Why we need new accident models

Sidney Dekker

Center for Human Factors in Aviation, IKP

Linköping Institute of Technology, SE-581 83 Linköping, Sweden

sidde@ikp.liu.se

The models we currently use to understand aerospace safety and accidents are based on a structuralist vocabulary, with mechanistic metaphors that describe the internal workings or failings of operators and their surrounding organizations. Such a view may be increasingly at odds with interpretative demands posed by recent accidents in otherwise very safe systems. Particularly the drift into failure, which represents a large category of residual risk in aerospace, is hard to model (and thereby understand and predict) with structuralist approaches. Drifting into failure is not so much about breakdowns or malfunctioning of components, but about an organization not adapting effectively to the complexity of its structure and environment. This requires aerospace to adopt a true systems approach, which sees sociotechnical complexity not as constituted of parts and their interactions, but as a web of dynamic, evolving relationships and transactions. This can lead to models that can make processes of drift come alive, and help point to more productive countermeasures.

Introduction

The greatest residual risk in today's safe aerospace systems is drift into failure. Drift into failure is a slow, incremental movement of systems operations towards the edge of their safety envelope. This movement is driven by pressures of scarcity and competition that subtly influence the many decisions and trade-offs made daily by operators and management hierarchies. The intransparency of complex sociotechnical systems that surround the operation of uncertain technology makes that people do not stop the drift (e.g. Perrow, 1984; Vaughan, 1996). Often they do not even see it. Accidents that lie at the end of drift are "the effect of a systematic migration of organizational behavior toward accidents under the influence of pressure towards cost-effectiveness in an aggressive, competitive environment." (Rasmussen & Svedung, 2000, p. 14). Drift into failure is hard to recognize because it is about normal people doing normal work in (seemingly) normal organizations, not about obvious breakdowns or failures or errors. Drift into failure is scary for all kinds of stakeholders because it reveals how harm can occur in organizations designed to prevent it. Drift into failure is also difficult to model and predict using current approaches in aerospace human factors. These are largely limited to a structuralist vocabulary. Our language of failures is a language of mechanics. We describe accident "trajectories", we seek causes and effects, interactions. We look for "initiating failures", or triggering events, and trace the successive domino-like collapse of the system that follows it. This worldview sees sociotechnical systems as machines with parts in a particular arrangement (blunt versus sharp ends, defenses layered throughout), with particular interactions (trajectories, domino effects, triggers, initiators), and a mix of independent or intervening variables (blame culture versus

safety culture). This is the worldview inherited from Descartes and Newton, the worldview that has successfully driven technological development since the scientific revolution half a millennium ago. The worldview, and the language that accompanies it, is based on particular notions of natural science, and exercises a subtle but very powerful influence on our understanding of sociotechnical success and failure today. Yet this worldview may be lagging behind the sociotechnical developments that have taken place in aerospace, leaving us less than well equipped to understand failure, let alone anticipate or prevent it. This paper looks at a case of drift into failure, and proposes how we may need new kinds of models to capture the workings and predict

Drifting into failure

The 2000 Alaska Airlines 261 accident is an example of drift. The MD-80 crashed into the Ocean off California after the trim system in its tail snapped. *Prima facie*, the accident seems to fit a simple category that has come to dominate recent accident statistics: mechanical failures as a result of poor maintenance. A single component failed because people did not maintain it well. Indeed, there was a catastrophic failure of a single component (a jackscrew-nut assembly). A mechanical failure, in other words. The break instantly rendered the aircraft uncontrollable and sent it plummeting into the Pacific. But such accidents do not happen just because somebody suddenly errs or something suddenly breaks: there is supposed to be too much built-in protection against the effects of single failures. Consistent with the patterns of drift into failure, it were the protective structures, the surrounding organizations (including the regulator) that themselves contributed, in ways inadvertent, unforeseen and hard

to detect. The organized social complexity surrounding the technological operation, the maintenance committees, working groups, regulatory interventions and approvals, manufacturer inputs, all intended to protect the system from breakdown, actually helped set its course to the edge of the envelope and across.

In Alaska 261, the drift towards the accident that happened in 2000 had begun decades before, during the first flights of the 1965 Douglas DC-9 that preceded the MD-80 type. In the MD-80 trim system, the front part of the horizontal stabilizer is connected to a nut which drives up and down a vertical jackscrew. An electrical trim motor rotates the jackscrew, which in turn drives the nut up or down. The nut then pushes the whole horizontal tail up or down. Adequate lubrication is critical for the functioning of a jackscrew and nut assembly. Without enough grease, the constant grinding will wear out the thread on either the nut or the screw (in this case the screw is deliberately made of harder material, wearing the nut out first). The thread actually carries the entire load that is imposed on the vertical tail during flight. This is a load of around 5000 pounds, similar to the weight of a whole family sedan hanging by the thread of a jackscrew and nut assembly. Were the thread to wear out on an MD-80, the nut would fail to catch the threads of the jackscrew. Aerodynamic forces then push the horizontal tailplane (and the nut) to its stop way out of the normal range, rendering the aircraft uncontrollable in the pitch axis. Which is essentially what happened to Alaska 261. Even the stop failed because of the pressure. A so-called torque tube runs through the jackscrew in order to provide redundancy (instead of having two jackscrews, like in the preceding DC-8 model). But even the torque tube failed in Alaska 261.

None of this is supposed to happen of course. When it first launched the aircraft in the mid 1960's, Douglas recommended that operators lubricate the trim jackscrew

assembly every 300 to 350 flight hours. For typical commercial usage that could mean grounding the airplane for such maintenance every few weeks. Immediately, the socio-technical, organizational systems surrounding the operation of the technology began to adapt. And set the system on its course to drift. Through a variety of changes and developments in maintenance guidance for the DC-9/MD-80 series aircraft, the lubrication interval was extended. A complex and constantly evolving web of committees with representatives from regulators, manufacturers, subcontractors and operators was at the heart of a development of maintenance standards, documents and specifications. Rationality for maintenance interval decisions was produced relatively locally, relying on incomplete, emerging information about what was, for all its deceiving basicness, still uncertain technology. While each decision was locally rational, making sense for decision makers in their time and place, the global picture became one of drift towards disaster.

Significant drift, in fact. Starting from a lubrication interval of 300 hours, the interval at the time of the Alaska 261 accident had moved up to 2,550 hours, almost an order of magnitude more. As is typical in the drift towards failure, this distance was not bridged in one leap. The slide was incremental: step by step; decision by decision. In 1985, jackscrew lubrication was to be accomplished every 700 hours, at every other so-called maintenance “B check” (which occurs every 350 flight hours). In 1987, the B-check interval itself was increased to 500 flight hours, pushing lubrication intervals to 1000 hours. In 1988, B checks were eliminated altogether, and tasks to be accomplished were redistributed over A and C checks. The jackscrew assembly lubrication was to be done each eighth 125-hour A check: still every 1000 flight hours. But in 1991, A check intervals were extended to 150 flight hours, leaving a lubrication every 1200 hours. Three years later the A check interval was extended

again, this time to 200 hours. Lubrication would now happen every 1600 flight hours. In 1996, the jackscrew assembly lubrication task was removed from the A check and moved instead to a so-called task card that specified lubrication every 8 months. There was no longer an accompanying flight hour limit. For Alaska Airlines 8 months translated to about 2550 flight hours. The jackscrew recovered from the ocean floor, however, revealed no evidence that there had been adequate lubrication at the previous interval at all. It might have been more than 5000 hours since it last received a coat of fresh grease.

---

insert picture 1 about here

After only a year of DC-9 flying, Douglas received reports of thread wear significantly in excess of what had been predicted. In response, the manufacturer recommended that operators perform a so-called end play check on the jackscrew assembly at every maintenance C-check, or every 3,600 flight hours. The end play check uses a restraining fixture that puts pressure on the jackscrew assembly, simulating the aerodynamic load during normal flight. The amount of play between nut and screw, gauged in thousandths of an inch, can then be read off an instrument. The play is a direct measure of the amount of thread wear.

From 1985 onwards, end play checks at Alaska became subject to the same kind of drift as the lubrication intervals. In 1985, end play checks were scheduled every other C check, since the required C checks consistently came in at 2,500 hours. 2,500 hours was rather ahead of the recommended 3,600 flight hours, unnecessarily grounding

aircraft. By scheduling an end play test every other C check, though, the interval was extended to 5000 hours. By 1988, C check intervals themselves were extended to 13 months, with no accompanying flight-hour limit. End play checks were now performed every 26 months, or about every 6,400 flight hours. In 1996, C check intervals were extended once again, this time to 15 months. This stretched the flight hours between end play tests to about 9,550. The last end play check of the accident airplane was conducted at the airline maintenance facility in Oakland, California in 1997. At that time, play between nut and screw was found to be exactly at the allowable limit of .040 inch. This introduced considerable uncertainty. With play at the allowable limit, what to do? Release the airplane and replace parts the next time, or replace the parts now? The rules were not clear. The so-called AOL 9-48A said "that jackscrew assemblies could remain in service as long as the end play measurement remained within the tolerances (between 0.003 and 0.040 inch)" (NTSB, 2002; p. 29). It was still 0.040 inch, so the aircraft could technically remain in service. Or? How quickly would the thread wear from there on? Six days, several shift changes and another, more favorable end play check later, the airplane was released. No parts were replaced: they were not even in stock in Oakland. The airplane "departed 0300 local time. So far so good", the graveyard shift turnover plan noted (ibid., p. 53). Three years later the trim system snapped and the aircraft disappeared into the ocean not far away. Between 2,500 hours to 9,550 hours there is more drift toward failure. Again, each extension made local sense, and was only an increment away from the previously established norm. No rules were violated, no laws broken. Even the regulator concurred with the changes in end play check intervals. Normal people doing normal work around seemingly normal, stable technology.

---

insert picture 2 about here

MD-80 maintenance technicians were never required to record or keep track of the endplay on the trim systems they measured. Even the manufacturer had expressed no interest in seeing these numbers or the slow, steady degeneration they may have revealed. If there was drift, in other words, no institutional or organizational memory would know it. The decisions, trade-offs, preferences and priorities which seem so out of the ordinary and immoral after an accident, were once normal and common sensical to those who contributed to its incubation.

Banality, conflict and incrementalism

Sociological research (e.g. Perrow, 1984; Weick, 1995; Vaughan, 1996; Snook, 2000) as well as prescient human factors work (Rasmussen & Svedung, 2000) and research on system safety (Leveson, 2002) has begun to sketch some of the internal workings of drift. They converge on some important commonalities. First, accidents, and the drift that precedes them, are associated with normal people doing normal work in normal organizations—not with miscreants engaging in immoral deviance. We can call this the "banality of accidents" thesis. Second, at the heart of trouble lies a conflictual model: organizations that involve safety-critical work are essentially trying to reconcile irreconcilable goals (staying safe *and* staying in business). Third, drifting

into failure is incremental. Accidents do not happen suddenly, nor are they preceded by monumentally bad decisions or bizarrely huge steps away from the ruling norm. The banality of accidents thesis says that the potential for having an accident grows as a normal by-product of doing normal business under normal pressures of resource scarcity and competition. No system is immune to the pressures of scarcity and competition (not even (or certainly not) regulators). The chief engine of drift hides somewhere in this conflict, in this tension between operating safely and operating at all.

In trade-offs between safety and efficiency there is a feedback imbalance. Information on whether a decision is cost-effective or efficient can be relatively easy to get. An early arrival time is measurable and has immediate, tangible benefits. How much is or was borrowed from safety in order to achieve that goal, however, is much more difficult to quantify and compare. If it was followed by a safe landing, apparently it must have been a safe decision. Extending a lubrication interval similarly saves immediately measurable time and money, while borrowing from the future of an apparently problem-free jackscrew assembly. Each consecutive empirical success (the early arrival time is still a "safe" landing; the jackscrew assembly is still operational) seems to confirm that fine-tuning (Starbuck & Milliken, 1988) is working well: the system can operate equally safely, yet more efficiently. As Weick (1993) points out, however, safety in those cases may not at all be the result of the decisions that were or were not made, but rather an underlying stochastic variation that hinges on a host of other factors, many not easily within the control of those who engage in the fine-tuning process. Empirical success, in other words, is not proof of safety. Past success does not guarantee future safety. Borrowing more and more from safety may go well for a while, but you never know when you are going to hit. This moves Langewiesche

(1998) to say that Murphy's law is wrong: everything that can go wrong usually goes right. And then we draw the wrong conclusion.

The nature of this dynamic, this fine-tuning, this adaptation, is incremental (Vaughan, 1996). The organizational decisions that are seen as "bad decisions" after the accident (even though they seemed like perfectly acceptable ideas at the time) are seldom big, risky steps. Rather, there is a long and steady progression of small, incremental steps that unwittingly take an operation toward its boundaries. Each step away from the original norm that meets with empirical success (and no obvious sacrifice of safety) is used as the next basis from which to depart just that little bit more. It is this incrementalism that makes distinguishing the abnormal from the normal so difficult. If the difference between what "should be done" (or what was done successfully yesterday) and what is done successfully today is minute, then this slight departure from an earlier established norm is not worth remarking or reporting on.

Drift into failure and incident reporting

This makes the definition of an incident deeply problematic. Before 1985, failing to perform an end play check every 2,500 hours could be considered an "incident", and given that the organization had a means for reporting it, it may even have been considered as such. But by 1996, the same deviance was normal. Regulated even. By 1996, the same failure was no longer an incident. And there was more. Why report that lubricating the jackscrew assembly often had to be done at night, in the dark, outside the hanger, standing in the little basket of a lift truck at a soaring height above the ground? Even when it was raining (which it does do in San Francisco)? Why

report that you, as a mechanic have to fumble your way through two small access panels that hardly allow room for one human hand—let alone space for eyes to see what is going on inside and what needs to be lubricated—if that is what you have to do all the time? It was normal work; it was required to get the job done. The mechanic responsible for the last lubrication of the accident airplane told investigators that he had taken to wearing a battery-operated head lamp during night lubrication tasks, so that he had his hands free and could see at least something (NTSB, 2002). Though perhaps remarkable after the fact, these things were "normal" then, they were not reportworthy. They were not "incidents". Why report that the end play checks were performed with one restraining fixture (the only one in the entire airline, fabricated in-house, nowhere near the manufacturer's specifications), if that is what you used every time you did an end play check? Why report that end play checks, either on the airplane or on the bench, generated widely varying measures, if that is what they did all the time, and if that is what maintenance work is often about? It is normal, it is not an incident. Even if the airline had a reporting culture, even if it had a "learning culture", even if it had a "just" culture so that people would feel secure in sending in their reports without fear of retribution, these would not be "incidents" that would turn up in the system. The failure to adequately see the part to be lubricated (that non-redundant, single-point, ultra safety-critical part), the failure to adequately and reliably perform an end play check—none of this appears in incident reports. But it is deemed "causal" or "contributory" in the accident report. These were not incidents. In very safe systems, such as commercial aviation in the Western world, incidents do not precede accidents. Normal work does. In these systems, the common cause hypothesis (that incidents and accidents stem from the same root) is false, and the value of incident reporting for making even greater progress on safety is dubious:

> "accidents are different in nature from those occurring in safe systems: in this case accidents usually occur in the absence of any serious breakdown or even of any serious error. They result from a combination of factors, none of which can alone cause an accident, or even a serious incident; therefore these combinations remain difficult to detect and to recover using traditional safety analysis logic. For the same reason, reporting becomes less relevant in predicting major disasters." (Amalberti, 2001, p. 112)

Despite this insight, independent errors and failures are still the major return of any accident investigation today. The 2002 NTSB report on flight 261, following Newtonian-Cartesian logic, speaks of deficiencies in Alaska Airlines' maintenance program, of shortcomings in regulatory oversight, of responsibilities not fulfilled, of flaws and failures and breakdowns. Of course, in hindsight they may well be just that. And finding faults and failures is fine because it gives the system something to fix. But why did nobody at the time see these so very apparent faults and failures for what they (in hindsight) were? This is where the structuralist vocabulary of traditional human factors and systems safety is most limited, and limiting. The "holes" found in the "layers of defense" (respectively the regulator, the manufacturer, the operator, the maintenance facility and lastly the technician) are easy to discover once the rubble is strewn before one's feet. But these deficiencies and failures are not seen as such, nor easy to see as such, by those on the inside (or even those relatively on the outside, like the regulator!) before the accident happens. Indeed, structuralist models can capture the "deficiencies" that result from drift very well: it accurately identifies latent

failures, resident pathogens in organizations and locates the holes in the layers of defense. But the build-up of "latent failures", if that is what you want to call them, is not modeled. The *process* of erosion, of attrition of safety norms, of drift towards margins, cannot be captured well by structuralist approaches, for those are inherently metaphors for resulting *forms*, not models oriented at processes of *formation*. Structuralist models are static.

Although the structuralist models of the 1990's are often called system models or systemic models, they are a far cry from what actually is considered systems thinking (e.g. Capra, 1982). The systems part of structuralist models has so far been limited to identifying, and providing a vocabulary for the upstream structures (blunt ends) behind the production of "errors" at the sharp end. The systems part of these models is a reminder that there is context; that we cannot understand errors without going into the organizational background from which they hail. All of this is necessary, of course, as "errors" are still all to often seen as the legitimate conclusion of an investigation (although under more fashionable labels such as "breakdown in CRM"). But reminding people of context is no substitute for beginning to explain the dynamics; the subtle, incremental processes that lead to, and normalize, the behavior eventually observed. This requires us to take a different perspective on the messy interior of organizations, and a different language to cast the observations in.

Systems as dynamic relationships

Capturing and describing the processes by which organizations drift into failure requires systems thinking. Systems thinking is about relationships and integration. It

sees a sociotechnical system not as a structure consisting of constituent departments, blunt ends and sharp ends, deficiencies and flaws, but as a complex web of dynamic, evolving relationships and transactions. Instead of building blocks, the systems approach emphasizes principles of organization. Understanding the whole is quite different from understanding an assembly of separate components. Instead of mechanical linkages between components (with a cause and an effect), it sees transactions—simultaneous and mutually interdependent interactions. Such emergent properties are destroyed when the system is dissected and studied as a bunch of isolated components (a manager, department, regulator, manufacturer, operator). Emergent properties do not exist at lower levels; they cannot even be described meaningfully with languages appropriate for those lower levels.

Take the lengthy, multiple processes by which maintenance guidance was produced for the DC-9 and later the MD-80 series aircraft. Separate components (such as regulator, manufacturer, operator) are difficult to distinguish, and the interesting behavior, the kind of behavior that helps drive drift into failure, emerges only as a result of complex relationships and transactions. At first thought the creation of maintenance guidance would seem a solved problem. You build a product, you get the regulator to certify it as safe to use, and then you tell the user how to maintain it in order to keep it safe. Even the second step (getting it certified as safe) is nowhere near a solved problem, and deeply intertwined with the third. But more about that later.

First the maintenance guidance. Alaska 261 reveals a large gap between the production of a system and its operation. Inklings of the gap appeared in observations of jackscrew wear that was higher than what the manufacturer expected. Not long after the certification of the DC-9, people began work to try to bridge the gap. An aviation industry team Maintenance Guidance Steering Group (MSG) was set up to

develop guidance documentation for maintaining large transport aircraft (particularly the Boeing 747) (see NTSB, 2002). Using this experience, another MSG developed a new guidance document in 1970, called MSG-2, which was intended to present a means for developing a maintenance program acceptable to the regulator, the operator and the manufacturer. The many discussions, negotiations and inter-organizational collaborations underlying the development of an "acceptable maintenance program" showed that how to maintain a once certified piece of complex technology was not at all a solved problem. In fact, it was very much an emergent thing: technology proved less certain than it had seemed on the drawing board (e.g. the DC-9 jackscrew wear rates were higher than predicted), and it was not before it hit the field of practice that "deficiencies" became apparent. If you knew where to look, that is.

In 1980, through combined efforts of the regulator, trade and industry groups and manufacturers of both aircraft and engines in the US as well as Europe, a third guidance document was produced, called MSG-3. This document had to deconfound earlier confusions, for example between "hard-time" maintenance, "on-condition" maintenance, "condition-monitoring" maintenance, and "overhaul" maintenance. Revisions to MSG-3 were issued in 1988 and 1993. The MSG guidance documents and their revisions were accepted by the regulators, and used by so-called Maintenance Review Boards (MRB) that convene to develop guidance for specific aircraft models. The MRB does not write guidance itself, however, this is done by industry steering committees, often headed by a regulator. These committees in turn direct various working groups. Through all of this, so-called on-aircraft maintenance planning (OAMP) documents get produced, as well as generic task cards that outline specific maintenance jobs. Both the lubrication interval and the end play check for MD-80 trim jackscrews were the constantly changing products of these evolving webs

of relationships between manufacturers, regulators, trade groups, and operators, who were operating off of continuously renewed operational experience, and a perpetually incomplete knowledge base about the still uncertain technology (remember, end play check results, for example, were not recorded or tracked). What are the rules? What should the standards be? The introduction of a new piece of technology is followed by negotiation, by discovery, by the creation of new relationships and rationalities. "Technical systems turn into models for themselves", says Weingart (1991, p. 8): "the observation of their functioning, and especially their malfunctioning, on a real scale is required as a basis for further technical development." Rules and standards do not exist as unequivocal, aboriginal markers against a tide of incoming operational data (and if they do, they are quickly proven useless or out of date). Rather, rules and standards are the constantly updated products of the processes of conciliation, of give and take, of the detection and rationalization of new data. Setting up the various teams, working groups and committees was a way of bridging the gap between building and maintaining a system, between producing it and operating it. Bridging the gap is about adaptation—adaptation to newly emerging data (e.g. surprising wear rates) about an uncertain technology. But adaptation can mean drift. And drift can mean breakdown.

Modeling live sociotechnical systems

What kind of safety model could capture such adaptation, and predict its eventual collapse? Structuralist models are limited. Of course, we could claim that the lengthy lubrication interval and the unreliable end play check were structural deficiencies.

That they were holes in layers of defense? Absolutely. But such metaphors do not help us look for where the hole occurred, or why. There is something complexly organic about MSG's, something ecological, that is lost when we model them as a layer of defense with a hole in it; when we see them as a mere "deficiency" or a latent failure. When we see systems instead as internally plastic, as flexible, we can begin to see them as organic. Their functioning is controlled by dynamic relations and ecological adaptation, rather than by rigid mechanical structures. They also exhibit self-organization (from year to year, the make-up of MSG's was different) in response to environmental changes, and self-transcendence: the ability to reach out beyond currently known boundaries and learn, develop and perhaps improve. What is needed is not yet another structural account of the end result of organizational deficiency. What is needed instead is a more functional account of living processes that co-evolve with respect to a set of environmental conditions, and that maintain a dynamic and reciprocal relation with those conditions (see Heft, 2001). Such accounts need to capture what happens within an organization, with the gathering of knowledge and creation of rationality within workgroups, once a technology gets fielded. A functional account could cover the organic organization of maintenance steering groups and committees, whose make-up, focus, problem definition and understanding co-evolved with emerging anomalies and growing knowledge about an uncertain technology.

A model that is sensitive to the *creation* of deficiencies, not just to their eventual presence, makes a sociotechnical system come alive, rather than the static simile of a structuralist metaphor. It must be a model of processes, not just a model of structure. Extending a lineage of cybernetic and systems engineering research, Nancy Leveson (2002) proposes that control models can fulfill part of this task. Control models use

the ideas of hierarchies and constraints to represent the emergent interactions of a complex system. In their conceptualization, a sociotechnical system consists of different levels, where each superordinate level imposes constraints on (or controls what is going on in) subordinate levels. Control models are one way to begin to map the dynamic relationships between different levels within a system—a critical ingredient of moving toward true systems thinking (where dynamic relationships and transactions are dominant, not structure and components). Emergent behavior is associated with the limits or constraints on the degrees of freedom of a particular level.

The division into hierarchical levels is an analytic artifact necessary to see how system behavior can emerge from those interactions and relationships. The resulting levels in a control model are of course a product of the analyst who maps the model onto the sociotechnical system. Rather than reflections of some reality out there, the patterns are constructions of a human mind looking for answers to particular questions. For example, a particular MSG would probably not see how it is superordinate to some level and imposing constraints on it, or subordinate to some other and thus subject to its constraints. In fact, a one-dimensional hierarchical representation (with only up and down along one direction) probably oversimplifies the dynamic web of relationships surrounding (and determining the functioning of) any such multi-party, evolving group as an MSG. But all models are simplifications, and the levels analogy can be helpful for an analyst who has particular questions in mind (Why did these people at this level or in this group make the decisions they did, and why did they see that as the only rational way to go?).

Control among levels in a sociotechnical system is hardly ever perfect. In order to control effectively, any controller needs a good model of what it is supposed to

control, and it requires feedback about the effectiveness of its control. But such internal models of the controllers easily become inconsistent with, and do not match the system to be controlled (Leveson, 2002). Buggy control models are true especially with uncertain, emerging technology (including trim jackscrews) and the maintenance requirements surrounding them. Feedback about the effectiveness of control is incomplete and can be unreliable too. A lack of jackscrew-related incidents may provide the illusion that maintenance control is effective and that intervals can be extended, while the paucity of risk actually depends on factors quite outside the controller's scope. In this sense, the imposition of constraints on the degrees of freedom is mutual between levels and not just top-down: if subordinate levels generate imperfect feedback about their functioning, then higher-order levels do not have adequate resources (degrees of freedom) to act as would be necessary. Thus the subordinate level imposes constraints on the superordinate level by not telling (or not being able to tell) what is really going on. Such a dynamic has been noted in various cases of drift into failure, including the Challenger Space Shuttle disaster (see Feynman, 1988).

Drift into failure as erosion of constraints and eventual loss of control

Nested control loops can make a model of a sociotechnical system come alive more easily than a line of layers of defense. And in order to model drift, it *has* to come alive. Control theory sees drift into failure as a gradual erosion of the quality or the enforcement of safety constraints on the behavior of subordinate levels. Drift results from either missing or inadequate constraints on what goes on at other levels.

Modeling an accident as a sequence of events, in contrast, is really only modeling the end-product of such erosion and loss of control. If safety is seen as a control problem, then events (just like the "holes" in layers of defense) are the *results* of control problems, not the causes that drive a system into disaster. A sequence of events, in other words, is at best the starting point of modeling an accident, not the analytic conclusion. The processes that generate these weaknesses are in need of a model.

One type of erosion of control occurs because original engineering constraints (e.g. 300-hour intervals) are loosened in response to the accumulation of operational experience. Such loosening occurs in response to local concerns with limited time-horizons and based on uncertain, incomplete knowledge. Often it is not even clear to insiders that constraints have become less tight as a result of their decisions in the first place, or that it at all matters if they have. And even when it is clear, the consequences may be hard to foresee, and judged to be a small potential loss in relation to the immediate gains. As Leveson (2002) puts it, experts do their best to meet local conditions, and in the busy daily flow and complexity of activities they may be unaware of any potentially dangerous side effects of those decisions. It is only with the benefit of hindsight or omniscient oversight (which is utopian) that these side-effects can be linked to actual risk.

Being a member of a system, then, can make systems thinking all but impossible. Perrow (1984) makes this argument very persuasively, and not just for the system's insiders. An increase in system complexity diminishes the system's transparency: diverse elements interact in a greater variety of ways that are difficult to foresee, detect, or even comprehend. Influences from outside the technical knowledge base exert a subtle but powerful pressure on the kinds of decisions and trade-offs that people will make, and constrain what will be seen as a rational decision or course of

action at the time (Vaughan, 1996). It is in these normal, day-to-day processes that we can find the seeds of organizational failure and success. And it is these processes we must turn to in order to find leverage for making further progress on safety. As Rasmussen and Svedung (2000, p. 14) put it:

> "To plan for a proactive risk management strategy, we have to understand the mechanisms generating the actual behavior of decision-makers at all levels… an approach to proactive risk management involves the following analyses:
> - a study of normal activities of the actors who are preparing the landscape of accidents during their normal work, together with an analysis of the work features that shape their decision making behavior
> - A study of the present information environment of these actors and the information flow structure, analyzed from a control theoretic point of view."

Reconstructing or studying the "information environment" in which actual decisions are shaped; in which local rationality is constructed, can help us penetrate processes of organizational sensemaking. These processes lie at the root of organizational learning and adaptation, and thereby at the source of drift into failure. The narrowness and incompleteness of the niche in which decision makers find themselves can come across as disquieting to retrospective observers, including people inside and outside the organization. It was after the Space Shuttle Columbia accident that the Mission Management Team

> "admitted that the analysis used to continue flying was, in a word, 'lousy'. This admission—that the rationale to fly was rubber-stamped—is, to say the least, unsettling." (CAIB, 2003; p. 190)

"Unsettling" it may be, and probably is—in hindsight. But from the inside, people in organizations do not spend a professional life making "unsettling" decisions. Rather, they do mostly normal work. Again, how can a manager see a "lousy" process to evaluate flight safety as normal, as not something that is worthy reporting or repairing? How could this process be normal? The CAIB itself provides clues to answers in their allusion to pressures of scarcity and competition:

> "The Flight Readiness process is supposed to be shielded from outside influence, and is viewed as both rigorous and systematic. Yet the Shuttle Program is inevitably influenced by external factors, including, in the case of STS-107, schedule demands. Collectively, such factors shape how the Program establishes mission schedules and sets budget priorities, which affects safety oversight, workforce levels, facility maintenance, and contractor workloads. Ultimately, external expectations and pressures impact even data collection, trend analysis, information development, and the reporting and disposition of anomalies. These realities contradict NASA's optimistic belief that pre-flight reviews provide true safeguards against unacceptable hazards." (2003, p. 191).

Perhaps there is no such thing as "rigorous and systematic" decision making based on technical expertise alone. This is probably an illusion. Expectations and pressures, budget priorities and mission schedules, contractor workloads and workforce levels

all impact technical decision making. All these factors determine and constrain what people there and then see as rational or unremarkable. While the intention was that NASA's flight safety evaluations were "shielded" from those external pressures, these pressures nonetheless seeped into even the collection of data, analysis of trends and reporting of anomalies. The information environments thus created for decision makers were continuously and insidiously tainted by pressures of production and scarcity (and in which organization are they not?), prerationally influencing the way people saw the world. Yet even this "lousy" process was considered "normal"—normal or inevitable enough, in any case, to not warrant the expense of energy and political capital on trying to change it. Drift into failure can be the result.

Engineering resilience into organizations

All open systems are continually adrift inside their safety envelopes. Pressures of scarcity and competition, the intransparency and size of complex systems, the patterns of information that surround decision makers, and the incrementalist nature of their decisions over time, can make that systems drift into failure. Drift is generated by normal processes of reconciling differential pressures on an organization (efficiency, capacity utilization, safety) against a background of uncertain technology and imperfect knowledge. Drift is about incrementalism contributing to extraordinary events, about the transformation of pressures of scarcity and competition into organizational mandates, and about the normalization of signals of danger so that organizational goals and "normal" assessments and decisions become aligned. In safe systems, the very processes that normally guarantee safety and generate

organizational success, can also be responsible for organizational demise. The same complex, intertwined sociotechnical life that surrounds the operation of successful technology, is to a large extent responsible for its potential failure. Because these processes are normal, because they are part and parcel of normal, functional organizational life, they are difficult to identify and disentangle. The role of these invisible and unacknowledged forces can be frightening. Harmful consequences can occur in organizations constructed to prevent them. Harmful consequences can occur even when everybody follows the rules (Vaughan, 1996).

The direction in which drift takes pushes the operation of the technology can be hard to detect, also or perhaps especially for those on the inside. It can be even harder to stop. Given the diversity of forces (political, financial, and economic pressures, technical uncertainty, incomplete knowledge, fragmented problem solving processes) both on the inside and outside, the large, complex sociotechnical systems that operate some of our most hazardous technologies today seem capable of generating an obscure energy and drift of their own, relatively impervious to outside inspection or inside control.

Recall that in normal flight, the jackscrew assembly of an MD-80 is supposed to carry a load of about 5000 pounds. But in effect this load was borne by a leaky, porous, continuously changing system of ill-taught and impractical procedures delegated to operator level that anxiously, but always unsuccessfully, tried to close the gap between production and operation, between making and maintaining. 5000 pounds of load on a loose and varying collection of procedures and practices, were slowly, incrementally grinding their way through the jackscrew threads. It was the sociotechnical system designed to support and protect the uncertain technology, not the mechanical part, that had to carry the load. It gave. The accident report

acknowledged that eliminating the risk of single catastrophic failures may not always be possible through design (as design is a reconciliation between irreconcilable constraints). It concluded that "when practicable design alternatives do not exist, a comprehensive systemic maintenance and inspection process is necessary" (p. 180). The conclusion, in other words, became to have a non-redundant system (the single jackscrew and torque tube) be made redundant through an organizational system of maintenance and airworthiness checking. The report was forced to conclude that the last resort should be a countermeasure which it just spent 250 pages proving does not work.

Drifting into failure is not so much about breakdowns or malfunctioning of components, as it is about an organization not adapting effectively to cope with the complexity of its own structure and environment (see Woods, 2003). Organizational resilience is not a property, it is a capability. A capability to recognize the boundaries of safe operations, a capability to steer back from them in a controlled manner, a capability to recover from a loss of control if it does occur. This means that human factors and system safety must find new ways of engineering resilience into organizations, of equipping organizations with a capability to recognize, and recover from, a loss of control. How can an organization monitor its own adaptations (and how these bound the rationality of decision makers) to pressures of scarcity and competition, while dealing with imperfect knowledge and uncertain technology? How can an organization become aware, and remain aware of its models of risk and danger? Answers to these questions hinge on our ability to develop more organic, co-evolutionary accident models. Organizational resilience is about finding means to invest in safety even under pressures of scarcity and competition, since that may be when such investments are needed most. Preventing drift into failure requires a

different kind of organizational monitoring and learning. It means fixing on higher-order variables; adding a new level of intelligence and analysis to the incident reporting and error counting that is done today.

References

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

Capra, F. (1982). *The turning point*. New York: Simon & Schuster.

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

Feynman, R. P. (1988). *"What do* you *care what other people think?" Further adventures of a curious character*. New York: Norton

Heft, H. (2001). Ecological psychology in context: James Gibson, Roger Barker and the legacy of William James's radical empiricism. Mahwah, NJ: Lawrence Erlbaum Associates.

Langewiesche, W. (1998). *Inside the sky: A meditation on flight*. New York: Pantheon Books.

Leveson, N. (2002). *A new approach to system safety engineering*. Cambridge, MA:

National Transportation Safety Board (2002). *Loss of control and impact with Pacific Ocean, Alaska Airlines Flight 261 McDonnell Douglas MD-83, N963AS, about 2.7 miles north of Anacapa Island, California, January 31, 2000 (AAR-02/01)*. Washington, D.C.: NTSB.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York, NY: Basic books.

Rasmussen, J., & Svedung, I. (2000). *Proactive risk management in a dynamic society*. Karlstad, Sweden: Swedish Rescue Services Agency.

Snook, S. A. (2000). *Friendly fire: The accidental shootdown of US Black Hawks over Northern Iraq*. Princeton, NJ: Princeton University Press.

Starbuck, W. H., & Milliken, F. J. (1988). Challenger: Fine-tuning the odds until something breaks. *Journal of Management Studies, 25*(4), 319-340.

Vaughan, D. (1996). *The Challenger lauch decision: Risky technology, culture and deviance at NASA*. Chicago, IL: University of Chicago Press.

Weick, K. E. (1993). The collapse of sensemaking in organizations. *Administrative Science Quarterly, 38*, 628-652.

Weick, K. E. (1995). *Sensemaking in organizations*. London: Sage.

Weingart, P. (1991). Large technical systems, real life experiments, and the legitimation trap of technology assessment: The contribution of science and technology to constituting risk perception. In T. R. LaPorte (Ed.), *Social responses to large technial systems: Control or anticipation*, pp. 8-9. Amsterdam, NL: Kluwer.

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.