. To provide a more nuanced understanding of the interaction between human-mediated errors and aviation security failures, this paper introduces Bak et al.'s (1987) conception of self-organized criticality (i.e., when a system moves towards a critical point without fine tuning or external adjustment of parameters). It also speculates whether the accumulation of, and the interactions between, human-mediated errors can be said to demonstrate emergent behavior; potentially hazardous behavior that is not predetermined. But, more than this, SOC has an alluringly logical appeal. It is a conceptually stimulating idea that crosses disciplinary boundaries and draws from one of the most provocative ideas to come out of theoretical physics. We have made significant progress in understanding system complexity and dangerous behaviors that take place in many other natural and man-made systems thanks to this explanatory framework. SOC (Bak et al. 1987; Wiesenfeld et al. 1989) gives a complete explanation of how complex dynamical systems (like aviation security) can, without any kind of central control, move toward a critical point where they are about to fail and, just as quickly, safely return to equilibrium when they are jolted out of that critical state.

Although there may be other contributing factors, the primary focus of this paper is on the potential for system failure related to the chance interactions between the occurrence of (human-mediated) errors and faults. By putting the Bak-Tang-Wiesenfeld Sandpile model in a new context, a conceptual link is made that aims to (i) figure out what the possible effects of these interactions might be, (ii) provide some theoretical justification for future risk mitigation and preventing system failures, and (iii) think about whether, from an interdisciplinary point of view, failure modes that can only be seen in hindsight can be found in advance and slowed down before a system failure.

This paper is organized as follows. First, it aims to conceptualize and persuade readers that aviation security may be viewed as a complex system that produces risky behaviors because of chance interactions between many forms of human error and suggests an interdisciplinary approach can help us better understand these behaviors. Second, by rethinking the Bak-Tang-Wiesenfeld (BTW) sandpile model, the paper introduces the explanatory framework of SOC to explore whether criticality might be viewed as a key element of aviation security. Thirdly, it elaborates on the effects of arbitrary interactions between various types of error using the BTW sandpile model's illustrative characteristics. The paper concludes by speculating that SOC can be used to generate new ways of thinking about interventions to mitigate failure and that academics and security professionals from various fields could collaborate to develop fresh ideas and integrated concepts to further our understanding of a crucial subject for the aviation industry.

Why is effective aviation security such a difficult task?

Most people agree that building an effective aviation security system is both an important and challenging task. The global network of civil aviation is extensive and has many facets. The safety of the worldwide commercial air transportation network depends critically on the effective security of air travel; a network that is made up of living and non-living elements that interact with a degree of complexity that is difficult to comprehend. Maintaining good aviation security is, of course, a demanding undertaking. To protect the civil aviation system from terrorists or other potential threat groups, a sophisticated socio-technical system that depends on interactions between a variety of human, organizational, and technical components was created over many decades. The extensive security flaws of 9/11 showed system complexity-related problems. Terrorists exposed unexpected and unforeseen forms of system failure by effectively exploiting flaws in one of the best-defended security systems. These kinds of failure were not novel, despite the system's failure to predict them. They were actually a number of error trajectory pathways (or failure modes) that were able to penetrate all the layers of the system's defenses through the haphazard combination of active errors and latent conditions in ways that were unanticipated by system managers (Reason 1990, 2008).

As such, 9/11 was therefore not an entirely unlikely event. Instead, it was characterized as a well-thought-out occurrence where the system's inability to recognize and promptly respond to warning signals was purposefully exploited. Failure conditions had been developing within the system for many years, despite these numerous warnings. Before 9/11, the system was "blinking red" according to the National Commission on Terrorist Attacks Upon the United States (2004, p.254). This plausible conjecture explains why many warning signs were not recognized as the fatal concoction of latent incubating conditions and active errors that, in the end, caused a complete collapse of all defensive layers. The underlying reason why a priori warnings go unnoticed is that the system can't recognize or understand the random occurrence of human-made mistakes that are hidden in the many layers of defense.

Most of the time, these dangerous system interactions are caused by two different kinds of human errors that can happen in these kinds of systems (Reason 1990; McFarlane 2020a, b). First, 'active' errors may have an immediate impact on how the system functions. These mistakes are frequently connected to the nefarious rule-breaking actions of front-line security personnel. For instance, when airport security staff willfully violate operating policies and procedures at passenger screening checkpoints, such as failing to react when an alarm is activated or improperly searching passengers or their hand luggage (as happened at Washington Dulles Airport during the 9/11 attacks).[1] On the other hand, 'latent' errors are less noticeable. They are conceived at the top levels of the organisation. Latent errors are more dangerous because they can be hidden by

[1] For clarity, the FAA did not prohibit box cutters and knives under 4 in. in US airports. Each each airline was responsible for its own security. Box cutters and knives under four inches in length were prohibited by the airline industry and not by law. However, security officers were required to address all alarm activations at passenger screening checkpoints and not allow passengers to progress until the cause was identified.

wrong ideas about how and why high-level decisions are made. These procedures can involve defining system risk; managing system design, operation, management, and maintenance; selecting and hiring personnel; providing appropriate training programs; and overseeing security personnel (Reason 1990, 1997, 2008; McFarlane 2020a, b). Due to the 'human' dimension of system failures, minimizing their effect by directing interventions at lowering the occurrence of active errors made by human operators presents certain challenges. When systems are poorly designed, installed, maintained, or managed, faults are invariably passed on to the human operators (Reason 1990).

To gain a better understanding of human error and system failure, Reason's (1997) 'Swiss Cheese' metaphor can be used to describe the important link between latent conditions and active errors. The metaphor explains, in general, that the precise form of the interplay between latent conditions and active errors is random and extremely unpredictable. When latent conditions and active errors combine to generate an error pathway across the system's layered defenses (think slices of cheese lined up together), there are numerous unknown components and variables involved. In this scenario, the holes in the cheese slices can be interpreted as latent conditions and active errors. The system defenses can be violated when the holes all line up to establish an error pathway through the layers (McFarlane 2020a). This pathway is dependent on so many unknown variables. The holes in the cheese are "in reality […] shifting around, coming and going, shrinking and expanding in response to operator actions and local demands" (Reason 1997, p.9). Without deliberate violations, the likelihood of a trajectory path, or a human-mediated mechanism of failure, that penetrates the many layers of a system is exceedingly remote (Reason 1990). As a result, the intention behind the violation is an important factor that influences the likelihood of reducing the prevalence of human-mediated error pathways. Violations are deliberate "deviations from those practices deemed necessary (by designers, managers and regulatory agencies) to maintain the safe operation of a […] system" (Reason 1990, p.195). Even if a rule is broken on purpose, the bad result isn't always foreseen at the time of the first violation (again, we saw this on 9/11 when security staff didn't resolve why the walk-through metal detector alarms were going off even though operating policy dictated that they should have done so) (Reason et al. 1998; Reason 2008).

There is only a limited body of empirical and theoretical knowledge that broadly speaks to the operational effects of these complex relationships, i.e., the outcome of the interaction in aviation security systems between kinds of human-mediated errors and exploitable failure modes (cf. McFadden and Towell 1999; Wiegmann and Shappell 2001a, b; Kraemer et al. 2009; Liang et al. 2010; Kirschenbaum et al. 2012; Kirschenbaum and Mariani 2012; Chiu and Hsieh 2016; Arcúrio et al. 2018). These effects, as well as the system processes and contributing mechanisms connected to their occurrence, are difficult to define and explain. Additionally, there has not been a concerted attempt to realize the advantages of contributions from across disciplines, and as a result, policymakers and industry professionals do not yet fully comprehend the theoretical and practical ramifications of these human-mediated interactions (McFarlane 2014, 2020a).

An interdisciplinary perspective: Aviation security is best understood as a complex socio-technical system

Herein lies the problem: unless we change the way we approach this crucial issue of how the system can anticipate and control human-mediated modes of failure, there will inevitably be more terrorist attacks in the future rather than fewer. It is thus surprising that the literature to date on this subject has not clarified the high-level advantages of conceptualizing aviation security as a complex socio-technical system, especially in comparison to other high-risk industries. As a result, by highlighting some of them in this paper, we hope to convince the reader of the advantages of such an interdisciplinary approach. First, by acknowledging that these systems are high-impact, hard-to-understand, and heavy on technology and their failure has wide-ranging ramifications for society, politics, and the economy (Wladawsky-Berger 2012). Second, understanding that bottom-up, simple conditions can have an impact on complicated systems is crucial. Because of this, random interactions between system elements can result in self-organizing emergent behavior, which is dangerous, unpredictable, and challenging for the system to comprehend (Mitchell 2011). Third, a variety of methodological techniques can be used to study the impact of these interactions (see Mandelbrot 1983; Flake 1998; Boccara 2004; Miller and Page 2007; Mitchell 2011 for a comprehensive review). Modelling these interactions from the bottom up can offer a more detailed understanding of the dynamics and behavior of the system without having to rely on intricate mathematics (Bonabeau 2002; Macy and Willer 2002). Oversimplification makes it harder to show how the real world is, but it doesn't stop these simplifications from giving useful ideas about the problems being studied (Lustick and Miodownik 2000; Lustick et al. 2004).

Introducing self-organized criticality: Using a concept from theoretical physics to explain system failure

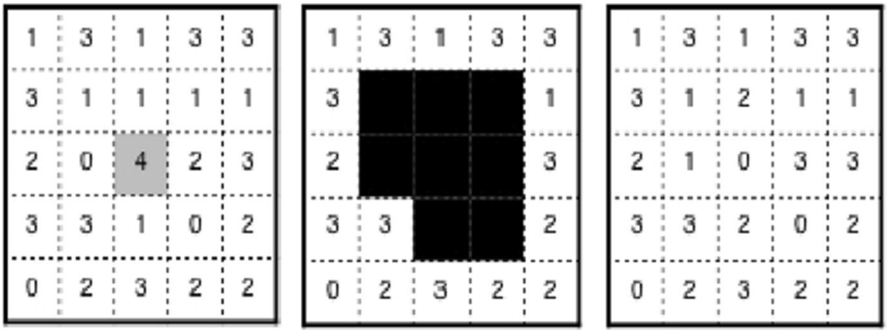
After highlighting some of the benefits of an interdisciplinary approach, it is entirely reasonable to base these thoughts on a broad, yet comprehensive set of concepts organized by the single explanatory mechanism of SOC (Bak et al. 1987). According to Watkins et al. (2016, p.4), SOC has appeared in many other scientific fields, including "statistical mechanics (e.g., Bak et al. 2002), materials science (e.g., Altshuler et al. 2001), condensed matter theory (e.g., Wijngaarden et al. 2006), ecology (e.g., Malamud et al. 1998), evolution (e.g., Sneppen et al. 1995), high energy astrophysics (e.g., Negoro et al. 1995; Dendy et al. 1998; Audard et al. 2000), neuroscience (e.g., Bédard et al. 2006; Chialvo 2010) and sociology (e.g., Hoffmann 2005)". SOC is a "powerful and intriguing" theoretical concept "that potentially has applications to a variety of natural and man-made systems" (Newman 2005, p.22). As a result, the contents of this explanatory device might be supplemented with existing knowledge about the features of aviation security failures covered in this paper, and conceptual linkages could be drawn to them. We may then start to tackle the fascinating interdisciplinary question of whether SOC should be regarded as a core component of aviation security by rethinking the Bak-Tang-Wiesenfeld (BTW) Sandpile model. We will focus on how the theoretical concepts from this model can be related to and used to steer fresh thinking about characteristics associated with the occurrence of human-mediated aviation security failures.

Before we proceed, we will outline the BTW Sandpile model's features. Random sand grains are inserted into a two-dimensional square in this model to reflect compounding human errors and supporting latent conditions (representing an open dynamical system). The sand grains don't move from their starting position. The sandpile's slope, however, steepens as the model advances in time as more and more sand grains are added at random. The slope eventually gets excessively steep, to the point that it is seriously unstable. A minor sand slide or avalanche begins as the next grain of sand is added. The associated collapse randomly distributes sand grains to nearby cells, which in turn raises the height profile of those cells. Sand grains continue to accumulate throughout the process, until the slope once more becomes unstable and collapses. Paradoxically, avalanches can broaden the base, which increases stability, but as the slope of the sandpile increases, adding more single grains of sand leads to more avalanche toppling events. By balancing the amount of sand supplied to that being removed at the margins, this process continues until the sandpile eventually reaches a stationary condition. The sandpile is now at a critical point where it is in a state of self-organized criticality. The size and extent of the next avalanches are unknown, so the future is uncertain, and anything could happen (Bak 1996).

A more formal representation of the Bak-Tang-Wiesenfeld Sandpile model

For the more formally inclined, the Sandpile model is represented by a two-dimensional (L X L) grid square. Each cell on the grid (designated by coordinates (x, y)) is assigned a number (Z (x)) indicating the number of grains present at that location (Z refers to the height of the cell). At the beginning (when t = 0), Z (x, y) = 0 for all x and y. The height Z of the cell at (x, y) is increased by one when a grain of sand is introduced to the grid. At each time step (t + 1), a single grain of sand is added at random to the grid. When a location surpasses the predetermined critical value Zcr, an avalanche toppling event happens and re-distributes sand to each of the neighbouring cells (e.g., if Zcr = 3, when Z = 4, one error is delivered to each of the four neighbours, and the height at the cell where Z (x, y) > Zcr will be reduced by 4). After the avalanche, the height Z of the four adjacent cells increases by one unit of sand. If neighbouring cells are also at the critical value (Z (x, y) = Zcr), more avalanches are initiated across the neighbouring cells. This process continues until all cells are below the crucial height value (Z (x, y) Zcr). Before adding sand units, the model awaits the completion of avalanches. The model then counts the avalanches to determine how many (N(A)) of a particular size there were. The avalanche magnitude is the logarithm (i.e., proportional to a fixed number) of the avalanche's size.

The black squares in Fig. 1 depict the effect of an avalanche caused by an error falling on a cell with Z = 3 and how this causes nine more avalanches to occur. In



1	3	1	3	3
3	1	1	1	1
2	0	4	2	3
3	3	1	0	2
0	2	3	2	2

1	3	1	3	3
3	■	■	■	1
2	■	■	■	3
3	3	■	■	2
0	2	3	2	2

1	3	1	3	3
3	1	2	1	1
2	1	0	3	3
3	3	2	0	2
0	2	3	2	2

Fig. 1 Example of Avalanche and Further Toppling Events

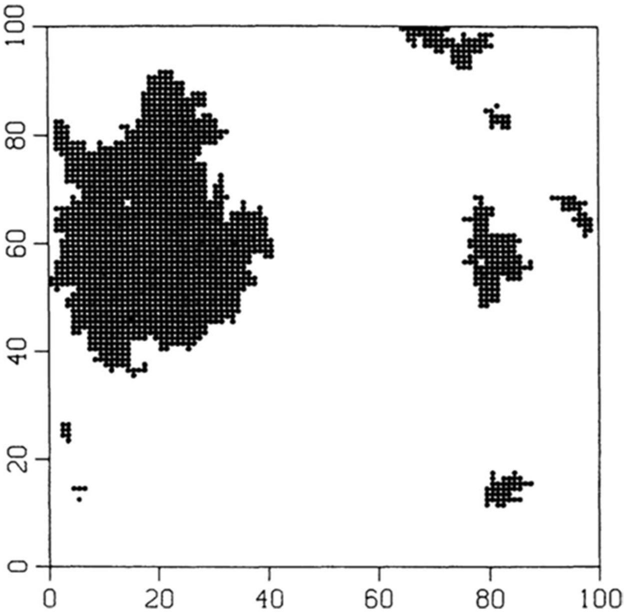


Fig. 2 Avalanches in the Sandpile model triggered by the addition of a single unit of sand. Taken from (Bak et al. 1988)

this instance, the magnitude of the avalanche is s = 9 cells. Figure 2 depicts avalanches caused by the addition of one unit of sand in a computational model. Four parameters can be used to define avalanches: (i) the frequency of toppling events; (ii) the size of the affected area; (iii) the total number of toppling events in the avalanche; and (iv) the lifetime of the avalanche, which is the number of update steps before the grid becomes stable following an avalanche. These output data concerning the frequency, magnitude, and duration of avalanches are used to observe for power-law scaling.

The explanatory function of self-organized criticality and the likelihood of aviation security failures

The ability of SOC to explain system events at critical times is likely its greatest strength when considering the theoretical relevance of the Sandpile model. Critical points become attractors. When a system is disturbed, it will naturally reorganize itself and gradually return to stability (however fleeting this may be). Phase transitions, a transformation process that involves changes from one state to another and where a small change in one variable can have a big impact on the system, specifically occur around the critical point. Nevertheless, precise parameter tweaking is not necessary; changes between phases might occur instantly or gradually over time. A system is said to be at the critical point, or on the verge of chaos, when it is poised, or delicately balanced, halfway between one phase and another.

The assertion that complex systems are on the verge of chaos has significant intellectual appeal (Miller and Page 2007), and it should easily resonate with security system professionals. It establishes the distinction between static and chaotic systems (Ibid.). According to Wolfram (1983, 2002), the behavior on the static-chaotic continuum can be categorized into four types: (i) fixed, (ii) periodic, (iii) chaotic, or (iv) complex. When the behavior is fixed, the system runs in a steady state, and when periodic, it settles into a cyclical pattern that repeats itself indefinitely. Similarly, the system generates random and aperiodic behavior with some pattern and structure in a chaotic state. However, when complex, it is in transition between the periodic and chaotic phases. Even though this final phase has some structure, system behaviors are dangerously difficult to predict (Mitchell 2011; Page 2010; Lamberson and Page 2012). And it is said to be in a state of self-organized criticality when it occupies this subtle zone; a “delicate equilibrium between two extremes of ‘boring’ regularity and ‘noisy’ disorder” (Berto and Taglibue 2012).

Each grid cell in our re-conceptualization of the BTW model symbolizes random components of the security system (e.g., passenger screening checkpoint). Each system component is either error-free at an arbitrary starting point or, more frequently in reality, has an error or latent enabling condition present. Like sand grains, further errors and their enabling conditions are gradually added to the grid over time (these additions should be viewed as human-mediated errors known to occur in socio-technical systems, such as procedural violations, e.g., deliberate rule-breaking by security checkpoint employees when failing to search properly or respond to alarm activations that we know occur from Red Team testing or ineffective supervision of employees performing important tasks). Similar to the real world, faults and error-causing behaviors can become dangerous if left unchecked by supervisory or system processes. Following an avalanche (think disturbance or warning event), errors are redistributed to other areas of the larger system. As more personnel breach the regulations (e.g., due to poor supervision or inadequate training) the consequences are that many additional system components and processes get compromised over time, weakening the system. If the disturbance goes unnoticed, the system restructures and finds its equilibrium again. These events in the model replicate those in a real-world system in which safety feedback mechanisms are not in place to regulate warnings of suboptimal system performance because they are not recognized or comprehended properly. Without efficient intervention (e.g., management controlling rule-breaking behaviors by security personnel), the process keeps on in an unpredictable way, establishing paths that the system doesn't recognize, rendering it continuously susceptible to failure. Security measures for systems are undermined. The system is easy to exploit, which means that terrorists or other threat groups can find holes in the security layers and use them to their advantage.

Self-organized criticality and its implications for aviation security

At various points, human-mediated modes of system failure in aviation security connect to the explanatory character of SOC. For instance, avalanches, or system disturbances like a near miss, could be viewed as leading indicators, potentially signaling an increasing risk of collapse. If these disturbances are accurately perceived and interpreted by the system, they may serve as a warning of a potentially dangerous accumulation of latent conditions and errors. Given the possible effects of these risky interactions, aviation security professionals and policymakers may want to think about the insights that can be used by thinking of criticality as a hidden condition that can affect the system's ability to prevent and stop failures.

The notion that aviation security systems may self-organize into a critical state between multiple types of dynamical behavior could be utilized to inform future preventative strategies and interventions. The circumstances leading up to the 9/11 attacks provide a practical, real-world example of the system organizing into a critical, vulnerable state. The National Commission report concluded that the US government, intelligence agencies, and the FAA were unable to process or understand the significance of critical information. This information included intelligence reporting (from a variety of sources, including signal interception and human agents) warning of the risk of the system defenses being overcome by Islamist terrorists (National Commission 2004). In this case, the available evidence was clear regarding the threat posed by al-Qaeda. In one scenario, a top-level assessment stated that Bin Ladin was plotting multiple operations. Another phone call to the US embassy said that Bin Laden's followers were plotting an attack in the US with powerful explosives (Ibid). These warnings should have alerted the system to the true threat posed by al-Qaeda.

The good news is that, when we return to the explanatory nature of SOC, the system may theoretically be managed in some way to prevent it from moving beyond the critical point, reducing the risk of larger avalanches, i.e., complete system failure. Although the probability of predicting modes of failure is extremely remote, we can speculate that if the system is capable of being controlled in some way to prevent it from moving into a state of disorder, the probability of larger error avalanches (equivalent to the increasing probability of the system failing) could be significantly reduced. If this barrier is overcome, criticality could be exploited to improve system performance in a manner comparable to that of other types of complex systems. Although it may be difficult to interfere with the dynamics of extremely large dissipating events (such as earthquakes and financial systems) in the real world, Cajueiro and Andrade (2013) explain that it may be possible to implement a 'control scheme' that reduces the risk of large events through some form of human control. Controlling (or reverse engineering, as the case may be, the volume of errors within the system and the frequency of their random interaction) the various types of dynamical behavior is also useful in systems where, for optimal performance, designers want them to occupy the space at the critical point, but not to veer to and remain in the chaotic and unpredictable period. Having a level of control could be especially helpful for systems that are close to their failure point. As we saw on 9/11, even small changes in security processes can have big effects on the whole system (Bak et al. 1987).

Experts in security should therefore begin to consider the possibility of creating a control strategy to reduce risk (Cajueiro and Andrade 2013). For example, somewhat ironically, specific types of human control could be applied to reduce the risk of large occurrences (such as creating minor snow avalanches on a mountainside to avoid massive, unanticipated ones). Applying a level of control may be a beneficial mechanism for systems that are finely positioned near a critical point, which, as we now know, can have unpredictable ramifications for the entire system. This mechanism, in theory, would determine the likelihood of avalanches occurring in a specific area or location by scanning for events or warning indicators when the risk of avalanches is thought to be high. To reduce the probability of severe future incidents, the system could trigger externally caused avalanche-type events. One thing to keep in mind regarding this control scheme concept is that it is easier to apply in systems that contain a ‘carrier’ for event propagation (e.g., trees that would otherwise enable the progress of a forest fire). This is not a part of the abstract model used in this paper, but it is very true in the real world, where human operators can easily propagate mistakes around the system (Ibid).

According to SOC, and relevant to future work in this area, identifying the rule or rules that will create complexity is the key to establishing an intervention that is more anticipatory and can enable early detection of errors accumulating within the system prior to the critical point (i.e., move the system between the periodic and chaotic phases). Miller and Page (2007, p.148) explain in their discussion of the edge of chaos that “if we slightly perturb a rule that produces complexity, we will get [another] rule that either generates chaos or stasis.” Consequently, the search for criticality and how to initiate or trigger the dispersion of errors should focus on how small changes in a rule affect its outcome behavior. In other words, for the best performance of the system, we need to figure out which rule or rules can be changed to cause an avalanche on purpose, before the system slowly falls into chaos and causes its own potentially fatal event.

The deliberate instigation of an avalanche in a real-world system would be akin to an intervention that stops the accumulation and interplay of latent circumstances and active errors. Consider the previously cited instance in which terrorists were able to safely board Flight 77 due to the purposeful violation of rules by security personnel at the passenger screening checkpoint at Washington Dulles Airport. Initiating our metaphorical avalanche sooner, when the errors were originally accumulating at the passenger checkpoint, could have prevented the terrorists from completely breaching the system. In this type of scenario, the control mechanism would scan the entire system for risky areas (such as the passenger screening checkpoint, hold baggage, air-side access control) where latent conditions and errors could have been allowed to accumulate, and having done so, would deliberately trigger mitigating action at a point far earlier in the build-up, rather than when too late of its own accord. However, a key challenge for policymakers and aviation security professionals is that the potential benefits of being poised at the edge of criticality will be reduced unless the system reconciles the harmful effect of erroneous perception of how it perceives that it would fail (like that observed before the 9/11 attacks, where the focus was on explosive devices being hidden in hold luggage rather than suicide hijackings) about how it perceives it can fail.

If this challenge can be overcome, criticality could be used to confer an advantage to improve performance in a similar way to that found in other types of complex systems. In our case, accepting that SOC can be applied profitably to human-mediated aviation security failures supports the proposal that aviation security managers become more focused and preoccupied with the prospect of failure. As such, mitigating the risk of security failures in aviation security should be part of an overarching risk management approach that identifies risk and applies control measures to reduce predictable behavior that results from the interplay of human-mediated system errors. Any future integrative approach should focus on reducing the occurrence of random interactions and implementing anticipatory measures to provide foresight and control as the system self-organizes into a state of criticality and avoid it behaving chaotically and unpredictably while in this critical space.

Next steps for inter-disciplinary research on aviation security failures

This paper adds to current discussions by speculating on the applicability of SOC in explaining real-world aviation security failures. SOC can be applied to generate new ways of thinking about interventions or control schemes in this early analysis of these notions. Future controls could be used to minimize the formation of unforeseen risk-laden states by mitigating both the accumulation and interactions of human-mediated errors. But more than that, this paper shows how academics from different scientific disciplines and security professionals from different fields could work together to come up with new ideas and integrated concepts and share knowledge to learn more about an important topic for the aviation industry and people who travel.

This paper also aims to encourage more inter-disciplinary research on human-mediated aviation security failures, which are significant causes of failure in aviation security systems. Future inter-disciplinary research could evaluate experimentally if SOC is a basic property of an effective aviation security system based on the theoretical principles expressed in this paper. A promising area for future study is to re-contextualize the BTW Sandpile model to develop a computational prototype, perhaps agent-based, model to empirically test for evidence of SOC. Researchers would need to develop a coherent set of assumptions to connect any future computational model to empirical data. These data, form real-world occurrences, could be fed into the model to define initial behaviors and rules for agent interactions. Experimental data could be analyzed for evidence of power-law scaling and whether simple rules can be applied to successfully mitigate the consequences of human-mediated errors.

Finally, we know that human-mediated errors contribute to aviation security system failures and that modelling such errors can be difficult. On the other hand, developing new integrative theories and methodologic techniques based on the abstractions presented in this paper has the potential to disclose how to reduce the risk of human-mediated forms of failure. More work from different fields on this topic could also help or drive the development of operational doctrine, protocols, and practical interventions by others in an important area of transportation security.

Authors' contributions Conceptualising, drafting, editing.

Data availability NA.

Declarations

Competing interests The author reports there are no competing interests to declare.

References

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

Altshuler E, Ramos O, Martínez C, Flores LE, Noda C (2001) Avalanches in one-dimensional piles with different types of bases. Phys Rev Lett 86(24):5490–3

Audard M, Güdel M, Drake JJ, Kashyap VL (2000) Extreme-ultraviolet flare activity in late-type stars. Astrophys J 541:396

Bak P (1996) How nature works: the science of self-organized criticality. Copernicus, New York

Bak P, Tang C, Wiesenfeld K (1987) Self-organized criticality: an explanation of the 1/f noise. Phys Rev Lett 59(1):381–384

Bak P, Tang C, Wiesenfeld K (1988) Self-organized criticality. Phys Rev A 38(1):364–374

Bak P, Christensen K, Danon L, Scanlon T (2002) Unified scaling law for earthquakes. Phys Rev Lett 88(17):178501

Bédard C, Kröger H, Destexhe A (2006) Does the 1/f frequency scaling of brain signals reflect self-organized critical states? Phys Rev Lett 97(11):118102

Berto F, Taglibue J (2012) Cellular automata [online]. In: Zalta, E (ed.) The Stanford encyclopaedia of philosophy. Available from: https://plato.stanford.edu/entries/cellular-automata/. (Accessed 2 Sept 2022)

Boccara N (2004) Modelling complex systems. Springer, New York

Bonabeau E (2002) Agent-based modelling: methods and techniques for simulating human systems. Proc Natl Acad Sci USA 99(3):7280–7287

Cajueiro DO, Andrade RFS (2013) Controlling self-organized criticality in *sandpile* models. Phys Rev E 81:015102–015112

Chialvo DR (2010) Emergent complex neural dynamics. Nat Phys 6(1):744–750

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

Dendy RO, Helander P, Tagger M (1998) On the role of self-organised criticality in accretion systems. Astron Astrophys 337:962–965

Flake GW (1998) The computational beauty of nature. MIT Press, Cambridge

Hoffmann MJ (2005) Proceedings of the symposium on normative multi-agent systems. In: AISB'05: social intelligence and interaction in animals, robots and agents, Hatfield, UK, April 12–15, 2005. University of Hertfordshire, Hatfield, UK, pp 117–125

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

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

Lamberson PJ, Page S (2012) Tipping Points. Q J Polit Sci 7(2):75–208

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

Lustick IS, Miodownik D (2000) Deliberative democracy and public discourse: the agent-based argument repertoire model. Complexity 5(4):13–30

Lustick IS, Miodownik D, Eidelson RJ (2004) Secessionism in multicultural states: does sharing power prevent or encourage it? Am Polit Sci Rev 98(2):209–230

Macy MW, Willer R (2002) From factors to actors: computational sociology and agent based modeling. Annu Rev Sociol 28(1):143–166

Malamud BD, Morein G, Turcotte DL (1998) Forest fires: an example of self-organized critical behavior. Science 281(5384):1840–2

Mandelbrot BB (1983) The fractal nature of geometry. W. H Freeman, New York

McFadden KL, Towell ER (1999) Aviation human factors: a framework for the new millennium. J Air Transp Manag 5(4):177–184

McFarlane P (2014) Towards a higher plane of air transportation security: from hubris to knowledge. J Transp Secur 7(2):115–121

McFarlane P (2020a) Linking aviation security failures to human-mediated error. A review of the related literatures with directions for policy and research. J Transp Secur 13:33–51

McFarlane P (2020b) Developing a systems failure model for aviation security. Saf Sci 124. https://doi.org/10.1016/j.ssci.2019.104571

Miller JH, Page SE (2007) Complex adaptive systems: an introduction to computational models of social life. Princeton University Press, New Jersey

Mitchell M (2011) Complexity: a guided tour. Oxford University Press, New York

National Commission on Terrorist Attacks upon the United States (2004) The 9/11 commission report. W.W. Norton & Company, New York

Negoro H, Kitamoto S, Takeuchi M, Mineshige S (1995) Statistics of x-ray fluctuations from Cygnus X-1: reservoirs in the disk? Astrophys J 452:L49

Newman MEJ (2005) Power laws, pareto distributions and Zipf's law. Contemp Phys 46(1):323–351

Page SE (2010) Diversity and complexity. Princeton University Press, Princeton New Jersey

Reason J (1990) Human error. Cambridge University Press, New York

Reason J (1997) Managing the risks of organisational accidents. Ashgate, Aldershot

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(1):289–304

Sneppen K, Bak P, Flyvbjerg H, Jensen MH (1995) Evolution as a self-organized critical phenomenon. Proc Natl Acad Sci USA 92(11):5209–5213

Stewart MG, Mueller J (2018) Are we safe enough? Measuring and assessing aviation security. Elsevier, New York

Watkins NW, Pruessner G, Chapman SC, Crosby NB, Jensen HJ (2016) 25 years of self-organized criticality: concepts and controversies. Space Sci Rev 198:3–44

Wiegmann 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

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(11):1006–1016

Wiesenfeld K, Bak P, Tang C (1989) A physicist's sandbox. J Stat Mech 54(5):1441–1458

Wijngaarden RJ, Welling MS, Aegerter CM, Menghini M (2006) Avalanches and self-organized criticality in superconductors. Eur Phys J B 50:117–122

Wladawsky-Berger I (2012) Complex sociotechnical systems: A case for a new field of study [online]. Available from: http://blog.irvingwb.com/blog/2012/05/complex-sociotechnicalsystems-the-case-for-a-new-field-of-study.html. (5th Nov 2021)

Wolfram S (1983) Statistical mechanics of cellular automata. Rev Mod Phys 55(3):601–644

Wolfram S (2002) A new kind of science. Wolfram Media, Champaign

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.