SCHOOL OF AVIATION
Lund University

Past the edge of chaos

Sidney W. A. Dekker

Technical Report 2006-03

Lund University School of Aviation
Address: 260 70 Ljungbyhed, Sweden
Telephone: +46-435-445400
Fax: +46-435-445464
Email: research@tfhs.lu.se

Abstract

The August 2005 Helios 522 accident may end up demonstrating that the reductionist model we apply to understanding safety and risk in aviation (taking systems apart and checking whether individual components meet prespecified criteria) no longer works well. Through a concurrence of functions and events, of which a language barrier was a product as well as constitutive, Helios 522 may have been pushed past the edge of chaos, that area in non-linear dynamics where new system behaviors emerge that cannot be anticipated using reductive logic. Complexity theory, in contrast, encourages us to fix on higher-order system properties if we want to gain confidence about the resilience of a system, i.e. its ability to recognize, adapt to, and absorb a disruption that falls outside the disturbances the system was designed to handle.

Quality is not the same as safety

Flight Operational Quality Assurance (FOQA) has become mandatory for most large aircraft operators. In its most general sense, Quality Assurance is a system of management activities to ensure that a process, an item, or a service, is of the type and quality demanded by applicable requirements. Quality assurance, then, is about checking whether components or systems meet certain prespecified criteria. 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.

Checking whether individual constituent components of a system meet certain prespecified criteria expresses a particular model of risk and safety. It implies a particular idea about where sources of trouble lie and a model of how accidents occur. Accidents are assumed to occur when individual components or processes fail to meet applicable criteria or migrate outside of prespecified boundaries. Flight Data Monitoring (FDM/FOQA), an important ingredient in airline quality assurance, builds on the idea that safety, once established, can be maintained by keeping the performance of a system's constituent components within certain bounds (people should not violate rules, flight parameters should not exceed particular limits, acme nuts should not wear beyond this or that thread, and so forth). Regulators have now followed this logic for a while too. Their safety oversight, under pressure of resource constraints and efficiency demands, has also oriented itself more toward the examination of operators' quality and safety management systems. This strategy ostensibly allows regulators to fix on higher-order variables and not, for example, send safety inspectors after every single nut and bolt that goes into an aircraft to match it against individual specifications. The idea is that if an airline's quality and safety management systems are in order, most constituent components are likely to be in order too. The practice is called "system oversight" (or self-regulation). Put crudely: you check the system, not the individual components.

If details that have emerged about the August 2005 Helios B737 accident are confirmed by formal investigation, then it poses some really interesting questions about the relationship between quality assurance and safety. It raises the possibility that the inspection and safety assurance regimes applied by the industry are increasingly at odds with the accident models it still assumes to be true. Checking whether individual components meet prespecified criteria, and keeping system performance within externally dictated bounds (e.g. through FDM/FOQA) may not protect us from a Helios 522. Or from an Alaska 261 (see Dekker, 2004).

Language as Disabling Device

As far as is known now, the two cockpit crew members aboard Helios flight 522 met the prespecified European criteria for acting as co-pilot and captain, respectively, on a Boeing 737. Preliminary insights suggest that after take-off from Cyprus, the aircraft did not pressurize well because of anomalies in its pressurization system (International Herald Tribune, 2005). The configuration warning system sounded an alarm after take-off—as designed. This is the same horn that goes off *before* take-off if the aircraft is incorrectly configured (in for example its flap setting) for getting airborne. This may have set a stage for confusion about what was ailing in the aircraft, if anything—a confusion that became compounded by an accelerating mental disorientation resulting from hypoxic hypoxia (cabin pressurization normally keeps the cabin altitude at about 8000 feet).

The aircraft, as programmed, kept climbing on autopilot. When it passed 14,000 feet, oxygen masks deployed in the cabin, and a master caution light illuminated in the cockpit.

About the same time, another alarm started sounding on a slightly related matter, warning that there was insufficient cooling air entering the compartment housing avionics equipment. Confusion escalated. The German captain and Cypriot co-pilot discovered that they did not have enough common ground in English to begin coordinating meaningfully about the problems at hand. This type of swelling situation—a creeping pressurization problem with seemingly unrelated, irrelevant or intrusive alarms —would have pushed any crew (impaired by hypoxia) far off the beaten track where standard ICAO English still sufficed. None of the two cockpit crew members onboard Helios 522 may have commanded enough English to understand the other's attempts at, or proposals for, fixing the problems. Nor did they speak each other's language. Crew coordination beyond routine checklist items and air traffic control clearances would be strenuous, labored, inefficient, arduous, ultimately acrimonious and ineffective.

Upon calling the carrier's maintenance base in Cyprus, they were advised that the circuit breaker to turn off the loud new alarm was in the cabinet behind the captain. The captain got up from his seat to look for the circuit breaker, leaving the confused co-pilot behind at the controls. The aircraft continued to climb on autopilot, and the air grew so thin that the captain passed out first, on the cockpit floor, followed by the co-pilot, who was still in his seat. The autopilot continued to do what it was programmed to do: fly the aircraft to Athens at 34,000 feet and enter a holding pattern. It remained there, shadowed by Greek military jets, until fuel ran low and one engine quit. The thrust imbalance caused the 737 to leave the holding pattern, and it crashed not much later.

Decomposition assumptions of quality management

If we believe that safety can be maintained by keeping system component performance within applicable bounds (and we partially express that belief in Quality Assurance) the combination of a properly trained and certified German captain and Cypriot co-pilot of Helios 522 would have been unproblematic. This is because we make certain decomposition assumptions (see Leveson, 2002). For example, we assume that each component or sub-system operates reasonably independently, so that the results of our safety analysis (e.g. inspection or certification of people or components or sub-systems) are not distorted when we start putting the pieces back together again. It also assumes, by the way, that the principles that govern the assembly of the entire system from its constituent sub-systems or components is straightforward. And that the interactions, if any, between the sub-systems will be linear: not subject to unanticipated feedback loops or non-linear interactions.

The pictorial representation of the popular accident model of the nineties (the Swiss Cheese: subsequent layers of defense with holes in them, see Reason, 1990) may unintentionally sustain and propagate these decomposition assumptions. The sub-systems (e.g. layers of defense) are represented independently, the entire system is assembled straightforwardly from a series of layers, and their interrelationship is linear (the "accident trajectory" through them is a straight line, going through one layer after another). If these assumptions were valid for the systems we inspect and regulate, then looking for the quality of individual components or sub-systems would suffice. But they aren't and it doesn't. Not anymore (cf. Amalberti, 2001).

If what we know now is true, then Helios 522 violates these assumptions. 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 sub-systems 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.
Yet the brittleness of having individual components meet prespecified criteria (e.g., being able to talk standard ICAO English to the satisfaction of an applicable examiner) and think they interact only linearly, would not have been brought to such stark light, were it not for the compounding problems that pushed demands for crew coordination off the routine. A German captain (or Cypriot co-pilot), whose English is sufficient to cover the necessary ICAO utterances, cannot be considered independent of the other crew members he is going to be interacting with, and cannot be considered independently from the possible problems that may have to get solved through efficient crew coordination under pressures of uncertainty, noise, time limitations, and waning oxygen.

Failing to cope with complexity

A system failure such as Helios 522 is not mainly a story about component failures, at least not at any interesting level. (Of course, such an accident story may well be constructed for Helios 522, as it has been for other accidents. But one accident, given its complexity and multifacetted nature, can always be carried in various ways by multiple competing accident stories—none of which is more privileged than others to speak the "truth"). Helios 522 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; Woods, 2003; Hollnagel *et al.*, 1996). The "stochastic fit" (see Snook, 2000) or functional resonance (Hollnagel *et al.*, 2006) that put together this crew, 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.
The probability of such stochastic concurrences would not seem to be going down in Europe either. Nor the potential consequences. Consider the increasing reliance on cabin crew from new, lower-wage, Eastern European member states in an environment of aggressive competition—an industrial-ecological niche where some low-cost carriers flourish. Language barriers there could perhaps easily deplete problem-solving capabilities, especially with problems elsewhere in the aircraft that require coordination across cockpit and cabin crew. And, if history is any guide, traditional, largely monocultural flag carriers may be forced to follow the mix-and-match low-wage suit too—eventually. Helios 522 with only two non-overlapping languages, in just the cockpit, could be a mere beginning, a hint.

Toward a new regulatory future: Making judgments of resilience

Moves towards "system oversight" put regulators and certifiers in a second-order role relative to their previous position. Rather than wanting to know exactly what problems an airline, or other inspection object, is having (e.g. bolts of the wrong size), the regulator wants to get an idea of how well the airline is able to deal with the problems that will come its way. The inspector, in other words, is trying to make a judgment of the resilience of the inspection object. The intention to help create safety through proactive resilient processes, rather than through reactive barriers, is laudable and productive. But the critical question is what to base a judgment of resilience on. This question is only beginning to be examined. Today, if the inspection object has a good quality system, then a regulator may assume that its ability to adapt to deal with novel and unanticipated problems—its resilience—is

relatively well-developed. But the strategies we currently deploy for assuring safety (e.g. checking a quality management system, which in turn checks whether individual components or processes or items meet prespecified requirements) occupy only a slice of the knowledge base for generating safety in complex, risky operations. This knowledge base is inherently and permanently imperfect (Rochlin, 1999), and no contemporary logics of rulemaking and inspection can arbitrate in any sustained way between what is safe or unsafe. The criteria used, after all, represent only a particular portion of the knowledge base, a particular model of risk, of what makes operations brittle or resilient. In a world of incomplete knowledge, of resource limitations and changing hazards, we have to assume that this representation, as any other, is a coarse approximation that covers the target world only partially, and may likely be obsolete.

As Helios 522 could end up testifying, the quality of individual components or sub-systems (even if these are higher-order sub-systems, such as an airline's recruitement practices or maintenance arm or manual tree or event reporting system) may say little about how those sub-systems and components could stochastically and non-linearly recombine to outwit the best efforts at anticipating pathways to failure.

Complexity theory and system safety

For the past few centuries, our central analogy for understanding how systems work has been the machine, and our central strategy reductionism. To understand how something works, we dismantle it and look at the parts that make up the whole. This implies that we can derive the macro properties of the system (e.g. safety) as a straightforward function of, or aggregation from, the lower-order components or subsystems that constitute it. Helios 522 could begin to question whether this is enough, or applicable at all. By dissecting a system and inspecting its parts, we "kill" it and cannot know what gives it its life.

Shifting from a machinistic interpretation of complex systems to a systemic one implies giving up the reflex to look mainly at parts. 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, according to the systemic understanding of life, can only be disturbed (see Capra, 2002), which is much less binary, and potentially much more resilient. Failure is not necessarily the result of individual or compound component breakage, but is more 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 over 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.

The principles and patterns of organization of a living system are unlike those of machines, and we need a different mathematics, for example that of complexity theory (nonlinear dynamics) to begin to model its intricacies. Complexity theory tries to understand how simple things can generate very complex outcomes that could not be anticipated by just looking at the parts themselves. It has found that 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 an interaction between 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 *et al.*, 1996). For us to begin to understand how systems

(e.g. the European-wide system of proficiency-checking and safety regulation) dynamically create safety, we should first acknowledge that:

- Practitioners and organizations 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 inspectorates) 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. Effective 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, & Scardigli, 1994). This, after all, can avoid narrow interpretations of risk and stale strategies (e.g. checking quality of components).

One concern driving the development of non-linear dynamics and resilience engineering is the search for the edge of chaos, a point of emergence beyond which new system behaviors can emerge that could not have been predicted using decompositional logic. Escalating circumstances onboard Helios 522, of which language as a disabling device was not only a victim but also constitutive, can be said to have pushed crew coordination capabilities past such a "tipping point", the point in complexity theory where stability is overtaken by instability; order supplanted by chaos. A tipping point in Helios 522, where confusion started accelerating, could be the triggering of additional alarm and system responses when passing 14,000 feet.

Fixing on higher-order properties

To keep a machine working, we want to check on the servicability of its parts and their interactions. Keep out the harmful forces, throw out the bad parts, build barriers around sensitive sub-systems to shield them from danger. To keep a living system working, that is not enough, if applicable at all. Instead, we must adopt a functional, rather than structural point of view. Resilience is the system's ability to effectively adjust to hazardous influences, rather than resist or deflect them (Hollnagel *et al.*, 1996). 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 recent record highs. But effective adjustment to these potentially hazardous influences did not occur at any level in the system in this case. In fact, the language-as-disabling-device issue appears to be rather underplayed in the European regulatory arena. Perhaps out of political imperative, it sits low on a variety of priority lists, except perhaps those of professional labor organizations (e.g. pilot associations).

As long as we see an organization as a componential structure, whose aggregate is a straightforward mapping of parts onto the whole, then we—as an entire industry—may not be well-equipped for a sudden stochastic outburst of complexity as the one in Helios 522. If our Quality Assurance logic, entry qualifications, data monitoring, and safety inspection regimes keep considering mainly parts and whether they meet their applicable criteria, then nonlinear concurrences (as in Helios 522) of events and functions within the system will keep outwitting us. If system oversight is to really work, and the second-order inspection role to become really meaningful, then looking for the quality of individual components or subsystems may no longer be a sufficient activity.

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 *et al.*, 1996). Failures represent breakdowns in adaptations directed at coping with complexity (Woods, 2003). Resilience, then, represents the system's ability to recognize, adapt to, and absorb a disruption that falls outside the disturbances the system was designed to handle. Making judgments of resilience thus means fixing on higher-order system properties, to leave it "alive" and not just pick it apart to examine component parts. Insight from past failures (e.g. Columbia Accident Investigation Board, 2003) informs us about where we could look to gain confidence in the resilience of a system (see also Woods, 2003):

- **Monitoring of safety monitoring** (or meta-monitoring). Does the system invest in an awareness of the models of risk it embodies in its safety strategies and risk countermeasures? This is important if the system wants to avoid stale coping mechanisms, misplaced confidence in how it regulates or checks safety, and does not want to miss new possible pathways to failure.
- **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 this case, its ability to deal with events at the edge of chaos may be hampered, as the system may be unprepared for the concurrences that push developments past the tipping point.
- **Distancing through differencing.** In this process, system members look at other failures and other organizations as not relevant to them and their situation. They discard other events because they appear to be dissimilar or distant. But just because the organization or section has different technical problems, 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 towards hazard.
- **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 (Vaughan, 1999). 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 that move a system closer to the edge of chaos.
- **Knowing the gap between work-as-imagined and work-as-done**. 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 ill-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 experiences from it.
- **Keeping the 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. This typically involves stakeholders discussing risk even when everything looks safe. Indeed, if discussions about risk are going on even in the absence of obvious threats to safety, we could get some confidence that an organization is investing in an analysis, and possibly in a critique and subsequent update, of its models of risk.
- **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. 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. Resilient systems build in this function at meaningful organizational levels, which relates to the next point.

- **The ability and extent of bringing 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. With a neutral observer or commentator thus "institutionalized", one can be slightly more confident that self-regulation or system oversight may work.

The "system" in the points above is not just an inspection object (airline, maintenance organization) or any of its sub-units, but could be a system at a higher level, e.g. European-wide safety regulation. The questions to get confidence about the resilience of the system apply at that level 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. Helios 522 may suggest that we, in Europe, may still be applying models that no longer are.

References

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

Capra, F. (2002). *The hidden connections*. New York: Doubleday.

Columbia Accident Investigation Board (2003). *Report Volume 1, August 2003*. Washington, D.C.: Government Printing Office.

Dekker, S. W. A. (2004). Why we need new accident models. *Journal of Human Factors and Aerospace Safety*, *4*(1), 1-18.

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

Hollnagel, E., Woods, D. D., & Leveson, N. G. (1996). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate Publishing Co.

Leveson, N. (2002). *A new approach to system safety engineering*. Cambridge, MA: Aeronautics and Astronautics, Massachusetts Institute of Technology.

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

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, NY: 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.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25*, 271-305.

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, D.C., 29 October 2003.