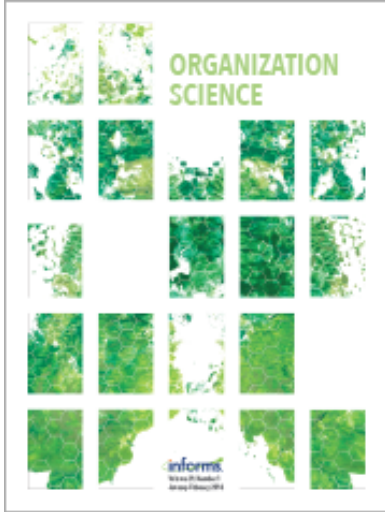




Organization Science

Publication details, including instructions for authors and subscription information:
<http://pubsonline.informs.org>

Cognition, Technology, and Organizational Limits: Lessons from the Air France 447 Disaster

Nick Oliver, Thomas Calvard, Kristina Potočník

To cite this article:

Nick Oliver, Thomas Calvard, Kristina Potočník (2017) Cognition, Technology, and Organizational Limits: Lessons from the Air France 447 Disaster. *Organization Science* 28(4):729-743. <https://doi.org/10.1287/orsc.2017.1138>

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You are free to download this work and share with others for any purpose, even commercially if you distribute your contributions under the same license as the original, and you must attribute this work as "*Organization Science*. Copyright 2017 The Author(s). <https://doi.org/10.1287/orsc.2017.1138>, used under a Creative Commons Attribution License: <http://creativecommons.org/licenses/by-sa/4.0/>."

Copyright © 2017, The Author(s)

Please scroll down for article—it is on subsequent pages



With 12,500 members from nearly 90 countries, INFORMS is the largest international association of operations research (O.R.) and analytics professionals and students. INFORMS provides unique networking and learning opportunities for individual professionals, and organizations of all types and sizes, to better understand and use O.R. and analytics tools and methods to transform strategic visions and achieve better outcomes. For more information on INFORMS, its publications, membership, or meetings visit <http://www.informs.org>

Cognition, Technology, and Organizational Limits: Lessons from the Air France 447 Disaster

Nick Oliver,^a Thomas Calvard,^a Kristina Potočník^a

^a University of Edinburgh Business School, Edinburgh EH8 9JS, United Kingdom

Contact: nick.oliver@ed.ac.uk,  <http://orcid.org/0000-0002-5410-8207> (NO); thomas.calvard@ed.ac.uk (TC); kristina.potocnik@ed.ac.uk (KP)

Received: August 21, 2015

Revised: August 22, 2016; November 10, 2016; March 3, 2017

Accepted: March 13, 2017

Published Online in Articles in Advance: June 9, 2017

<https://doi.org/10.1287/orsc.2017.1138>

Copyright: © 2017 The Author(s)

Abstract. Organizations, particularly those for whom safety and reliability are crucial, develop routines to protect them from failure. But even highly reliable organizations are not immune to disaster and prolonged periods of safe operation are punctuated by occasional catastrophes. Scholars of safety science label this the “paradox of almost totally safe systems,” noting that systems that are very safe under normal conditions may be vulnerable under unusual ones. In this paper, we explain, develop, and apply the concept of “organizational limits” to this puzzle through an analysis of the loss of Air France 447. We show that an initial, relatively minor limit violation set in train a cascade of human and technological limit violations, with catastrophic consequences. Focusing on cockpit automation, we argue that the same measures that make a system safe and predictable may introduce restrictions on cognition, which over time, inhibit or erode the disturbance-handling capability of the actors involved. We also note limits to cognition in system design processes that make it difficult to foresee complex interactions. We discuss the implications of our findings for predictability and control in contexts beyond aviation and ways in which these problems might be addressed.

 **Open Access Statement:** This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. You are free to download this work and share with others for any purpose, even commercially if you distribute your contributions under the same license as the original, and you must attribute this work as “*Organization Science*. Copyright 2017 The Author(s). <https://doi.org/10.1287/orsc.2017.1138>, used under a Creative Commons Attribution License: <http://creativecommons.org/licenses/by-sa/4.0/>.”

Keywords: managerial and organizational cognition • interpretation and sense making • decision making • complex systems analysis • ambidextrous organizations

Things that have never happened before happen all the time.
(Sagan 1995)

Errors and failures are troublesome for organizations. They can cause tragic accidents, destroy value, waste resources, and damage reputations (Coombs 2007, Yu et al. 2008). Many organizations therefore go to great lengths to avoid failure, particularly when the consequences are severe, and some “high reliability organizations” are able to achieve remarkably error-free operation even in the face of challenging conditions (Roberts 1990, Weick and Sutcliffe 2007, Weick et al. 1999). However, scholars of safety science have observed that accident rates in “ultra-safe” systems (such as commercial aviation and nuclear power) seem to be asymptotic at around five disastrous accidents per 10^{-7} safety units of the system (Amalberti 2001). Thus, even safety-critical organizations appear to find it difficult to eliminate all failures, apparently supporting the argument that accidents are inevitable in complex, tightly coupled systems (Leveson et al. 2009, Perrow 1984).

In this paper we explore this problem, drawing on Farjoun and Starbuck’s concept of organizational limits (Farjoun and Starbuck 2007, Starbuck and Farjoun 2005). We focus on commercial aviation because it represents an almost totally safe system that both confronts and constructs limits of many types, from those inherent to the physics of flight, to regulations, operating routines, and many parameters of aircraft and system design. Aviation provides a rich environment in which to study limits because limit violations are relatively tangible and visible and detailed data on these violations are publicly available (Syed 2015).

We develop the concept of limits and discuss the causes and consequences of limit violations through analysis of Air France flight 447 (AF447), which was lost when a temporary loss of speed indications unexpectedly caused the autopilot to disconnect. In responding to this, one of the pilots caused an aerodynamic stall, from which the crew were unable to recover. We examine how cockpit automation places limits on pilot experience and we explore the consequences of this. AF447 shows how a system normally capable of

operating to very high standards of safety and predictability can rapidly spiral out of control when faced with an unusual situation. We discuss the implications of a limits analysis for issues of predictability, control, and adaptability in organizations more generally (Farjoun 2010).

AF447 is classified as a “loss of control” incident. Loss of control is currently the single greatest cause of casualties in commercial aviation. It accounted for nearly 1,400 fatalities in 15 fatal air accidents between 2006 and 2015 according to Boeing (2016) and 37 fatal accidents and 1,242 fatalities (43% of all fatalities) between 2010 and 2014 according to analysis by IATA (2015). Most types of aviation accidents have declined over time, but loss of control incidents have not (IATA 2015). Intriguingly, the loss of control problem has been attributed to some of the very same measures, such as sophisticated cockpit automation, that have also reduced accidents (Harris 2011, 2014; Learmount 2011; Rochlin 1997).

We consider AF447, and loss of control incidents more generally, as extreme examples of failure in a very safe system that normally operates well within its limits. In doing this, we seek to contribute to knowledge in three distinct ways. First, we discuss limits concepts, drawing on the work of Farjoun, Starbuck, and colleagues. Second, we use limits concepts to interpret the events that led to the loss of AF447 and in doing this seek to theorize the paradox of almost totally safe systems more deeply. Finally, we discuss the implications of a limits perspective for organization science more generally, in particular how organizational strategies geared to predictability and control interact with those required to handle uncertainty (Farjoun 2010).

From a limits perspective, failures occur when organizations attempt to do things that are beyond their capabilities. The concept emerged from analysis of the loss of the space shuttle *Columbia*, which concluded that a cause of the disaster was that NASA had “pushed or been pushed to the *limit* of what an organization can accomplish” (Starbuck and Farjoun 2005, p. 360; emphasis added). In this case, the limit that NASA exceeded was its ability to meet multiple demands while operating the space shuttle safely. A limits perspective is thus implicitly a stress model in which demands exceed coping capabilities (Karasek 1979, Lazarus and Folkman 1984). In the run up to the *Columbia* disaster, NASA was being judged against no fewer than 211 performance targets (Starbuck and Stephenson 2005). Over many years, pressures to secure legitimacy and funding had led NASA to overpromise and to oversell the reliability of its technology (Boin and Schulman 2008). One manifestation of this was to portray the shuttle as an operational, rather than as an experimental vehicle, resulting in schedule pressures that intensified after NASA made

a public commitment that the core of the International Space Station would be complete by February 2004. Yet the reality was that NASA was not dealing with “settled knowledge” (Boin and Schulman 2008) but with complex, unreliable technologies, operating under extreme conditions, requiring “real-life experimentation at the edges of knowledge” (Farjoun and Starbuck 2007, p. 556). This meant that with every flight there were many issues and anomalies to be resolved.

Schedule pressures and other demands therefore severely tested NASA’s capability to meet them. A culture and vocabulary developed that privileged schedule over safety (Haunschild et al. 2015) and that was “not hospitable” to discussions of risk and uncertainty (Ocasio 2005, p. 118), along with a subtle shaping of collective cognition that encouraged significant anomalies to be treated as “in-family” events, thereby normalizing deviance (Vaughan 1997). Consequently, the crucial foam strike was classified as a maintenance issue to be addressed once the orbiter had returned to Earth and not as a potential safety issue that required immediate investigation. The engineers who were most concerned about the foam strike struggled to get their voices heard by mission management. The result was “structurally induced blindness” (Ocasio 2011) toward certain issues:

There was coordination within an organizational level but not between levels. As a result, abstractions that made sense within levels were senseless between levels. Abstractions favored within the top management level prevailed. Abstractions of the engineers were ignored. (Weick 2005, p. 165)

Thus, the overall “limit” that NASA exceeded was its ability to fly the shuttle safely in the face of multiple external demands and a highly ambitious launch schedule, while deploying complex, unreliable technologies “at the frontier.” Organizationally, NASA exceeded the limit of its ability to identify, interpret, communicate, and act upon information about the foam strike while simultaneously attending to other demands.

Organizational Limits

The limits concept was subsequently defined by Farjoun and Starbuck as follows:

All organizations have limits in the range, amount, duration, and quality of things they can do with their current capabilities, and these limits may originate in their members’ perceptions, in their policies, in the technologies they adopt, or in their environments. (Farjoun and Starbuck 2007, p. 543)

This conception goes beyond the stress model implicit in the *Columbia* analysis because it identifies a number of limiting factors that together restrict the overall ability of an organization to meet the demands

made upon it. Farjoun and Starbuck single out three such factors: cognition, management policies, and constraints in the environment.

Limits to *cognition* are significant because they constrain the ability of actors to recognize, interpret, and respond appropriately to events. Cognition figures extensively in various analyses of Columbia (Dunbar and Garud 2009, Garud et al. 2011, Weick 2005) and of course also underpins much of the literature on sense-making and catastrophe (Weick 1993, 2010). Yet limits to cognition are not a given. Some organizations find ways to create valid, sophisticated, shared mental models, even in complex and dynamic operating environments, thereby extending the limits within which they can operate predictably and safely (Roberts and Rousseau 1989, Weick and Roberts 1993, Weick and Sutcliffe 2007). Others struggle to do so (Farjoun and Starbuck 2007). Conceptually, cognitive limits are rooted in constraints in the capacity of human beings to pay attention to many things at once while processing and sharing information, constraints that have long been recognized by scholars of decision making (March and Simon 1958, Ocasio 1997, Simon 1972).

The second category of limits identified by Farjoun and Starbuck emerges from a managerial quest for coordination and control. Examples of such limits include deadlines, budgets, and organizational policies. Deadlines and budgets are mechanisms to control resources and to coordinate interdependent activities by establishing limits within which actors are expected to work. Such limits are an integral part of the apparatus of organizational control, providing some predictability of outcome without constant monitoring and/or detailed specification of inputs. They also reduce the risk of managerial overload (Ashby 1958, Child 1984, Galbraith 1974). Limits therefore underpin many fundamental organizational processes:

All of the concepts on which organizations rely—such as order, purpose, choice, power, conflict, division of labor, coordination, trust, reliability, and accountability—require or assume limits of some sort.

(Farjoun and Starbuck 2007, p. 545)

Cognition-based and managerially induced limits share some common features. Both recognize limited capacity for attention and information processing. From the cognitive perspective, a crucial limiting factor of what an organization can do is determined by the ability of its members to make sense of what is happening around them; transgression of this limit is likely to lead to failure. Managerially defined limits typically serve to either focus attention (controlling time or cost, or limiting task variety, for example) or provide a framework within which decisions can be devolved to lower levels, thereby reducing monitoring and information-processing costs (Galbraith 1974).

The first two categories of limits are endogenous to most organizations because they stem from aspects of organizational cognition, structure, and process that contribute to (or impede) an organization's ability to meet demands. The third category of limits is exogenous, in that the limits originate in the organization's environment. Examples include societally defined restrictions that may be expressed through laws or regulations, or market mechanisms that penalize organizations that fail to match the price, quality, and service levels of their competitors. Laws of science that constrain what is physically or technically possible represent particularly immutable exogenous limits.

In this paper we will use *endogenous limits* to refer to the limits of what an organization is able to do, with reasonable consistency and reliability, given its characteristics and capabilities. Capabilities stem from the resources available to an organization (e.g., skills, knowledge, and experience) coupled with its ability to mobilize and apply these resources toward appropriately scoped and prioritized goals. We use *exogenous limits* to refer to restrictions on organizational action that emanate from the environment in which an organization operates. The nature of these can vary, from constraints based on physical laws (e.g., thermodynamics or gravity) to socially constructed limits (e.g., legislation, regulations, and norms about what is acceptable or desirable). The key point is that the limits to what an organization can do are partly endogenous (limited by its capabilities) and partly exogenous, limited by what social and physical features of its environment permit.

The distinction between endogenous and exogenous limits raises an important question: Endogenous or exogenous to *what*? In various analyses of the Columbia disaster, the focus is on NASA as an organization. Therefore “endogenous” limits stem from factors within NASA as an organization and “exogenous” ones from NASA's environment. But as one moves between levels of aggregation, a feature that is a source of capability and is therefore endogenous at one level may represent an exogenous limit at another. For example, for a project team a budget or deadline represents an exogenous limit. For the organization within which the project team is located, budgets and deadlines are tools to facilitate coordination and the control of cost and time, thereby influencing the organization's endogenous limits.

This distinction is particularly significant for the relationship between technology and limits, which we review in the next section, because technology can represent both an endogenous and an exogenous limit. When technology contributes to a capacity to do things (e.g., through data storage and processing power) it is endogenous to the entity that is using it. When technology serves as a constraint on those who interact with it

(e.g., by prescribing their sequence of actions) it functions as an exogenous limit. This may be intentional (e.g., when operators are prevented from advancing through a data entry process unless valid values have been entered) or it may be a side effect of the pursuit of other priorities, such as cost or simplicity, which render the technology incapable of certain functions.

Limits, Technology, and Aviation

In aviation, technology, in particular cockpit automation, has attracted attention ever since the “glass cockpit” revolution began to change the work of pilots on the flight deck (Rochlin 1997). The “glass cockpit” originally referred to the replacement of electromechanical dials and gauges with computer-generated panel displays (Rochlin 1997), but the term also describes an ensemble of technologies that process and present data to pilots, manage the relationship between pilot input and aircraft response (“fly-by-wire” technologies), and fly the plane automatically. In a glass cockpit, pilots spend much of their time monitoring and managing, rather than manually flying, their aircraft.

Glass cockpit technology has contributed significantly to the decline in aviation accidents in recent decades (Carr 2015, Grose 1988, Harris 2011). However, there are concerns that it erodes situational awareness, with pilots sometimes unsure about what the technology is doing (Harris 2011, Learmount 2011, Young et al. 2006). Long haul pilots in particular typically spend very little time actually flying their planes, something that can adversely affect their ability to handle unusual, demanding situations (Adams et al. 1995, Endsley 1996, Learmount 2011).

Viewed through a limits lens, cockpit automation affects both the exogenous and endogenous limits experienced by a flight crew. First, automation intervenes to prevent dangerous maneuvers, thereby acting as a protective, exogenous limit that insulates pilots from the consequences of their actions but in doing so it restricts pilots’ repertoires of behavior and experience (Learmount 2011). The sudden loss of exogenous limits previously provided by technology can quickly thrust a crew into a zone from which it was previously excluded, with only limited time to answer fundamental questions such as “What is this technology doing?” and “What will it do next?” (Sarter et al. 1997, Weick et al. 1999). Automation surprises, where the technology malfunctions or fails to function as expected, pose a particular problem (Sarter et al. 1997, Weiner 1989). Second, automation reduces the cognitive load of pilots, who are relieved of the burden of scanning multiple instruments, processing information, and flying the plane manually, thereby reducing the risk of overload-related errors. Third, it may subtly erode pilots’ capabilities (Learmount 2011, Weick 1990a). Finally, there is a risk that under

unusual conditions, automation may give ambiguous or inappropriate signals, which in turn precipitate and aggravate errors (Bainbridge 1983, Parasuraman and Wickens 2008, Rouse et al. 1987).

In the field of safety science, many of these issues are expressed in the “paradox of almost totally safe systems” (Amalberti 2001, Reason 2000b). This paradox recognizes that most systems need to stay within certain limits for safe operation. Designers and controllers therefore construct procedures, checks, and controls—including technology-based ones—to ensure that these limits are not transgressed. For operators, such as pilots, such measures constitute exogenous limits on their actions. However, they also have the side effect of reducing operators’ “cognitive experience of the system and jumble [...] meta-knowledge, confidence, and protective signals when approaching boundaries” (Amalberti 1998, p. 9). Continuous operation well within limits does not stimulate challenge and enquiry and therefore can undermine situational awareness and mindfulness (Amalberti 1998, 2001; Reason 2000b, 1997; Roe and Schulman 2008). This erosion is most likely to be revealed in unfamiliar or unexpected circumstances that function as “brutal audits” of the coping ability of those involved (Amalberti 2001, Dismukes et al. 2007, Farjoun 2010, Reason 2000b, Richardson 1995, Sastry 1997, Weick and Sutcliffe 2007). Hence the paradox—safe, predictable, error-free operation under normal conditions may come at the expense of reduced capability to deal with abnormal conditions. Or, in limits terms, the reduced risk of errors due to exogenous limits imposed by system design may have a detrimental effect on the endogenous limits of the actors concerned.

Contribution of a Limits Perspective

The various types of limit that we have discussed map onto a number of established bodies of research. Cognition-based limits recognize the limits of attention and their significance for decision making (March and Simon 1958, Ocasio 2011, Simon 1972), an issue also relevant to sensemaking (Weick 1993, 2005, 2010), high-reliability theory (Roe and Schulman 2008, Weick and Roberts 1993, Weick and Sutcliffe 2007), and organizational mindfulness (Sutcliffe et al. 2016, Weick et al. 1999). All of these areas address issues of social cognition and the ability of actors to perceive, interpret, share, and act appropriately when faced with information that is complex and ambiguous. A limits perspective invokes cognition as one of the critical limiting factors of an organization’s repertoire of responses to the demands that it faces. Managerially induced limits are based on notions of coordination and control, in which limits serve as boundary conditions for behavior (for instance through rules and policies) and resource consumption (such as deadlines and budgets)

delivering some control while regulating variety and information-processing load (Beer 1981, Child 1984, Galbraith 1974, Lawrence and Lorsch 1986). A limits perspective draws attention to some of the negative and unintended consequences of such limits (Starbuck 2009). But what does the perspective add to what are already well-established concepts about how organizations work or fail to work? The answer, according to one commentator, is that “perceptions of organizational failure... become more meaningful when they are linked to concepts such as limits” (Weick 2016, p. 5).

We concur with this view and suggest that the value of a limits perspective is fourfold. First, a limits perspective considers combinations of organizational processes that may otherwise be treated in isolation—such as cognition, communication, decision making—and relates these to an organization’s capacity to deal with the demands it faces and to the consequences of its inability to meet these demands. Second, a limits perspective prompts questions such as “What factors limit the capacity of this organization to perform?” and “What are the consequences of exceeding this capacity?” Third, the idea that organizations have limits that can be exceeded alerts us to the risk of “overreach,” leading to outcomes that are unpredictable and in many cases undesirable. Finally, the distinction between endogenous and exogenous limits draws attention to the constraining effects of both organizational capabilities and factors in the environment.

Methods

Limits research faces several challenges. Limits can be difficult to observe and define and are not always visible or are only visible for short periods (Farjoun and Starbuck 2007). Some limits are only revealed by violations that often carry negative consequences, so that those involved may be reticent to be subjects of research. There may be posthoc reconstructions of events in order to deflect responsibility. Events that are subject to detailed, forensic public inquiry are therefore promising candidates for limits analysis and indeed are often studied as organizational failures (Starbuck and Farjoun 2005; Weick 1990b, 1993, 2010). Official reports may be shaped by political and other forces (Brown 2000), but safety-critical activities are perhaps less susceptible to this problem.

Aviation is therefore well suited to limits research. A great deal of information is collected as part of normal operations. Flight data and cockpit voice recorders (“black boxes”) record pilot conversations and actions and aircraft behavior. Aviation personnel are encouraged to report errors and anomalies, including those that do not result in accidents, so that safety can be improved (Dekker 2012, Reason 2000a, Syed 2015). The details of accident investigations are widely available.

Our analysis of AF447 is based on two main sources: the official report on the accident by the French air accident investigation agency (BEA 2012), and an additional analysis by an Airbus 330 pilot (Palmer 2013). The official report includes the transcript of the cockpit voice recorder (CVR) for the final two hours of the flight and readouts from the flight data recorder (FDR). The FDR provides information on the status of many aircraft parameters for the last 40 minutes of the flight. Palmer is an Airbus 330 pilot with a major international airline. He is lead author and editor for the airline’s A330 systems manual and of numerous A330 training publications. His book provides background information on the aircraft involved and on operational and other procedures not explained in the official report. Palmer also provides extensive interpretation of much technical information in the official report.

Because of its dramatic nature, there have been many accounts and analyses of the accident, such that a Google search using the search term “Air France 447” in February 2017 produced nearly 900,000 hits. The aircraft was out of radar contact when it disappeared, there was no distress call and no survivors, so there was relatively little information for investigators to work with until the wreckage of the aircraft was located in 4,000 meters of water and the cockpit voice and flight data recorders recovered, some two years after the crash. Therefore, virtually all accounts are based on the same source material from the official report and its associated documents. We reviewed many accounts of the accident but it quickly became clear that many of these introduced errors and embellishments to the original data or omitted important items of information. We therefore restricted ourselves to data that appeared in the official report and its associated documents, supplemented by Palmer’s book because of the specialist additional information that it provided.

To compile our data set, we first extracted four streams of information from the official report and Palmer’s book. These were (1) the transcript of the CVR, (2) the data from the FDR, (3) the commentary and analysis in the official report, and (4) key points from Palmer’s account of the incident. A master data table was created and verbatim extracts from each source were placed in one of four columns (CVR, FDR, Official Report, Palmer) in approximate chronological order from the start of the flight up to the crash. This was necessary to establish the precise flow of events, as neither the official report nor Palmer presented all relevant data in exact chronological order. Two further columns were then added. The first contained the precise times at which various events occurred. Each block of time was assigned a unique row. The second column tracked the altitude of the aircraft and how this changed over time. The material was then sequenced

into precise chronological order. There were a number of points at which several things were happening simultaneously or in quick succession; particular attention was paid to these sequences. This process created a document that ran to 26 A3 pages and comprised over 23,000 words, in six columns and 118 rows.

The transcript from the CVR provided data on how the pilots interacted with each other, how they responded to events, and clues as to their cognition and comprehension as events progressed. The voice recorder also picked up sounds that helped build up a picture of what was happening on the flight deck (such as ice particles hitting the fuselage at the start of the incident) and aural warnings emitted by the aircraft instruments (for example, the stall warning, which sounded repeatedly during the final minutes of the flight). The FDR provided information about the status and behavior of the aircraft and the inputs made by the pilots.

The three authors independently reviewed the data document, noting conditions, events, and actions relevant to limits and limit violations. This produced a long list of elements, many of which were interdependent (e.g., pilot actions, aircraft response, instrument readings, and aircraft parameters). Individual judgments were compared and discussed until consensus on each was achieved and then aggregated to produce an agreed set of limits issues.

The timeline was then divided into three distinct phases. The first covered the period of approximately two hours leading up to the disconnection of the autopilot. This phase represents a baseline of normality, before any significant limit violations occurred. The second phase lasted from the disconnection up until when the aircraft stalled. In this phase the crew was beyond limits of their experience and struggling to respond, but the situation was not totally out of control. The final phase was from the stall to the end of the flight.

One of the shocking features of the AF447 story is that apart from the short, transitory loss of airspeed indications, there were no technical faults with the aircraft. It was a modern aircraft, operated by a reputable airline with a good safety record, flown by an experienced, well-trained crew. The information necessary to diagnose the situation was available to the crew and the situation was probably recoverable up until the last minute or so of flight.

The Loss of AF447

Flight AF447 crashed into the Atlantic on June 1, 2009, on a night flight from Rio to Paris. While crossing the Inter-Tropical Convergence Zone (ITCZ), an area renowned for bad weather, the aircraft entered a tropical storm. Its speed indications briefly became invalid because of icing of the aircraft's pitot tubes, part of the

system that measures the aircraft's forward airspeed. This caused the autopilot to disconnect, requiring the pilots to take manual control. The responses of the pilot who took control caused the aircraft to leave its safe flight envelope, resulting in an aerodynamic stall. The crew were unable to diagnose what was happening to the rapidly descending aircraft until it was too late to recover and AF447 crashed into the sea with the loss of all 228 passengers and crew. The entire episode, from disconnection of the autopilot to impact, lasted 4 minutes and 23 seconds.

Phase One—From Departure to the Loss of Speed Indications

There were three members of flight crew on AF447: Captain Marc Dubois (aged 58, 10,988 flight hours) and two first officers, David Robert (aged 37, 6,547 flight hours) and Pierre-Cedric Bonin (aged 32, 2,936 flight hours). The captain and two first officers had flown 16, 39, and 5 return trips between Europe and South America, respectively.

AF447 left Rio at 22:29 UTC. The first three hours of the flight were unremarkable and Robert spent much of this time in the crew rest area. The aircraft climbed to its initial cruise altitude of 35,000 feet and on the flight deck the dialogue between Dubois and Bonin was relaxed and routine, punctuated by occasional calls to and from air traffic control. At about 00:30 the crew received information about a convective zone ahead of them, but took no action. Most other flights in the area that night made diversions to avoid the worst of the weather system. At 01:35 Bonin remarked "We've got a thing straight ahead" and the FDR showed that both he and Dubois made adjustments to their weather radar displays. Bonin expressed a wish to climb to try to avoid the weather and raised this possibility a number of times. He and Dubois discussed this and concluded that a climb was not possible because of the relatively high air temperature and aircraft's fuel load. The instruments advised a maximum altitude of 37,500 feet, which Dubois and Bonin acknowledged. The official report notes that Bonin showed "a real preoccupation [with crossing the ITCZ], beyond the simple awareness of an operational risk. Some anxiety was noticeable in his insistence" (BEA 2012, p. 168). The report describes Dubois as "very unresponsive" to Bonin's concerns, "vaguely rejecting" Bonin's suggestions to climb, but not providing a clear decision, instructions, or recommendations for dealing with the weather conditions (BEA 2012, p. 168). Dubois' position is revealed by his remark "We'll wait a little (and see if) that goes away," which, given that he was about to leave the cockpit for his break, meant that any decisions contingent on the weather were delegated to his junior colleagues.

At 01:56 Dubois called Robert back to the flight deck. Bonin, the most junior officer and least experienced

member of the crew, was designated as the pilot flying the aircraft. The handover itself was quite casual:

Dubois: [Speaking to Bonin] Who's doing the landing, is it you? Well, right, he [Robert] is going to take my place... You're a PL [Officier Pilote de Ligne] aren't you?

Bonin: Yeah.

The casualness of Dubois' handover may have created ambiguity in the control structure among the two first officers, one manifestation of which was Robert's use of the left (captain's) seat rather than the right seat, as was customary for the pilot not flying. Later analysis of the pilots' seats also revealed that when Robert took the seat vacated by Dubois, he left it well back on its rails, good for comfort, but not ideal for flying the aircraft.

About eight minutes after Dubois left for his break, Robert increased the sensitivity of the weather radar and suggested an adjustment to the course to avoid the worst of the weather system ahead. Bonin executed this and asked about a strange odor in the cockpit; Robert replied that it was ozone and explained what caused it. The official report comments as follows:

A natural assertion of authority by the PNF [pilot not flying—Robert] is then observable: he seemed to master the environmental context better (ozone) and suggested, even asserted, the avoidance strategy. The PF [pilot flying—Bonin] did not resist this tendency. Without this leading to the slightest conflict, after the autopilot disconnection, it rapidly led to the inversion of the normal hierarchical structure in the cockpit, with leadership passing to the PNF in the left seat without the role of command being formally and explicitly transferred.

(BEA 2012, p. 170)

Up to this point, apart from the weather system in the path of AF447, the situation appeared normal and certainly seemed to be viewed as such by Dubois. Bonin exhibited anxiety; events were to prove that this was with good reason. AF447's failure to make a timely diversion around the storm did not violate any limits per se, but increased the probability that the crew would face difficult and challenging conditions; in other words, the limits of their capabilities were more likely to be tested. The maximum safe altitude for AF447 was 37,500 feet—an exogenous limit that ruled out climbing above the weather system, narrowing the crew's options.

Several conditions, each minor in itself, now combined to compromise the crew's ability to deal with the situation that lay ahead. The least experienced member of the crew, already anxious about the weather system, was designated as relief captain. The casual handover of command by Dubois created ambiguity in the authority structure on the flight deck, subtly reinforced by the seating layout. Dubois' decision to take his break

reduced cognitive resources on the flight deck just as AF447 entered the storm. Without realizing it, the crew had suffered a significant diminution in capability and at the same time had increased the risk of substantial workload, hence shifting the demands-capability balance. The margins of safety narrowed as the crew moved closer to key endogenous and exogenous limits.

Phase Two—From the Loss of Speed Indications to the Stall

The phase from the icing of the pitot tubes until the stall lasted only about one minute, but a great deal happened during this brief period. Shortly after Robert and Bonin adjusted course, the CVR recorded the sound of ice crystals against the fuselage. These temporarily blocked the three pitot tubes that are part of the system that calculates the forward airspeed of the aircraft. The readings produced by the pitots are used by the electronic flight control system, which is programmed to disengage when these readings are inconsistent. The automatic pilot, which was controlling parameters such as thrust, altitude, attitude, and roll disconnected, requiring the pilots to take manual control. Pilots rarely fly manually at high altitude because the safe flight envelope is small and even modest pilot inputs produce significant responses from the aircraft. (The safe flight envelope refers to the combination of conditions necessary for an aircraft to remain in flight, the edges of which are defined primarily by airspeed, angle of attack, and air density.) The aircraft's flight control system switched from "normal" to "alternate" law, disabling the protections that automatically prevent excursion from the safe flight envelope.

Several limit violations occurred at this point. The first was that the volume and density of ice particles temporarily exceeded the capacity of the pitot tube heaters to clear them, blocking the tubes. The electronic flight control system disconnected, exactly as it was designed to do when faced with unreliable data, so the pilots were forced to hand fly at high altitude, a situation outside their normal experience. The pilots thus abruptly found themselves beyond their endogenous limits, facing an unforgiving exogenous limit in the form of the very restricted flight envelope and without the usual automatic protection against inappropriate actions. The situation was not yet a crisis—the only real issues were that the speed readings were inconsistent and that the flight path had to be maintained manually.

Bonin took control of the aircraft using his sidestick, calling out "I have the controls." He attempted to correct a slight roll to the right, but overcompensated, causing the aircraft to roll left. He overcorrected again and the aircraft rolled left and right 10 times in 30 seconds. In addition to lateral stick movements to try to control the roll, Bonin also pulled back on his stick, putting the aircraft into a climb, possibly in response to

an erroneous indication of slight loss of altitude when the pitot tubes blocked. The aircraft rapidly gained altitude while losing airspeed.

The appropriate response to autopilot disconnection is for pilots to touch as little as possible and to keep the aircraft flying straight and level while they try to understand the situation (BEA 2012). A postaccident simulation demonstrated that without Bonin's inputs the plane would have gradually rolled further to the right but attitude and altitude would have remained stable. There was no immediate risk to the aircraft until Bonin's inputs began to move it toward the edge of the safe flight envelope.

As the aircraft pitched up in response to Bonin's initial nose-up input, the stall warning (a synthetic voice announcing "stall, stall") sounded three times. Within 10 seconds of the disconnection, both pilots had recognized that there was an issue with the airspeed indications:

- Bonin: We haven't got a good
 Bonin: We haven't got a good display . . . of speed.
 Robert: We've lost the the the speeds so . . . [reading out ECAM¹ messages] engine thrust A T H R engine lever thrust.
 Robert: [continuing to read the ECAM]¹ . . . alternate law protections- (law /low /lo²).
 Bonin: Engine lever?
 Robert: Watch your speed, watch your speed.
 Bonin: Okay, okay, okay I'm going back down.
 Robert: Stabilise.
 Bonin: Yeah.
 Robert: Go back down. According to that we're going up. According to all three you're going up so go back down.
 Bonin: Okay.
 Robert: You're at [. . .] go back down.
 Bonin: It's going, we're going (back) down.

Bonin was quite possibly unaware that flight envelope protection had been withdrawn and Robert's disorganized reading of the ECAM messages did little to correct this. So just as the startled crew confronted an unfamiliar situation that tested their endogenous limits, many of the protective exogenous limits bestowed by the electronic flight control system had disappeared.

Although struggling to assimilate what was happening, both pilots, particularly Robert, had some grasp of the situation. Both showed awareness of the inconsistent airspeed readings and Robert recognized the risk posed by altitude gain and loss of airspeed. Yet despite Robert's warnings, Bonin continued to pull back on his sidestick and within about a minute AF447 had climbed to nearly 38,000 feet, violating the safe altitude limit that Bonin and Dubois had discussed less than 20 minutes earlier. Bonin's actions were invisible to Robert because on Airbus aircraft each pilot has a sidestick to manually control the plane, located on opposite sides of the aircraft. The sidestick inputs of one pilot

are therefore not apparent to the other. If pilots make conflicting sidestick inputs these are averaged by the system, a warning message is displayed and a synthetic voice calls out "dual input."

Robert's attention was initially split between monitoring the flight path, giving instructions to Bonin, and reading and interpreting the messages on the ECAM. It appears that Robert quickly concluded that the situation was beyond his capacity to resolve and his priority became recalling Dubois to the flight deck. Robert made at least six calls to the crew rest area within about 30 seconds (approximately 50–80 seconds after disconnection). By 02:11:07 (one minute three seconds after disconnection) the icing had cleared and airspeed indications were valid once more. However, the climb had wiped nearly 90 knots off the indicated airspeed, so the pilots may not have believed the now-valid speed readings.

In limits terms, several things happened during this phase, with one limit violation triggering a cascade of additional human, technological, and physical limit violations. The initial limit violation was technological—the capacity of the heating elements to keep the pitot tubes clear was exceeded. However, ice ingestion was a known issue that had been under investigation for nearly a year before the loss of AF447. We revisit this issue in the discussion, as it reveals both how actual limits may be established and the difficulty of ascertaining exactly where they lie.

Other limit violations quickly followed. The disconnection of the autopilot and the reversion to alternate law are purposefully designed responses to inconsistencies in input data to the flight control system. The role of the pilots in this situation is essentially that of "disturbance handlers" (Mintzberg 1989) who apply human judgment to resolve the situation. The AF447 pilots appear to have been so caught by surprise that they were momentarily pushed beyond the limits of their ability to handle this disturbance. As they struggled to understand what was happening, Bonin rapidly and unwittingly took the plane toward the edge of its safe flight envelope, possibly unaware that there was now no protection against a stall. The official report suggests that this, along with aural saturation and mental overload, may be why the pilots never acknowledged the stall warning, which called out "stall" a total of 75 times. Under normal flight law a stall is virtually impossible, so the pilots may have been unable to absorb or believe the synthetic voice telling them that this was indeed what was happening. If so, this demonstrates how limits constrain cognition and perceptions of plausibility, thereby impeding problem recognition and resolution.

Robert, who initially had a better grasp of the fundamentals, was soon overwhelmed as Bonin's actions

rapidly aggravated the situation. The crew's collective cognition, expressed and supported by an ability to coordinate and cross-check tasks and readings, processes inherent to effective crew resource management, collapsed and never recovered. In effect, a cascade of limit violations occurred. The ice ingestion led to the withdrawal of flight protections and the autopilot, which in turn thrust the pilots, Bonin in particular, into a situation that was outside the limits of their normal experience. The crew's ability to pool cognitive resources, which could have offered a route to recovery, broke down in the face of ill-preparedness and a strong startle effect. Their increasingly uncoordinated actions rapidly propelled the situation toward a full blown crisis.

Phase Three—From the Stall to the End of the Flight

While Robert was trying to recall Dubois to the cockpit, the aircraft reached its peak altitude of 37,924 feet and exited the flight envelope—a violation of a crucial exogenous limit. In the seconds that preceded the stall, the stall warning began to sound in the cockpit and the CVR recorded vibrations, most probably the onset of stall buffet. Neither Bonin nor Robert acknowledged the stall warning or buffet.

After the autopilot disconnection the main task for the pilots had been to stabilize the flight path while they diagnosed what was happening and worked out a plan of action. Pilot training for stalls emphasizes recognition of approach to a stall and stall avoidance. It does not include an actual stall and recovery from this. Once AF447 stalled, the situation changed very dramatically. Further limit violations quickly ensued and a pressing new limit, time, entered the picture. The aircraft was in free fall, falling at 10–15,000 feet a minute. The crew had only around three and a half minutes until the aircraft reached the ocean, a very small recovery window. "At this point, only descent of the aeroplane through a nose-down input on the sidestick would have made it possible to bring the aeroplane back within the flight envelope" (BEA 2012, p. 179).

However, neither Bonin nor Robert recognized that the aircraft was stalled. They were therefore struggling to understand what was happening, let alone take appropriate corrective action. Their bewilderment is clear from the CVR, approximately a minute and a half into the episode:

Robert: But we've got the engines, what's happening (...)?
Do you understand what's happening or not?

Bonin: (...) I don't have control of the airplane any more now. I don't have control of the airplane at all.

Robert: Controls to the left (...) what is that?

Bonin: I have the impression (we have) the speed.

Dubois: [Noise of cockpit door opening] Er, what are you (doing)?

Robert: What's happening? I don't know, I don't know what's happening.

Bonin: We're losing control of the aeroplane there.

Robert: We lost all control of the aeroplane, we don't understand anything, we've tried everything.

Dubois returned to the cockpit at 02:11:42 as the aircraft passed through 35,000 feet, the same altitude as when he had left the cockpit. In theory, his return increased the crew's capacity to resolve the situation, but he too could not comprehend what was happening.

The aircraft's rate of descent was far beyond the limits envisaged by the designers of the aircraft's systems and instruments. As a consequence of this, many readings aggravated the pilots' difficulties in understanding and responding to their rapidly deteriorating situation. One example was the "flight directors." These display crossbars that prompt the pilots as to which pitch (up or down) and roll (left or right) inputs they should make to achieve an intended flight path. Under normal conditions, the flight directors provide guidance from shortly after takeoff until landing, reducing the workload of the pilots who would otherwise have to scan and integrate the readings of several instruments. However, "It is easy to fall into the trap of following the flight directors so intently that the actual instrument indications are ignored" (Palmer 2013, p. 1409). The procedure for unreliable airspeed indications states that pilots should switch off the flight directors to avoid erroneous guidance, but the AF447 crew did not do this.

Because of the unreliable airspeed indications, the flight directors disappeared and reappeared three times in the 40 seconds following disconnection. Although they initially directed a return to the original cruise altitude of 35,000 feet, after a few seconds they switched to commanding a climb in response to Bonin's persistent nose-up inputs. During the four and a half minutes of the episode the flight directors disappeared five times. They displayed for around two minutes in total and for at least 75% of this time they commanded a climb—the exact opposite of the nose-down response necessary to recover from the stall. It is not possible to know if Bonin followed the flight directors, but Palmer's analysis of the relationship between the flight director guidance and Bonin's actions with the stick indicate that this is a distinct possibility (Palmer 2013, p. 2338).

The extreme vertical speed of the aircraft had a number of consequences. Forward airspeed indications again became unreliable because the angle of attack was so steep that the airflow through the sensors was disrupted. This interacted with another technological limit. To avoid false stall alarms, the A330's aural stall warning is designed to automatically shut off when the indicated forward airspeed falls below 60 knots, which it did several times because of the rate

and angle of AF447's descent. But this meant that when the crew twice made correct, nose-down inputs, the angle of attack reduced, the speed indications became valid again and the stall warning reactivated. This may have sent an erroneous cue that the nose-down inputs were making things worse, rather than better. The erratic forward speed indications caused by the rate of descent were also responsible for the disappearance and reappearance of the flight director displays. To make matters even worse, the aircraft's rate of descent was so great, and so far outside the design limits of the instruments, that vertical speed indications also became erratic. Palmer describes the likely scene on the flight deck:

The crew saw an airplane with operating engines, pitched up, erratic airspeed, an altimeter moving many times faster than they have ever seen one move, and a vertical speed indicator that was blank, erratic, or pegged beyond the limit of its normal display range.

(Palmer 2013, p. 1903)

Bonin interpreted the stall buffet as a sign that the aircraft was flying too fast, and reduced the engine thrust and applied the speed brakes, the exact opposite of what was required. He was immediately overruled by Robert.

As the plane passed through 10,000 feet Robert and Bonin made conflicting inputs via their sidesticks. A synthetic voice announced "dual input" repeatedly, warning that two pilots were attempting to fly the plane:

Robert: Wait, me, I have I have the controls eh?

Synthetic voice: Dual input.

Bonin: What is... how come we're continuing to go right down now?

....

Bonin: Nine thousand feet.

Dubois: Careful with the rudder bar there.

Robert: Climb, climb, climb, climb.

Bonin: But I've been at maxi nose-up for a while.

Synthetic voice: Dual input.

Dubois: No, no, no, don't climb.

Robert: So go down.

Synthetic voice: Dual input.

Bonin: Go ahead, you have the controls, we are still in TOGA [Take Off and Go Around, i.e., a high power setting] eh?

Synthetic voice: Dual input.

Bonin's declaration of "But I've been at maxi nose-up for a while" provided the missing piece of the jigsaw for the other two pilots, as Dubois' exclamation of "No, no, no, don't climb" and Robert's "So go down" make clear. But by then there was insufficient altitude left to recover from the stall. Even after Dubois' eventual diagnosis of the situation (around 50 seconds before impact) and his instructions to Bonin to take corrective action, Bonin continued to make nose-up inputs that cancelled out those of Robert, eliciting further warnings of "dual input" from the aircraft's instruments. The recording ended at 02:14:28 hours.

Discussion

Aviation is an environment in which limits and limit violations are relatively visible and in which there are detailed data on the antecedents and consequences of violations. We propose that the application of a limits lens to the loss of AF447 yields several insights.

The first insight concerns the interaction between aircraft automation and pilots and, more generally, between exogenous and endogenous limits. A limits perspective highlights what can happen when consciously designed limits (in this case cockpit automation) that normally constrain actors from venturing into a danger zone suddenly disappear. Deprived of this protection, AF447's pilots found themselves in a world that they could not comprehend, exposing their endogenous, cognition-based limits.

The obstruction of the pitot tubes triggered a rapid sequence of further limit violations. The pilots, possibly already suffering from degraded collective capacity to handle disturbance, were abruptly confronted with a situation that was outside of their normal experience. Neither was able to make a timely diagnosis; Bonin aggravated the situation by his inappropriate inputs. The protections normally afforded by the flight control system disappeared, probably without the pilots being fully aware of this. Within a minute the aircraft left the flight envelope—again, without the pilots realizing it. Limit violation compounded limit violation as the behavior of the aircraft exceeded the parameters imagined by its designers, causing the instruments to give misleading cues to the pilots. Bonin's individual incapacity to cope quickly developed into collective incapacity as his actions introduced further conditions that neither Robert nor Dubois could readily diagnose. The coordination, communication, and cross-checking (collective cognition) that might have allowed stabilization of the flight path and diagnosis of the problem broke down, a pattern also observed in other catastrophes (Weick 1990b, 1993).

The idea that all organizational defenses have holes and that accidents occur when these holes line up, often following a triggering event—the "Swiss cheese" model of failure—is well known (Reason 2000a, 1997). Limits concepts enrich this model because they highlight how different elements of a situation may interact in a cycle of escalation. In the case of AF447, a triggering event, itself a limit violation, occurred. Not only did this expose holes in defenses as protective exogenous limits fell away, but the situation put unusual demands on the pilots, exposing and exceeding their endogenous limits. The pilots then precipitated further violations of exogenous limits, such as the stall, moving events even further beyond their experience and capabilities. Thus, contagion and destructive spirals occurred as successive limits were breached and the window for recovery rapidly shrank.

A second insight from AF447 concerns the challenge of recognizing where limits actually lie and how the positions of limits are established. This issue is graphically illustrated by the icing of AF447's pitot tubes, and more generally by the assumed ability of the overall "human-technical system" to deal with this eventuality. The limit of the tubes to withstand ice particle ingestion appears to be a technical question. Yet icing of pitot tubes on Airbus aircraft was a known problem. Nine incidents of unreliable airspeed indications on A330/A340 aircraft because of icing were reported by Air France captains alone between May 2008 and March 2009. Two reports highlighted the potentially destabilizing nature of these incidents because of the difficulty of diagnosing them (BEA 2012, p. 123). Air France reported the issue to Airbus in July 2008, triggering dialogue between Airbus, Air France, and Thales, the manufacturer of the pitot tubes. Airbus' position was that pilots should follow the unreliable airspeed procedure and advised them to "not be taken by surprise" and to avoid areas where icing was a risk. Meanwhile, evidence was accumulating that a newer version of pitot tube was more resistant to icing than the original model. By April 2009, Air France had decided to replace all the original pitot tubes fitted to its long-haul A330/340 fleet as soon as the parts were available. The first batch of replacement tubes arrived six days before the loss of AF447 and the first aircraft was modified shortly after that. AF447 was still fitted with the original tubes.

The pitot tube issue illustrates how limits are often not visible and when they are, it may only be for a short period (Farjoun and Starbuck 2007). It also reveals the complex and subtle processes by which the real, working limits of complex systems are established and why it may be very difficult to ascertain exactly where limits lie until they are tested under multiple and varied conditions—a central argument of normal accident theory (Perrow 1984). The icing issue had been investigated and discussed by multiple parties. In a sense the limit that was being established through this process was the capability of the "system" (i.e., the combination of technology, procedures, and pilot intervention) to cope, safely, with a situation that rarely arose, namely, icing and loss of speed indications. In the early stages, neither the problem, which occurred only infrequently, nor the solution were clearly defined or understood. Even after it had been decided to replace the original tubes, the working assumption was that the original tubes, backed up by pilot intervention that followed the unreliable airspeed procedure, were sufficient to ensure safe flight until such time as the new tubes could be fitted. AF447 demonstrated that this assumption was incorrect and overestimated the capability of flight crew to act as "disturbance handlers" under all flying conditions. In effect, the limits of this combined

technical-human system meant that it was unable to handle the full range of possible conditions that it might face. This was partly because of the difficulty of envisaging exactly what these conditions might be, including the faithful simulation of icing conditions during design and testing, as well as possible pilot responses under different conditions. This is a salutary reminder that design and test processes also have endogenous limits. It can be difficult to foresee all the possible ways in which technology, organization, and actors can interact, yet it is precisely these interactions that often determine the real limits of a system's capability, particularly in an almost-totally safe system where many controls are designed in. Studies of catastrophes often focus on the cognitive limits of operators who are confronted with anomalies. An implication of AF447, based on both pitot tube issue and the behavior of some of the aircraft instruments as the situation escalated, is that attention to cognitive limits during the system design and development process is also warranted. Conceptualized through a limits lens, normal accident theory could be viewed in terms of the cognitive limits of designers, expressed as an inability to conceive of the full spectrum of interdependencies in a complex system (Perrow 1984).

The pitot issue raises uncomfortable questions about the implicit model of management and control that underpins many complex systems in which designed limits (such as automation and procedures) do much of the work of ensuring that the system operates safely, backed up by human judgment to deal with exceptions and anomalies. AF447 demonstrates that a situation that defeats designed limits is also likely to tax the capabilities of humans, particularly when (a) these capabilities have eroded through lack of practice and (b) humans are caught by surprise and have only a limited window of time for judgment and response. Viewed through a limits lens, AF447 demonstrates that exogenous and endogenous limits can interact in toxic ways, raising questions about the relationship between humans and the complex systems that they control. In aviation, these questions are reflected in loss of control incidents more widely and it is to these that we now turn.

The loss of AF447 was a loss of control incident, a category of accident causing concern in the aviation community (Belcastro 2012, Belcastro et al. 2014, Brooks 2010, Harris 2011, IATA 2015, Learmount 2011, Plant and Stanton 2012, RASFOG 2010). Two aspects of the loss of control problem are particularly relevant to our discussion of limits, especially the interaction between exogenous and endogenous limits. These are the difficulty of preparing pilots for rare events and flight deck automation.

Few pilots ever face the situation in which the pilots of AF447 found themselves, largely because the limits

imposed by automation and aviation operating protocols are so effective at avoiding such a situation in the first place. Extreme situations are difficult to reproduce in a simulated training environment. There are few data on how commercial aircraft behave in extreme attitudes on which flight simulator models can be based. There is also a psychological challenge in reproducing extreme conditions:

The development and acquisition of skills related to correctly and appropriately responding to the psycho/physiological reactions inherent in confronting undesirable aircraft states is fundamental to executing a safe recovery from an unexpected aircraft upset. The required learning cannot be achieved absent from the consequences faced in actual flight. (Brooks 2010, p. 8)

AF447 graphically illustrates this point. We cannot know the precise role of psycho/physiological factors, but the official report refers repeatedly to Bonin's anxiety and to the startle effect of the sudden disconnection. The problem that this highlights is how to develop the capability to deal with out-of-limit conditions while staying reasonably safe, i.e., in limits.

A second issue is flight deck automation. The glass cockpit delivers many benefits but it also subtly distances pilots from the systems that they oversee and control, eroding their ability to diagnose and respond to automation surprises and other unusual conditions. The glass cockpit enhances safety, but by definition it means that for most pilots, for most of the time, life is spent well within the safe flight envelope. Cockpit automation removes the need for extensive manual flying, which means that pilots do not have continuous hands-on experience of aircraft handling under varied conditions. Within the aviation community there is concern that constant operation within limits causes a subtle degradation of pilots' ability to interpret and respond to situations that lie beyond such limits. This degradation is not only caused by extensive use of automation but also hidden by it.

Aviation regulators are taking this issue seriously. In 2013 the Federal Aviation Administration (FAA) issued a safety directive, which notes that "continuous use of autoflight systems could lead to degradation of the pilot's ability to quickly recover the aircraft from an undesired state" and goes on to state that "Operational policies should be developed or reviewed to ensure there are appropriate opportunities for pilots to exercise manual flying skills...during low workload conditions" (FAA 2013, p. 1). It is not that flight deck automation poses risks in normal operations; on the contrary, it contributes hugely to the impressive safety record of modern commercial aviation. The problem is more complex than this. As anomalies and opportunities for error are designed out of a system, actors have less exposure to rare, extreme events and less daily, hands-on experience. Consequently, when

unusual events do occur, they may be ill-prepared to handle them. In limits terms, the application of exogenous limits to regulate load and control variation has implications for endogenous limits by reducing actors' cognitive capabilities, both individual and collective, to deal with variation when it does occur. To make things worse, this erosion of capabilities may be concealed by the protections that exogenous limits provide, only to be revealed in rare combinations of conditions. Thus, the very same organizational attributes that yield safe operation under in-limits conditions may increase the risk of catastrophe when out-of-limits conditions are encountered. It is this, we suggest, that produces a pattern of remarkably safe operation most of the time, interspersed with occasional, infrequent disasters. These, essentially, are the dynamics of an almost totally safe system (Amalberti 1998, 2001; Reason 2000b).

If our theory is correct and the paradox of almost totally safe systems applies, responding to failures by imposing more stringent exogenous limits is likely to further degrade the disturbance-handling capability of actors, unless measures are actively taken to avoid this.

Implications

Our findings carry a number of theoretical and practical implications for organization science. Chief among these is the identification of strategies that allow controls to be designed into systems while also developing and maintaining the disturbance-handling capabilities of those who operate them. As Starbuck and Farjoun observed, limits in one form or another underpin many organization processes (Farjoun and Starbuck 2007), so constructing and confronting limits is part and parcel of organizational life. Managerially induced limits can be mechanisms to achieve predictability and control, regulating risks and containing information-processing loads to manageable levels (Ashby 1958, Beer 1981, Farjoun and Starbuck 2007, Galbraith 1974, March 1999, Simon 1982). These limits function to direct and constrain behavior and, as demonstrated by both NASA and AF447, cognition. By definition, limits restrict attention and ranges of behavior and therefore are likely to limit the cognitive capability of actors to absorb, diagnose, and respond to less familiar contingencies, just as automation on a flight deck restricts the repertoire of pilots. Inhibition of organizational intelligence (March 1999) and increased organizational stupidity (Alvesson and Spicer 2012) therefore follow, unless compensating actions are taken.

High reliability organizations give some clues as to what these compensating actions steps might be. Some of the signature characteristics of high reliability organizations look very much like antidotes to some of the dysfunctions of limits, such as "sensitivity to operations" ("do not lose touch with your system")

and “reluctance to simplify” (“do not make too many compromises in regulating information load”), both of which could be construed as calls for a balance between exogenous and endogenous limits (Weick and Sutcliffe 2007). High reliability organizations may therefore hold important lessons for other organizations as they tread a path between developing capabilities and avoiding errors and failure. The parallels between paradox in safety science and paradox in organizations more widely (Farjoun 2010) are a fruitful area for further work on limits.

Several practical implications follow from our findings. The first is a reminder of how the controllers of complex systems, whether they are pilots or executives, run the risk of becoming insulated from the systems that they oversee. In the case of pilots, the culprit may be automation. For executives, it might be separation from front-line operations, such as when responsibilities are delegated to units who largely follow established protocols, resulting in organizational mindlessness (Sutcliffe et al. 2016). In short, there are many organizational equivalents of autopilot. In the field of management, there is no FAA to advocate more hand-flying for executives, but the implication is that this is necessary if executives are to develop and maintain the ability to respond appropriately to unusual conditions.

Limitations and Future Research

We chose aviation as our test bed for limits ideas because limits and limit violations can be readily observed and because aviation’s intensive recording of data provides a good foundation for forensic analysis. However, these features may also limit the generalizability of aviation-based research. Many organizational limits are less tangible than those in aviation. Not only are they harder to see, but social and political forces mean that exogenous limits are likely to be more malleable, negotiable, and contested than limits defined by the laws of physics. Taking an aircraft out of the flight envelope will cause it to fall. Taking an organization beyond its capability, or violating an exogenous limit set by a regulator (running a bank with very low capital ratios, for example) does not necessarily result in disaster. The regulator may grant a concession, government may step in with a rescue package, creditors renegotiate terms, and so on. Organizational limits may be adjusted to accommodate transgressions and transgressors may escape the consequences of violating a limit. Thus, while the flight envelope is a powerful metaphor for the limits of a zone of safe, predictable operation, there are limits to the analogy. However, there have been applications of the flight envelope concept in the organization science literature, for example, in understanding the “survival space” of global auto firms relative to the capabilities they possess and the constraints that they face (Holweg and Oliver 2016).

In aviation the consequences of limit violations are severe and the speed at which events unfold can be very rapid—the AF447 episode only lasted four and a half minutes from autopilot disconnection to its tragic conclusion. Short recovery windows put particular strain on collective cognition, not only for pilots, but for system designers and integrators who must envisage a near-infinite range of conditions. In common with other environments with limited scope for trial-and-error learning (Rochlin 1993) the pressure to design out errors is acute. A limits analysis suggests that the risk of degradation of actor capabilities is therefore higher in environments of this nature. Less safety-critical environments may not experience these processes so potently.

Future research into limits would benefit from further case studies in other safety-critical environments to see if the interplay between endogenous and exogenous limits seen in aviation is found in other settings. Investigation of the ways in which organizations that face volatile and variable conditions not amenable to procedural solutions develop their people could reveal a great deal about how disturbance-handling capability is developed and sustained. Finally, studies of heroic recoveries as well as disasters could help pinpoint capabilities that contribute to recovery, rather than dwelling on those whose absence contributed to disaster.

We hope that through this paper we have conveyed a sense of what the crew of AF447 faced on the night of June 1, 2009. For organization science researchers, AF447 is a salutary reminder of how our capacity as humans to create highly complex systems is not always matched by our ability to organize and control them in the face of most conceivable conditions, let alone inconceivable ones. As organizations and systems grow in scale and complexity, the issue of how we develop our organizations—and ourselves as actors—to handle unexpected and extreme events grows ever more pressing.

Acknowledgments

The authors are grateful to many colleagues at the University of Edinburgh Business School for their constructive comments on early drafts of this paper. Particular thanks go to Ian Graham, Rick Woodward, Melike Senturk, and Susan Murphy as well as to those who attended workshops at which this paper was discussed and who provided useful feedback. The authors are very grateful to *Organization Science* editor Ann Majchrzak, and to the anonymous reviewers whose thoughtful comments helped develop the paper. This paper is dedicated to the passengers and crew who lost their lives on flight AF447.

Endnotes

¹ECAM stands for “Electronic Centralized Aircraft Monitoring.” This is a display that displays messages about aircraft parameters in an abbreviated style similar to a text message.

²Robert's words were not clear to the transcriber, but he was probably in the middle of saying "Alternate law—protections lost." This was crucial information concerning the loss of flight envelope protection.

References

- Adams MJ, Tenney YJ, Pew RW (1995) Situation awareness and the cognitive management of complex systems. *Human Factors: J. Human Factors Ergonom. Soc.* 37(1):85–104.
- Alvesson M, Spicer A (2012) A stupidity-based theory of organizations. *J. Management Stud.* 49(7):1194–1220.
- Amalberti R (1998) Automation in aviation: A human factors perspective. Wise JA, Hopkin VD, Garland DJ, eds. *Handbook of Aviation Human Factors* (CRC Press, Boca Raton, FL), 173–192.
- Amalberti R (2001) The paradoxes of almost totally safe transportation systems. *Safety Sci.* 37(2–3):109–126.
- Ashby WR (1958) Requisite variety and its implications for the control of complex systems. *Cybernetica* 1(2):83–99.
- Bainbridge L (1983) Ironies of automation. *Automatica* 19(6):775–779.
- Beer S (1981) *Brain of the Firm: The Managerial Cybernetics of Organization* (J. Wiley, New York).
- Belcastro CM (2012) Loss of control prevention and recovery: Onboard guidance, control, and systems technologies. *AIAA Conf. Guidance, Navigation Control* (American Institute of Aeronautics and Astronautics, Reston, VA).
- Belcastro CM, Groff L, Newman RL, Foster JV, Crider DA, Klyde DH, Huston AM (2014) Preliminary analysis of aircraft loss of control accidents: Worst case precursor combinations and temporal sequencing. *Proc. AIAA Guidance Navigation, Control Conf., National Harbor, MD*.
- Boeing (2016) Statistical summary of commercial jet airplane accidents 1959–2015. Accessed May 31, 2017, http://www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf.
- Boin A, Schulman P (2008) Assessing NASA's safety culture: The limits and possibilities of high-reliability theory. *Public Admin. Rev.* 68(6):1050–1062.
- Brooks RL (2010) Loss of control in flight. *European Airline Training Sympos., Istanbul*.
- Brown AD (2000) Making sense of inquiry sensemaking. *J. Management Stud.* 37(1):45–75.
- Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA) (2012) Final report on the accident on June 1, 2009, to the Airbus A330-203 registered F-GZCP operated by Air France flight AF447 Rio de Janeiro–Paris. Accessed May 31, 2017, <https://www.bea.aero/docs/2009/f-cp090601.en/pdf/f-cp090601.en.pdf>.
- Carr N (2015) *The Glass Cage: Where Automation Is Taking Us* (Random House, London).
- Child J (1984) *Organization: A Guide to Problems and Practice* (Sage, London).
- Coombs WT (2007) Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Rev.* 10(3):163–176.
- Dekker S (2012) *Just Culture: Balancing Safety and Accountability* (Ashgate Publishing, Farnham, UK).
- Dismukes K, Berman BA, Loukopoulos LD (2007) *The Limits of Expertise: Rethinking Pilot Error and the Causes of Airline Accidents* (Ashgate Publishing, Farnham, UK).
- Dunbar RL, Garud R (2009) Distributed knowledge and indeterminate meaning: The case of the Columbia shuttle flight. *Organ. Stud.* 30(4):397–421.
- Endsley MR (1996) Automation and situation awareness. Parasuraman R, Mouloua M, eds. *Automation and Human Performance: Theory and Applications* (Lawrence Erlbaum, Mahwah, NJ), 163–181.
- Federal Aviation Administration (FAA) (2013) *Safety Alert for Operators—Manual Flight Operations* (Federal Aviation Administration, Washington, DC).
- Farjoun M (2010) Beyond dualism: Stability and change as a duality. *Acad. Management Rev.* 35(2):202–225.
- Farjoun M, Starbuck WH (2007) Organizing at and beyond the limits. *Organ. Stud.* 28(4):541–566.
- Galbraith JR (1974) Organization design: An information processing view. *Interfaces* 4(3):28–36.
- Garud R, Dunbar RL, Bartel CA (2011) Dealing with unusual experiences: A narrative perspective on organizational learning. *Organ. Sci.* 22(3):587–601.
- Grose VL (1988) Coping with boredom in the cockpit before it's too late. *Risk Management* 35(8):30–35.
- Harris D (2011) *Human Performance on the Flight Deck* (Ashgate Publishing, Farnham, UK).
- Harris D (2014) Improving aircraft safety. *Psychologist* 27(2):90–94.
- Haunschild PR, Polidoro F Jr, Chandler D (2015) Organizational oscillation between learning and forgetting: The dual role of serious errors. *Organ. Sci.* 26(6):1682–1701.
- Holweg M, Oliver N (2016) *Crisis, Resilience and Survival: Lessons from the Global Auto Industry* (Cambridge University Press, Cambridge, UK).
- International Air Transport Association (IATA) (2015) *Loss of Control In-Flight Accident Analysis Report, 2010–2014*, 1st ed. (International Air Transport Association, Montreal).
- Karasek RA, Jr (1979) Job demands, job decision latitude, and mental strain: Implications for job redesign. *Admin. Sci. Quart.* 24(2):285–308.
- Lawrence PR, Lorsch JW (1986) *Organization and Environment: Managing Differentiation and Integration* (Irwin, Homewood, IL).
- Lazarus RS, Folkman S (1984) *Stress, Appraisal, and Coping* (Springer Publishing Company, New York).
- Learmount D (2011) AF447. full.mov. Accessed June 1, 2017, <https://www.youtube.com/watch?v=ARybu2kHeZ8>.
- Leveson N, Dulac N, Marais K, Carroll J (2009) Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Organ. Stud.* 30(2–3):227–249.
- March JG (1999) *The Pursuit of Organizational Intelligence: Decisions and Learning in Organizations* (Blackwell Publishers, Hoboken, NJ).
- March JG, Simon HA (1958) *Organizations* (Wiley, Oxford, UK).
- Mintzberg H (1989) *Mintzberg on Management: Inside Our Strange World of Organizations* (Simon and Schuster, New York).
- Ocasio W (1997) Towards an attention-based view of the firm. *Strategic Management J.* 18(Summer):187–206.
- Ocasio W (2005) The opacity of risk: Language and the culture of safety in NASA's space shuttle program. Starbuck W, Farjoun M, eds. *Organization at the Limit: Lessons from the Columbia Disaster* (Blackwell Publishing, Oxford, UK), 101–121.
- Ocasio W (2011) Attention to attention. *Organ. Sci.* 22(5):1286–1296.
- Palmer B (2013) *Understanding Air France 447* (Publisher: Author).
- Parasuraman R, Wickens CD (2008) Humans: Still vital after all these years of automation. *Human Factors: J. Human Factors Ergonom. Soc.* 50(3):511–520.
- Perrow C (1984) *Normal Accidents: Living with High-Risk Technologies* (Basic Books, New York).
- Plant KL, Stanton NA (2012) Why did the pilots shut down the wrong engine? Explaining errors in context using schema theory and the perceptual cycle model. *Safety Sci.* 50(2):300–315.
- Reason J (1997) *Managing the Risks of Organizational Accidents* (Ashgate, Farnham, UK).
- Reason J (2000a) Human error: Models and management. *British Medical J.* 320(7237):768–770.
- Reason J (2000b) Safety paradoxes and safety culture. *Injury Control Safety Promotion* 7(1):3–14.
- Richardson B (1995) Paradox management for crisis avoidance. *Management Decision* 33(1):5–18.
- Roberts KH (1990) Some characteristics of one type of high reliability organization. *Organ. Sci.* 1(2):160–176.
- Roberts KH, Rousseau DM (1989) Research in nearly failure-free, high-reliability organizations: Having the bubble. *Engrg. Management, IEEE Trans.* 36(2):132–139.

- Rochlin GI (1993) Defining “high reliability” organizations in practice: A taxonomic prologue. Savendy G, ed. *New Challenges to Understanding Organizations* (Wiley, Oxford, UK), 11–32.
- Rochlin GI (1997) *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton University Press, Princeton, NJ).
- Roe E, Schulman PR (2008) *High Reliability Management: Operating on the Edge* (Stanford University Press, Palo Alto, CA).
- Rouse WB, Geddes ND, Curry RE (1987) An architecture for intelligent interfaces: Outline of an approach to supporting operators of complex systems. *Hum.-Comput. Interact.* 3(2):87–122.
- Royal Aeronautical Society Flight Operations Group (RASFOG) (2010) *Aeroplane Upset Recovery Training, History, Core Concepts and Mitigation* (Royal Aeronautical Society, London).
- Sagan SD (1995) *Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (American Association for the Advancement of Science, Washington, DC).
- Sarter NB, Woods DD, Billings CE (1997) Automation surprises. Savendy G, ed. *Handbook of Human Factors and Ergonomics* (Wiley, Oxford), 1926–1943.
- Sastry MA (1997) Problems and paradoxes in a model of punctuated organizational change. *Admin. Sci. Quart.* 42(2):237–275.
- Simon HA (1972) Theories of bounded rationality. *Decision Organ.* 1(1):161–176.
- Simon HA (1982) *Models of Bounded Rationality: Empirically Grounded Economic Reason* (MIT Press, Cambridge, MA).
- Starbuck W, Farjoun M (2005) *Organization at the Limit: Lessons from the Columbia Disaster* (Blackwell Publishing, Malden, MA).
- Starbuck W, Stephenson J (2005) Making NASA more effective. Starbuck W, Farjoun M, eds. *Organization at the Limit: Lessons from the Columbia Disaster* (Blackwell Publishers, Oxford, UK), 309–335.
- Starbuck WH (2009) Perspective-cognitive reactions to rare events: Perceptions, uncertainty, and learning. *Organ. Sci.* 20(5):925–937.
- Sutcliffe KM, Vogus TJ, Dane E (2016) Mindfulness in organizations: A cross-level review. *Annual Rev. Organ. Psych. Organ. Behav.* 3(March):55–81.
- Syed M (2015) *Black Box Thinking: The Surprising Truth About Success* (John Murray, London).
- Vaughan D (1997) *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (University of Chicago Press, Chicago).
- Weick KE (1990a) Technology as equivoque: Sensemaking in new technologies. Goodman P, Sproull, eds. *Technology and Organizations* (Jossey-Bass, San Francisco), 1–44.
- Weick KE (1990b) The vulnerable system: An analysis of the Tenerife air disaster. *J. Management* 16(3):571–593.
- Weick KE (1993) The collapse of sensemaking in organizations—The Mann Gulch disaster. *Admin. Sci. Quart.* 38(4):628–652.
- Weick KE (2005) Making sense of blurred images: Mindful organizing in mission STS-107. Starbuck W, Farjoun M, eds. *Organization at the Limit* (Blackwell Publishing, Oxford, UK), 159–177.
- Weick KE (2010) Reflections on enacted sensemaking in the Bhopal disaster. *J. Management Stud.* 47(3):537–550.
- Weick KE (2016) 60th Anniversary essay constrained comprehending: The experience of organizational inquiry. *Admin. Sci. Quart.* 61(3):333–346.
- Weick KE, Roberts KH (1993) Collective mind in organizations—Heedful interrelating on flight decks. *Admin. Sci. Quart.* 38(3):357–381.
- Weick KE, Sutcliffe KM (2007) *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (Jossey-Bass, San Francisco).
- Weick KE, Sutcliffe KM, Obstfeld D (1999) Organizing for high reliability: Processes of collective mindfulness. Sutton RI, Staw BM, eds. *Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews*, Vol. 21 (JAI Press, Stamford, CT.), 81–123.
- Weiner EL (1989) Human factors of advanced (“glass cockpit”) transport aircraft. Report, NASA, Ames Research Center, Moffett Field, CA.
- Young JP, Fanjoy RO, Suckow MW (2006) Impact of glass cockpit experience on manual flight skills. *J. Aviation/Aerospace Education Res.* 15(2):27–32.
- Yu T, Sengul M, Lester RH (2008) Misery loves company: The spread of negative impacts resulting from an organizational crisis. *Acad. Management Rev.* 33(2):452–472.

Nick Oliver is professor of management at the University of Edinburgh Business School, United Kingdom. He received his PhD in organizational psychology from the Open University, United Kingdom. His research focuses on high performance organization, in particular lean and resilient organizational forms. He is coauthor of *The Japanization of British Industry* (1992) and *Crisis, Resilience and Survival: Lessons from the Global Auto Industry* (2016).

Thomas Calvard is lecturer in organization studies at the University of Edinburgh Business School. He received his PhD in organizational psychology from the University of Sheffield. His research focuses on the sensemaking processes surrounding diversity, technology, and boundaries in organizations.

Kristina Potočník is senior lecturer in human resource management at the University of Edinburgh Business School. She received her PhD in psychology from the University of Valencia. Kristina’s research explores diverse factors that determine individual, team, and organizational performance, looking particularly at how creative and innovative performance can be fostered in different organizational settings.