CHAPTER

5

The High Reliability Organization Perspective

Sidney W.A. Dekker and David D. Woods
Lund University School of Aviation SE—260 70
Ljungbyhed Sweden

s0010

INTRODUCTION

p0010 High reliability theory describes the extent and nature of the effort that people, at all levels in an organization, have to engage in to ensure consistently safe operations despite its inherent complexity and risks. It is founded on an empirical research base that shows how safety originates in large part in the managerial and operational activities of people at all levels of an organization. The high reliability organizations (HROs) perspective is relevant here, since aviation has done an effective job in institutionalizing and systematizing its learning from incidents and accidents. HRO, however, tries to go further—pulling learning forward in time, studying how managerial and operational activities can encourage the exploration and exchange of safety-related information. The aim is to pick up early signs that trouble may be on the horizon and then be able to make modifications without having to wait for the more obvious signs of failure in the form of incidents or accidents. HROs are able to stay curious about their own operations and keep wondering why they are successful. They stay open-minded about the sources of risk, try to remain complexly sensitized to multiple sources of safety information, keep inviting doubt and

minority opinion, and stay ambivalent toward the past, so that confidence gleaned from previous results are not taken as a guarantee of future safety (Weick, 1993).

p0020 This chapter first considers some of the origins of HRO, then addresses the "reliability" part of its label as applied to aviation safety in part on the basis of an example of a systems accident, and concludes with how Resilience Engineering represents the action agenda of HRO (Hollnagel et al., 2006). With an emerging set of techniques and models to track how organizations learn, adapt and change without waiting for major failures, Resilience Engineering introduces ways to indicate where overconfidence in past results may be occuring, where minority viewpoints may risk getting downplayed, and where acute performance or production demands may trump chronic safety concerns. The reason such instrumentality is important for aviation is both its high safety and its complexity: accidents have long ceased to be the result from single component failures. Rather, they emerge from the system's organized complexity (Amalberti, 2001). It takes more than tracking individual component behavior to anticipate whether aviation systems can keep coping with change and complexity.

s0020 HRO: SOME ORIGINS

p0030 Through a series of empirical studies, HRO researchers have found that through leadership safety objectives, the maintenance of relatively closed systems, functional decentralization, the creation of a safety culture, redundancy of equipment and personnel, and systematic learning, organizations can achieve the consistency and stability required to effect nearly failure-free operations (LaPorte and Consolini, 1991). Some of these categories were very much inspired by the worlds studied—naval aircraft carrier air operations, for example (Rochlin, LaPorte, and Roberts, 1987). There, in a relatively self-contained and disconnected closed system, systematic learning was an automatic by-product of the swift rotations of naval personnel, turning everybody into instructor and trainee, often at the same time. Functional decentralization meant that complex activities (like landing an aircraft and arresting it with the

wire at the correct tension) were decomposed into simpler and relatively homogenous tasks, delegated down into small workgroups with substantial autonomy to intervene and stop the entire process independent of rank. HRO researchers found many forms of redundancy—in technical systems, supplies, even decision-making and management hierarchies, the latter through shadow units and multiskilling.

p0040 When HRO researchers first set out to examine how safety is created and maintained in such complex systems, they took an approach that can be found in parts of aviation human factors today. They focused on errors and other negative indicators, such as incidents, assuming that these were the basic units that people in these organizations used to map the physical and dynamic safety properties of their production technologies, ultimately to control risk (Rochlin, 1999). The assumption turned out wrong: they were not. Operational people, those who work at the sharp end of an organization, hardly defined safety in terms of risk management or error avoidance. Ensuing empirical work by HRO, stretching across decades and a multitude of high-hazard, complex domains (aviation, nuclear power, utility grid management, navy) would paint a more complex, and in many ways a more constructive picture with safety not being the *absence* of negatives, but rather the *presence* of certain activities to manage risk. HRO began to describe how operational safety—how it is created, maintained, discussed, mythologized—should be captured as much more than the control of negatives. As Rochlin (1999, p. 1549) put it,

> the culture of safety that was observed is a dynamic, intersubjectively constructed belief in the possibility of continued operational safety, instantiated by experience with anticipation of events that could have led to serious errors, and complemented by the continuing expectation of future surprise.

p0050 The creation of safety, in other words, involves a belief about the possibility to continue operating safely (Woods and Cook, 2003). This belief is built up and shared among those who do the work every day. It is moderated or even held up in part by the constant preparation for future surprise—preparation for situations that

may challenge people's current assumptions about what makes their operation risky or safe. And yes, it is also a belief punctuated by encounters with risk. But errors, or any other negatives, function at most as the narrative spice that keeps the belief flavorful and worth sharing. They turned out not to be its main substance.

p0060 Intriguingly, the label "high reliability" grew increasingly at odds with the findings this school produced. What was a research effort to examine how high-risk systems can produce high-reliability outcomes despite their inherent danger (i.e., measured in terms of reducing negatives, or failure events), transmogrified into a discovery of safety as a reflexive social construct that challenged virtually all available methodological, ontological and theoretical guidance available at the time. Safety, HRO concluded, does not exist "out there," independent from the minds or actions of the people who create it through their practice, simply to be discovered, laid bare, by those with the right measuring instrument. Knowing about safety cannot be synonymous with a tabulation of "objective" measures from real-world performance. And, indeed, the predictive value of such measures is generally quite disappointing. While ensuring consistent and reliable component performance (both human and machine) has been a hugely important contributor to the successful safety record of aviation to date, there are limits to this approach, particularly when it comes to avoiding complex system accidents that emerge from the normal functioning of already almost totally safe transportation systems (Amalberti, 2001).

s0030 Reliability and its Effects on Safety

p0070 To be sure, safety is not the same as reliability. A part can be reliable, but in and of itself it cannot be safe. It can perform its stated function to the expected level or amount, but it is context, the context of other parts, of the dynamics and the interactions and cross-adaptations between parts, that make things safe or unsafe. Reliability as an engineering property can be expressed as a component's failure rate or probablilities over a period of time. In other words, it addresses the question of whether a component lives up to its prespecified performance criteria. Organizationally, reliability is often associated with a reduction in variability, and concomitantly,

with an increase in replicability: the same process, narrowly guarded, produces the same predictable outcomes. Becoming highly reliable may be a desirable goal for unsafe or moderately safe operations (Amalberti, 2001). The guaranteed production of standard outcomes through consistent component performance is a way to reduce failure probability in those operations, and it is often expressed as a drive to eliminate errors and technical breakdowns.

p0080 In moderately safe systems, such as chemical industries, driving or chartered flights, approaches based on reliability can still generate significant safety returns (Amalberti, 2001). Regulations and safety procedures have a way of converging practice onto a common basis of proven performance. Collecting stories about negative near-miss events (errors, incidents) has the benefit in that the same encounters with risk show up in real accidents that happen to that system. There is, in other words, an overlap between the ingredients of incidents and the ingredients of accidents: recombining incident narratives has predictive (and potentially preventive) value. Finally, developing error-resistant and error-tolerant designs helps prevent errors from becoming incidents or accidents.

p0090 The monitoring of performance through operational safety audits, error counting, flight data collection, and incident tabulations has become institutionalized and in many cases required by legislation or regulation. The latest incarnation, an integrative effort to make both safety management and its inspection more streamlined with other organizational processes, is known as the Safety Management System (SMS), which is now demanded in most Western countries by regulators. Safety management systems typically encompass a process for identifying hazards to aviation safety and for evaluating and managing the associated risks, a process for ensuring that personnel are trained and competent to perform their duties and a process for the internal reporting and analyzing of hazards, incidents and accidents and for taking corrective actions to prevent their recurrence. The SMS is also about itself; about the bureaucratic accountability it both represents and spawns. Regulators typically demand that an SMS contains considerable documentation containing all safety management

system processes and a process for making personnel aware of their responsibilities with respect to them. Quality assurance and safety management within the airline industry are often mentioned in the same sentence or used under one department heading. The relationship is taken as non-problematic or even coincident. Quality assurance is seen as a fundamental activity in risk management. Good quality management will help ensure safety. This idea, together with the growing implementation of SMS, may indeed have helped aviation attain even stronger safety records than before, as SMSs help focus decision makers' attention on risk management and safety aspects of both organizational and technological change, forcing an active consideration and documentation of how that risk should be managed.

p0100 One possible downside is that pure quality assurance programs (or reliability in the original engineering sense) contain decomposition assumptions that may not really be applicable to systems that are overall as complex as aviation (see Leveson, 2006). For example, it suggests that each component or subsystem (layer of defense) operates reasonably independently, so that the results of a safety analysis (e.g., inspection or certification of people or components or subsystems) are not distorted when we start putting the pieces back together again. It also assumes that the principles that govern the assembly of the entire system from its constituent subsystems or components is straightforward. And that the interactions, if any, between the subsystems will be linear: not subject to unanticipated feedback loops or nonlinear interactions.

p0110 The assumptions of such a reliability (or quality assurance) approach imply that aviation must continue to strive for systems with high theoretical performance and a high safety potential. A less useful portion of this notion, of course, is the elimination of component breakdowns (e.g., human errors), but it is still a widely pursued goal, sometimes suggesting that the aviation industry today is the custodian of an already safe system that needs protection from unpredictable, erratic components that are its remaining sources of unreliability. This common sense approach, says Amalberti (2001), which indeed may have helped aviation progress to the safety levels of today, is perhaps less applicable to a system

that has the levels of complexity and safety already enjoyed today. This is echoed by Vaughan (1996, p. 416):

> …we should be extremely sensitive to the limitations of known remedies. While good management and organizational design may reduce accidents in certain systems, they can never prevent them … technical system failures may be more difficult to avoid than even the most pessimistic among us would have believed. The effect of unacknowledged and invisible social forces on information, interpretation, knowledge, and—ultimately—action, are very difficult to identify and to control.

p0120 As progress on safety in aviation has become asymptotic, further optimization of this approach is not likely to generate significant safety returns. In fact, there could be indications that continued linear extensions of a traditional-componential reliability approach could paradoxically help produce a new kind of system accident at the border of almost totally safe practice (Amalberti, 2001, p. 110):

> The safety of these systems becomes asymptotic around a mythical frontier, placed somewhere around 5×10^{-7} risks of disastrous accident per safety unit in the system. As of today, no man-machine system has ever crossed this frontier, in fact, solutions now designed tend to have devious effects when systems border total safety.

p0130 The aviation accident described in the following section may illustrate some of the challenges ahead in terms of thinking about what reliability (or HRO) really should mean in aviation. Through a concurrence of functions and events, of which a language barrier was a product as well as constitutive, the flight of a Boeing 737 out of Cyprus in 2005 may have been pushed past the edge of chaos, into that area in nonlinear dynamic behavior where new system behaviors emerged that could be difficult to anticipated using a logic of decomposition. The accident encourages us to consider HRO for its ability to monitor higher-order system properties: the system's ability to recognize, adapt to, and absorb disruptions that fall outside the disturbances it was designed to handle.

s0040 An Accident Perhaps Beyond the Reach of Traditional Reliability

p0140 On August 13, 2005, on the flight before the accident, a Helios Airways Boeing 737−300 flew from London to Larnaca, Cyprus. The cabin crew noted a problem with one of the doors, and convinced

the flight crew to write that the "Aft service door requires full inspection" in the aircraft logbook. Once in Larnaca, a ground engineer performed an inspection of the door and carried out a cabin pressurization leak check during the night. He found no defects. The aircraft was released from maintenance at 03:15 and scheduled for flight 522 at 06:00 via Athens, Greece to Prague, Czech Republic (AAISASB, 2006).

p0150 A few minutes after taking off from Larnaca, the captain called the company in Cyprus on the radio to report a problem with his equipment cooling and the takeoff configuration horn (which warns pilots that the aircraft is not configured properly for takeoff, even though it evidently had taken off successfully already). A ground engineer was called to talk with the captain, the same ground engineer who had worked on the aircraft in the night hours before. The ground engineer may have suspected that the pressurization switches could be in play (given that he had just worked on the aircraft's pressurization system), but his suggestion to that effect to the captain was not acted on. Instead, the captain wanted to know where the circuit breakers for his equipment cooling were so that he could pull and reset them.

p0160 During this conversation, the oxygen masks deployed in the passenger cabin as they are designed to do when cabin altitude exceeds 14,000 feet. The conversation with the ground engineer ended, and would be the last that would have been heard from Flight 522. Hours later, the aircraft finally ran out of fuel and crashed in hilly terrain north of Athens. Everybody on board had been dead for hours, except for one cabin attendant who held a commercial pilots license. Probably using medical oxygen bottles to survive, he finally had made it into the cockpit, but his efforts to save the aircraft were too late. The pressurization system had been set to manual so that the engineer could carry out the leak check. It had never been set back to automatic (which is done in the cockpit), which meant the aircraft did not pressurize during its ascent, unless a pilot had manually controlled the pressurization outflow valve during the entire climb. Passenger oxygen had been available for no more than 15 minutes, the captain had left his seat, and the co-pilot had not put on an oxygen mask.

p0170 Helios 522 is illustrative, because nothing was "wrong" with the components. They all met their applicable criteria. "The captain and First Officer were licensed and qualified in accordance with applicable regulations and Operator requirements. Their duty time, flight time, rest time, and duty activity patterns were according to regulations. The cabin attendants were trained and qualified to perform their duties in accordance with existing requirements" (AAISASB, 2006, p. 112). Moreover, both pilots had been declared medically fit, even though postmortems revealed significant arterial clogging that may have exacerbated the effects of hypoxia. And while there are variations in what JAR-compliant means across Europe, the Cypriot regulator (Cyprus DCA, or Department of Civil Aviation) complied with the standards in JAR OPS 1 and Part 145. This was seen to with help from the U.K. CAA, who provided inspectors for flight operations and airworthiness audits by means of contracts with the DCA. Helios and the maintenance organization were both certified by the DCA.

p0180 The German captain and the Cypriot co-pilot met the criteria set for their jobs. Even when it came to English, they passed. They were within the bandwidth of quality control within which we think system safety is guaranteed, or at least highly likely. That layer of defense—if you choose speak that language—had no holes as far as our system for checking and regulation could determine in advance. And we thought we could line these subsystems up linearly, without complicated interactions. A German captain, backed up by a Cypriot co-pilot. In a long-since certified airframe, maintained by an approved organization. The assembly of the total system could not be simpler. And it must have, should have, been safe.

p0190 Yet there was a brittleness of having individual components meet prespecified criteria which became apparent when compounding problems pushed demands for crew coordination beyond the routine. As the AAISASB observed, "Sufficient ease of use of English for the performance of duties in the course of a normal, routine flight does not necessarily imply that communication in the stress and time pressure of an abnormal situation is equally effective. The abnormal situation can potentially require words that are

not part of the "normal" vocabulary (words and technical terms one used in a foreign tongue under normal circumstances), thus potentially leaving two pilots unable to express themselves clearly. Also, human performance, and particularly memory, is known to suffer from the effects of stress, thus implying that in a stressful situation the search and choice of words to express one's concern in a non-native language can be severely compromised. …In particular, there were difficulties due to the fact that the captain spoke with a German accent and could not be understood by the British engineer. The British engineer did not confirm this, but did claim that he was also unable to understand the nature of the problem that the captain was encountering" (pp. 122–123).

p0200 The irony is that the regulatory system designed to standardize aviation safety across Europe, has, through its harmonization of crew licensing, also legalized the blending of a large number of crew cultures and languages inside of a single airliner, from Greek to Norwegian, from Slovenian to Dutch. On August 14, 2005, this certified system may not have been able to recognize, adapt to, and absorb a disruption that fell outside the set of disturbances it was designed to handle. The "stochastic fit" (see Snook, 2000) that put together this crew, this engineer, from this airline, in this airframe, with these system anomalies, on this day, outsmarted how we all have learned to adapt, create and maintain safety in an already very safe industry. Helios 522 testifies that the quality of individual components or subsystems cannot always effectively predict how they can recombine to create novel pathways to failure (see Dekker, 2005).

s0050 Emergence and Resilience

p0210 Helios 522 in a sense represents the temporary inability to cope effectively with complexity. This is true, of course, for the cockpit crew after climbing out from Larnaca, but this is even more interesting at a larger system level. It was the system of pilot and airline certification, regulation, in an environment of scarcity and competition, with new operators in a market role which they not only fulfill but also help constitute beyond traditional Old Europe boundaries—that could not recognize, adapt to, and absorb a

disruption that fell outside the set of disturbances the system was designed to handle (see Rochlin, 1999; Weick et al., 1999; Woods, 2003; 2005; Hollnagel et al., 1996). The "stochastic fit" (see Snook, 2000) or functional resonance (Hollnagel, Woods, and Leveson, 2006) that put together this crew, from this airline, in this airframe, with these system anomalies, on this day, in a way challenged how an industry learned to adapt, create and maintain safety when it was already very safe.

p0220 It could be interesting to shift from a mechanistic interpretation of complex systems to a systemic one. A machine can be controlled, and it will "fail" or perform less well or run into trouble when one or more of its components break. In contrast, a living system can be disturbed to any number of degrees. Consequently, its functioning is is much less binary, and potentially much more resilient. Such resilience means that failure is not really, or can't even really be, the result of individual or compound component breakage. Instead, it is related to the ability of the system to adapt to, and absorb variations, changes, disturbances, disruptions and surprises. If it adapts well, absorbs effectively, then even compound component breakages may not hamper chances of survival. United 232 in July 1989 is a case in point. After losing control of the aircraft's control surfaces as a result of a center engine failure that ripped fragments through all three hydraulic lines nearby, the crew figured out how to maneuver the aircraft with differential thrust on two remaining engines. They managed to put the crippled DC-10 down at Sioux City, saving 185 lives out of 293.

p0230 Simple things can generate very complex outcomes that could not be anticipated by just looking at the parts themselves. Small changes in the initial state of a complex system (e.g., a Cypriot and German pilot, rather than, say, two Cypriot ones) can drastically alter the final outcome. The underlying reason for this is that complex systems are dynamically stable, not statically so (like machines): instability emerges not from components, but from concurrence of functions and events in time. The essence of resilience is the intrinsic ability of a system to maintain or regain a dynamically stable state (Hollnagel, Woods, and Leveson, 2006).

p0240 Practitioners and organizations, as adaptive systems, continually assess and revise their approaches to work in an attempt to remain sensitive to the possibility of failure. Efforts to create safety, in other words, are ongoing. Not being successful is related to limits of the current model of competence, and, in a learning organization, reflects a discovery of those boundaries. Strategies that practitioners and organizations (including regulators and inspectors) maintain for coping with potential pathways to failure can either be strong or resilient (i.e., well-calibrated) or weak and mistaken (i.e., ill-calibrated). Organizations and people can also become overconfident in how well-calibrated their strategies are. High-reliability organizations remain alert for signs that circumstances exist, or are developing, in which that confidence is erroneous or misplaced (Rochlin, 1993; Gras, Moricot, Poirot-Delpech, and Scardigli, 1994). This, after all, can avoid narrow interpretations of risk and stale strategies (e.g., checking quality of components).

p0250 Resilience is the system's ability to effectively adjust to hazardous influences, rather than resist or deflect them (Hollnagel, Woods, and Leveson, 2006). The reason for this is that these influences are also ecologically adaptive and help guarantee the system's survival. Engaging crews from different (lower-wage) countries makes it possible to keep flying even with oil prices at record highs. But effective adjustment to these potentially hazardous influences did not occur at any level in the system in this case. The systems perspective, of living organizations whose stability is dynamically emergent rather than structurally inherent, means that safety is something a system does, not something a system has (Hollnagel, Woods, and Leveson, 2006; Hollnagel, 2009). Failures represent breakdowns in adaptations directed at coping with complexity (Woods, 2003). Learning and adaptation as advocated by HRO are ongoing—without it, safety cannot be maintained in a dynamic and changing organizational setting and environment. As HRO research found, this involves multiple rationalities, reflexivity and self-consciousnesses, since the ability to identify situations that had the potential to evolve into real trouble (and separate them from the ones that did not) is in itself part of the safe operation as social construct. Differently positioned actor-groups are learning,

and are learning different things at different times—never excluding their own structure or social relations from the discourse in which that learning is embedded (Rochlin, 1999).

s0060 **Ensuring Resilience in High-Reliability Organizations**

p0260 The HRO perspective has given credence to the notion of safety as something that an organization does, not something that an organization has. How can we collapse some of these research results into useful guidance for organizations in aviation and elsewhere? How can we keep an organization's belief in its own continued safe operation curious, open-minded, complexly sensitized, inviting of doubt, and ambivalent toward the past? Resilience is in some sense the latest action agenda of HRO, with some of the following items:

p0270 *Not taking past success as guarantee of future safety.* Does the system see continued operational success as a guarantee of future safety, as an indication that hazards are not present or that countermeasures in place suffice? In their work, HRO researchers found how safe operation in commercial aviation depends in part on front-line operators treating their operational environment not only as inherently risky, but also as actively hostile to those who misestimate that risk (Rochlin, 1993). Confidence in equipment and training does not take away the need operators see for constant vigilance for signs that a situation is developing in which that confidence is erroneous or misplaced (Rochlin, 1999). Weick (1993) cites the example of Naskapi Indians who use caribou shoulder bones to locate game. They hold the bones over a fire until they crack and then hunt in the directions where the cracks point. This means future decisions about where to hunt are not influenced by past success, so the animal stock is not depleted and game does not get a chance to habituate to the Indians' hunting patterns. Not only are past results not taken as reason for confidence in future ones—*not* doing so actually increases future chances of success.

p0280 *Distancing through differencing.* In this process, organizational members look at other incidents or failures in other organizations or subunits as not relevant to them and their situation (Cook and Woods, 2006). They discard other events because they appear to be

dissimilar or distant. But just because the organization or section has different technical problems, different operational settings, different managers, different histories, or can claim to already have addressed a particular safety concern revealed by the event, does not mean that they are immune to the problem. Seemingly divergent events can represent similar underlying patterns in the drift toward hazard.

p0290 *Fragmented problem solving.* It could be interesting to probe to what extent problem-solving activities are disjointed across organizational departments, sections or subcontractors, as discontinuities and internal handovers of tasks increase risk (Patterson, Roth, Woods, Chow, and Gomez, 2004). With information incomplete, disjointed and patchy, nobody may be able to recognize the gradual erosion of safety constraints on the design and operation of the original system (Woods, 2005). HRO researchers have found that the importance of free-flowing information cannot be overestimated. A spontaneous and continuous exchange of information relevant to normal funtioning of the system offers a background from which signs of trouble can be spotted by those with the experience to do so (Weick, 1993; Rochlin, 1999). Research done on handovers, which is one coordinative device to avert the fragmentation of problem-solving (Patterson et al., 2004) has identified some of the potential costs of failing to be told, forgetting, or misunderstanding information communicated. These costs, for the incoming crew, include:

u0010 • Having an incomplete model of the system's state;
u0020 • Being unaware of significant data or events;
u0030 • Being unprepared to deal with impacts from previous events;
u0040 • Failing to anticipate future events;
u0050 • Lacking knowledge that is necessary to perform tasks safely;
u0060 • Dropping or reworking activities that are in progress or that the team has agreed to do;
u0070 • Creating an unwarranted shift in goals, decisions, priorities, or plans.

p0370 *The courage to say no.* Having a person or function within the system with the authority, credibility and resources to go against common interpretations and decisions about safety and risk (Woods, 2006).

A shift in organizational goal trade-offs often proceed gradually as pressure leads to a narrowing focus on some goals while obscuring the trade-off with other goals. This process usually happens when acute goals like production/efficiency take precedence over chronic goals like safety. If uncertain "warning" signs always led organizations to make sacrifices on schedule and efficiency, it would be difficult to meet competitive and stakeholder demands. By contrast, if uncertain "warning" signs are always rationalized away the organization is acting much riskier than it realizes or wishes. Sometimes people need the courage to put chronic goals ahead of acute short term goals. Thus it is necessary for organizations to support people when they have the courage to say "no" (e.g., in procedures, training, feedback on performance) as these moments serve as reminders of chronic concerns even when the organization is under acute pressures that easily can trump the warnings (see Dekker, 2007, about how to create a Just Culture). Resilient systems build in this function at meaningful organizational levels, which relates to the next point.

p0380 *The ability to bring in fresh perspectives.* Systems that apply fresh perspectives (e.g., people from another backgrounds, diverse viewpoints) on problem-solving activities seem to be more effective: they generate more hypotheses, cover more contingencies, openly debate rationales for decision making, reveal hidden assumptions (Watts-Perotti & Woods, 2009). In HRO studies of some organizations constant rotation of personnel turned out to be valuable in part because it helped introduce fresh viewpoints in an organizationally and hierarchically legitimate fashion (Rochlin, 1999). Crucially important here is also the role of minority viewpoints, those that can be dismissed easily because they represent dissent from a smaller group. Minority viewpoints can be blocked because they deviate from the mainstream interpretation which will be able to generate many reasons the minority view misunderstands current conditions and retards the organizations formal plans (Woods, 2006b). The alternative readings that minority viewpoints represent, however, can offer a fresh angle that reveals aspects of practice that were obscured from the mainstream perspective (Starbuck and Farjoun, 2005). Historically, "whistleblowers" may hail from lower

ranks where the amount of knowledge about the extent of the problem is not matched by the authority or resources to do something about it or have the system change course (Vaughan, 1996). Yet in risky judgments we have to defer to those with technical expertise (and have to set up a problem-solving process that engages those practiced at recognizing anomalies in the event).

p0390 All of this can serve to *keep a discussion about risk alive* even (or especially) when everything looks safe. One way is to see whether activities associated with recalibrating models of safety and risk are going on at all. Encouraging this behavior typically creates forums where stakeholders can discuss risks even when there is no evidence of risk present in terms of current safety statistics. As Weick (1993) illustrates, extreme confidence and extreme caution can both paralyze people and organizations because they sponsor a closed-mindedness that either shuns curiosity or deepens uncertainties (see also DeKeyser and Woods, 1990). But if discussions about risk are going on even in the absence of obvious threats to safety, one could get some confidence that an organization is investing in an analysis, and possibly in a critique and subsequent update, of its models of how it creates safety.

p0400 *Knowing the gap between work-as-imagined and work-as-practiced.* One marker of resilience is the distance between operations as management imagines they go on and how they actually go on. A large distance indicates that organizational leadership may be mis-calibrated to the challenges and risks encountered in real operations. Also, they may also miss how safety is actually created as people conduct work, construct discourse and rationality around it, and gather meaning from it (Weick et al., 1999; Dekker, 2006).

p0410 *Monitoring of safety monitoring (or meta-monitoring).* In developing their safety strategies and risk countermeasures, organizations should invest in an awareness of the models of risk they believe in and apply. This is important if organizations want to avoid stale coping mechanisms, misplaced confidence in how they regulate or check safety, and if do not want to miss new possible pathways to failure. Such meta-monitoring would obviously represent an interesting new task for regulators in aviation worldwide, but it applies reflexively to themselves, too. The most important

ingredient of engineering a resilient system is constantly testing whether ideas about risk still match with reality; whether the model of operations (and what makes them safe or unsafe) is still up to date—at every level in the operational, managerial and regulatory hierarchy.

s0070 **High Resilience Organizations**

p0430 Over the past two decades, high reliability research has begun to show how organizations can manage acute pressures of performance and production in a constantly dynamic balance with chronic concern for safety. Safety is not something that these organizations have, it is something that organizations do. Practitioners and organizations, as adaptive systems, continually assess and revise their work so as to remain sensitive to the possibility of failure. Efforts to create safety are ongoing, but not always successfully so. An organization usually is unable to change its model of itself unless and until overwhelming evidence accumulates that demands revising the model. This is a guarantee that the organization will tend to learn late, that is, revise its model of risk only after serious events occur. The crux is to notice the information that changes past models of risk and calls into question the effectiveness of previous risk reduction actions, without having to wait for complete clear cut evidence. If revision only occurs when evidence is overwhelming, there is a grave risk of an organization acting too risky and finding out only from near misses, serious incidents, or even actual harm. The practice of revising assessments of risk needs to be continuous.

p0440 High reliability organization research is, and will always be, a work in progress, as its language for accommodating the results, and the methodological persuasions for finding and arguing for them, evolves all the time. It is already obvious, though, that traditional engineering notions of reliability (that safety can be maintained by keeping system component performance inside acceptable and prespecified bandwidths) have very little to do with what makes organizations highly reliable (or, rather, resilient). As progress on safety in aviation has become asymptotic, further optimization of this reliability approach is not likely to

generate significant safety returns. In fact, adhering to it may partly become constitutive of new kinds of system accidents, as illustrated by the Helios 522 case in this chapter. Failure in aviation today is not really, or not in any interesting or predictively powerful way, the result of individual or compound component breakage. Instead, it is related to the ability of the industry to effectively adapt to, and absorb variations, changes, disturbances, disruptions, and surprises.

p0450 Resilience Engineering is built on insights derived, in part, from the HRO work described here (Weick et al., 1999; Sutcliffe & Vogus, 2003). It is concerned with assessing organizational risk, that is the risk that holes in organizational decision making will produce unrecognized drift toward failure boundaries. While assessing technical hazards is one kind of input into Resilience Engineering, the goal is to monitor organizational decision making. For example, Resilience Engineering would monitor evidence that effective cross checks are well-integrated when risky decisions are made or that the organization is providing sufficient practice at handling simulated anomalies (and what kind of anomalies are practiced).

p0460 Other dimensions of organizational risk include the commitment of the management to balance the acute pressures of production with the chronic pressures of protection. Their willingness to invest in safety and to allocate resources to safety improvement in a timely, proactive manner, despite pressures on production and efficiency, are key factors in ensuring a resilient organization. The degree to which the reporting of safety concerns and problems is truly open and encouraged provides another significant source of resilience within the organization. Assessing the organization's response to incidents indicates if there is a learning culture or a culture of denial. Other dimensions of organizations which could be monitored include:

p0470 Preparedness/Anticipation: is the organization proactive in picking up on evidence of developing problems versus only reacting after problems become significant?

p0480 Opacity/Observability—does the organization monitor safety boundaries and recognize how close it is to "the edge" in terms

of degraded defenses and barriers? To what extent is information about safety concerns widely distributed throughout the organization at all levels versus closely held by a few individuals?

p0490 Flexibility/Stiffness—how does the organization adapt to change, disruptions, and opportunities?

p0500 Successful, highly reliable aviation organizations in the future will have become skilled at the three basics of Resilience Engineering:

o0010 (1) detecting signs of increasing organizational risk, especially when production pressures are intense or increasing;

o0020 (2) having the resources and authority to make extra investments in safety at precisely the times when it appears least affordable;

o0030 (3) having a means to recognize when and where to make targeted investments to control rising signs of organizational risk and rebalance the safety and production trade-off.

p0540 These mechanisms will produce an organization that creates foresight about changing risks before failures and harm occur.

References

Air Accident Investigation and Aviation Safety Board (AAIASB). (2006). Aircraft accident report (11/2006): Helios Airways flight HCY522, Boeing 737–31S at Grammatiko, Hellas on 14 August 2005. Athens, Greece: Helenic Republic Ministry of Transport and Communications.

Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Safety science, 37*, 109–126.

Cook, R. I., Woods, D. D. (2006). Distancing through Differencing: An Obstacle to Learning Following Accidents. In E. Hollnagel, D. D. Woods, and N. Leveson (Eds.), *Resilience engineering: concepts and precepts* (pp. 329–338). Aldershot, UK: Ashgate.

De Keyser, V., & Woods, D. D. (1990). Fixation errors: Failures to revise situation assessment in dynamic and risky systems. In A. G. Colombo and A. Saiz de Bustamante (Eds.), *System reliability assessment* (pp. 231–251). The Netherlands: Kluwer Academic.

Dekker, S. W. A. (2005). *Ten questions about human error: A new view of human factors and system safety*. Mahwah, NJ: Lawrence Erlbaum Associates.

Dekker, S. W. A. (2006). Resilience Engineering: Chronicling the emergence of a confused consensus. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), Resilience engineering: concepts and precepts (pp. 77–92). Aldershot, UK: Ashgate.

Dekker, S. W. A. (2007). Just Culture: Balancing safety and accountability. Aldershot, UK: Ashgate.

Gras, A., Moricot, C., Poirot-Delpech, S. L., & Scardigli, V. (1994). *Faced with automation: The pilot, the controller, and the engineer (trans. J. Lundsten)*. Paris: Publications de la Sorbonne.

Hollnagel, E. (2009). *The ETTO principle, efficiency-thoroughness tradeoff: Why things that go right sometimes go wrong*. Aldershot, UK: Ashgate.

Hollnagel, E., Leveson, N., & Woods, D. D. (Eds.), (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

LaPorte, T. R., & Consolini, P. M. (1991). Working in Practice but not in Theory: Theoretical Challenges of High-Reliability Organizations. *Journal of public administration research and theory*, *1*, 19–47.

Leveson, N. (2006). *A new approach to system safety engineering*. Cambridge, MA: Aeronautics and Astronautics, Massachusetts Institute of Technology.

Patterson, E. S., Roth, E. M., Woods, D. D., Chow, R., & Gomez, J. O. (2004). Handoff strategies in settings with high consequences for failure: Lessons for health care operations. *International journal for quality in health care*, *16*(2), 125–132.

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

Rochlin, G. I., LaPorte, T. R., & Roberts, K. H. (1987). The self-designing high-reliability organization: aircraft carrier flight operations at sea. Naval War College Review Autumn 1987.

Rochlin, G. I. (1993). Defining high-reliability organizations in practice: A taxonomic prolegomenon. In K. H. Roberts (Ed.), *New challenges to understanding organizations* (pp. 11–32). New York: Macmillan.

Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics*, *42*, 1549–1560.

Snook, S. A. (2000). *Friendly fire: the accidental shootdown of us black hawks over northern Iraq*. Princeton, NJ: Princeton University Press.

Starbuck, W. H., & Farjoun, M. (Eds.), (2005). *Organization at the limit: lessons from the columbia disaster*. London: Blackwell Publishing.

Sutcliffe, K., & Vogus, T. (2003). Organizing for resilience. In K. S. Cameron, I. E. Dutton, & R. E. Quinn (Eds.), *Positive organizational scholarship* (pp. 94–110). San Francisco: Berrett-Koehler.

Vaughan, D. (1996). *The challenger launch decision: risky technology, culture and deviance at NASA*. Chicago: University of Chicago Press.

Watts-Perotti, J., & Woods, D. D. (2009). Cooperative Advocacy: A Strategy for Integrating Diverse Perspectives in Anomaly Response. *Computer supported cooperative work: the journal of collaborative computing*, *18*(2), 175–198.

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of management studies*, *25*(4), 305–317.

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative science quarterly*, *38*(4), 628–652.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in organizational behavior*, *21*, 13–81.

Woods, D.D (2003). Creating foresight: How resilience engineering can transform NASA's approach to risky decision making. *US Senate Testimony for the Committee on Commerce, Science and Transportation*, John McCain, chair. Washington, DC, October 29 2003. http://csel.eng.ohio-state.edu/podcasts/woods/.

Woods, D. D. (2005). Creating foresight: Lessons for resilience from *Columbia*. In W. H. Starbuck & M. Farjoun (Eds.), *Organization at the limit: NASA and the columbia disaster* (pp. 289–308). Malden, MA: Blackwell.

Woods, D. D. (2006a). Essential characteristics of resilience for organizations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

Woods, D. D. (2006b). How to design a safety organization: Test case for resilience engineering. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineering: concepts and precepts* (pp. 315–324). Aldershot, UK: Ashgate.

Woods, D. D. (2009). Escaping failures of foresight. *Safety science*, *47*(4), 498–501.

Woods, D. D., & Cook, R. I. (2003). Mistaking error. In M. J. Hatlie & B. J. Youngberg (Eds.), *Patient safety handbook* (pp. 95–108). Sudbury, MA: Jones and Bartlett.

Woods, D. D., Dekker, S. W. A., Cook, R. I., Johannesen, L., & Sarter, N. (in press). *Behind Human Error* (2nd ed). Aldershot, UK: Ashgate.