Resilience Engineering: New directions for measuring and maintaining safety in complex systems

Final Report, November 2008

Sidney Dekker, Erik Hollnagel, David Woods and Richard Cook

Lund University School of Aviation

Resilience Engineering: New directions for measuring and maintaining safety in complex systems

Final Report
December 2008

Sidney Dekker, Erik Hollnagel, David Woods and Richard Cook

Executive summary

Resilience Engineering represents a new way of thinking about safety. Whereas established risk management approaches are based on hindsight and emphasise error tabulation and calculation of failure probabilities, Resilience Engineering looks for ways to enhance the ability of organisations to create processes that are robust yet flexible, to monitor and revise risk models, and to use resources proactively in the face of disruptions or ongoing production and economic pressures. In Resilience Engineering failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent the converse of the adaptations necessary to cope with the real world complexity. Individuals and organisations must always adjust their performance to the current conditions; and because resources and time are finite it is inevitable that such adjustments are approximate. Success has been ascribed to the ability of groups, individuals, and organisations to anticipate the changing shape of risk before damage occurs; failure is simply the temporary or permanent absence of that.

In resilience engineering, assuring safety does not mean tighter monitoring of performance, more counting of errors, or reducing violations, since that may well be based on a faulty assumption: that safety should be defined as the *absence* of something because systems are already safe. The corrolary of this wrong assumption is that safety-critical systems need protection from unreliable humans—by more procedures, tighter monitoring, automation. We are not custodians of already safe systems. These systems always have to meet multiple opposing goals at the same time, and always with limited resources. It's only people who can reconcile these conflicting demands, who can hold together such inherently imperfect systems. People, at all levels of an organization, create safety through practice. So safety is not about the absence of something. It is about the presence of something.

But the presence of what? When we see things go right under difficult circumstances, we've found that it's mostly because of people's adaptive capacity—their ability to recognize, absorb, and adapt to changes and disruptions—some of which may even fall outside of what the system has been trained or designed to do. This is why we call it resilience—the ability to accommodate change, conflict, disturbance, without breaking down, without catastrophic failure. Resilience is not about reducing negatives (incidents, errors, violations). It's about identfying and then enhancing the positive capabilities of people and organizations that allow them to adapt effectively and safely under pressure.

Resilience Engineering wants to understand and enhance how people themselves build, or engineer, adaptive margin into their system, how they create safety — by developing capacities that help them anticipate and absorb pressures, variations and disruptions. Resilience is about a constant calibration of these differential sources of risk and resource usage — how do they weigh up against each other?

Resilience Engineering is getting inspiration from a wide range of fields, way beyond traditional safety disciplines, particularly biological sciences. Organic systems, like viruses, are great at adjusting when they recognize a shortfall in their adaptive capacity—which is key to the creation of resilience. Here's some of the things that we see teams and organizations do that are good at this:

- They don't take past success as guarantee of future safety. Past results are not enough for them to be confident that their adaptive strategies will keep working.
- They keep a discussion of risk alive even when everthing looks safe. That things look safe doesn't mean they are: the model of what is risky may have become old, wrong, so they keep updating it.
- They are able to bring in different and fresh perspectives on problems. They listen to minority viewpoints, invite doubt, stay curious and open-minded, complexly sensitized.
- And they inspire and reward in their people the courage to say "no" to trading chronic safety concerns for acute production pressures; the courage to put the foot down and invest in safety when everybody else says that they can't. Because that is exactly the time when such investments may be necessary.

We already know how to measure whether you have become faster, better or cheaper, but has the organization become less resilient as a result? Checking organizations on those four points above can turn resilience into a fourth management variable that may help sustain safety-critical businesses under uncertainty, constant production and resource pressures.

A short film on resilience, produced in part with support of this project, is available on www.youtube.com (type "Sidney Dekker" in the window). A longer lecture on resilience (as well as the link to the shorter film) is available on www.lusa.lu.se/research

Introduction: Resilience Engineering in a meta-theoretical perspective

A pivotal development in the structuring of knowledges since the 1960's, coming from opposite ends of the traditional academic division between "superdomains" (natural versus social sciences), has created the opening for a field like Resilience Engineering. Newtonian-Cartesian premises have enjoyed feudal tenure on the hard sciences for three and a half centuries, and have influenced social sciences from the moment of their academic institutionalization with ideas about what it takes to be "scientific." In this, fundamental assumptions were made about the existence of cause and effect and their relationship, about symmetry between past and future, and about time-reversibility, linearity, decomposability, and stability. Both the long-standing adherence to these assumptions, as well as their recent unraveling, has important consequences for safety research.

Most natural scientists today agree that the world should be viewed as a less stable, less predictable and more complex place. Rather than a Newtonian-Cartesian machine, nature is now increasingly seen as active, adaptive, self-organizing, resilient—creative even. Science, accordingly, has begun to adopt radically different perspectives that attempt to account better for instability, for complexity and non-linearity, for the role of perturbations, bifurcations and emergence. The language and analytics of systems thinking and complexity theory that have been emerging, direct inquiry and refract findings in entirely different ways. They are rapidly shrinking the divide between superdomains and offer new questions and leverage points for safety interventions in complex systems.

Newtonian-Cartesian precepts propose, for example, that we can derive the macro properties of a system (e.g. safety) as a straightforward function of, or aggregation from, the lower-order components or subsystems that constitute it. An assumption in many accident models and safety practices is that safety can be increased by guaranteeing the reliability of the individual system components (human as well as machine), and that if components (even layers of defense) do not fail, or if only a number in some linear order fail, then accidents will not occur (e.g. Reason, 1990). Accidents that did not involve broken parts, or where nobody did anything wrong relative to the industry's understanding of "normal" at the time (e.g. Vaughan, 1996; Snook, 2000; Dekker, 2006) are literally inexplicable on the basis of these assumptions.

The broken component assumption of accidents, however, has had a long and tenacious reign in safety work, even though it was not until the Twentieth centrury that human error became seen as a managerial problem. This put it within the ambit of responsibility of the organization, if not the state (e.g. through safety regulation). With that, the custodian role of safety management arose, becoming a master narrative, a central legitimating myth that is today often taken for granted in how we discuss safety. Thus, the idea that we are caretakers of already basically safe systems runs deep. The corollary is that already safe systems need better protection from the unreliability of the human component—a commitment recently exemplified by Lee and Harrison (2000, pp. 61-62; emphasis in the original):

It is now generally acknowledged that individual human frailties … lie behind the majority of the remaining accidents. Although many of these have been anticipated in safety rules, prescriptive procedures and management treatises, people don't always do what they are supposed to do. Some employees have negative attitudes to safety which adversely affect their behaviours. This undermines the system of multiple defences that an organisation constructs and maintains to guard against injury to its workers and damage to its property.

The frailties of individuals are seen here as the major residual source of risk: they undermine the engineered and managed features of already safe systems. This master narrative bestows legitimacy on a set of unifying and very common countermeasures. "People don't always do what they are supposed to do" literally spells unreliability: an erratic, unpredictable residue of variability that should be engineered out of these systems through more automation, better education or indoctrination in safety, stricter procedures, or, most techno-optimistically, tighter monitoring of their behavior in the workplace.

That these ideas are relatively recent illustrates that safety research is not yet enjoying a period of wholesale post-Newtonian infatuation. Instead, safety research is undergoing something more unsettled and turbulent—a situation of tentative engagement, uncertainty and experimentation. While a techno-optimistic preoccupation with componential approaches is intensifying in some quarters (e.g. flight data monitoring), it is in this period, this important era, that Resilience Engineering is emerging as an exciting, new systems approach to understanding safety and risk.

One important concept in resilience is that of emergence, which means that simple entities, because of their interaction and feedback, their cross-adaptation and cumulative change, can produce far more complex behaviors as a collective, and produce effects across scales different from those along which the entities themselves operate. Emergence tries to shed light on the micro-macro connection: how local behavior can produce global effects in ways that are unpredictable at the local level. One common experience is that infinitesimally small changes in starting conditions (e.g. one assumption made in one line of software code) can lead to huge consequences (enormous releases of energy, such as a Mars Polar Lander crashing onto the surface, or huge overdoses of radioactive energy in cancer treatment with radiation therapy (Leveson, 2002)). Small changes in the initial state of a complex system, in other words, can drastically alter the final outcome. Such effects are impossible to capture with linear or sequential models that make Newtonian cause-effect assumptions and that cannot accommodate non-linear feedback loops, growth, or cumulative change. Also, Gaussian models where means and medians dominate discussions of probability, cannot account for (let alone predict) the devastating effects of outliers (those at the tail ends of the Gaussian distribution, of the bell curve) (Taleb). Instead, it takes for example complexity theory to understand how simple things can generate very complex outcomes that could not be anticipated by just looking at the parts themselves.

The systems perspective, of living organizations whose stability is dynamically emergent rather than structurally inherent, suggests that safety is something a system does, not something a system has. Failures in the systems perspective represent breakdowns in adaptations directed at coping with complexity: it is related to limits of the current model of competence, and, in a learning organization, reflects a discovery of those boundaries (which, in dynamic operational environments, are shifting most of the time). The aim of a resilient organization is not stability, but sustainability. Taking the living-system perspective means that the future is uncertain; the system's conditions irreversible (in Newtonian physics they would be time-reversible: only the initial conditions and the machinistic Newtonian laws need to be known). In systems thinking, any laws that could be formulated can only enumerate possibilities, never certainties. This means that the usefulness of retrospective event analysis, such as in accident investigations, is limited: in a complex, living system, possibilities for its future are not determined by what it displayed in the past—the science of linear equilibria does not apply, nor the Newtonian symmetry between past and future.

Social science initially aimed to learn the truth through empirical experiments and a positivist science, so as not to invent or intuit the truth, or simply tell stories about it, as for example

history had done. The way in which social science fragmented into different disciplines during the nineteenth century was meant to secure and advance this supposedly objective knowledge; a liberation from metaphysics and theology as acceptable modes of explaining reality (Wallerstein et al., 1996). This search for quantifiable laws of the social world was a first mimetic endeavor by social inquiry to safeguard its status as a real science: producing "hard" evidence and numbers rather than soft arguments. But even though a nomothetic epistemology had come to dominate 20th century social science by applying Newtonian concepts to social phenomena, this hold is now loosening. Efforts by social sciences to be taken as a legitimate academic enterprise are changing, and as one result, natural sciences seem closer to "soft" social science. Such rapprochement comes not, this time, because of social science's mechanization of humanity or its ever-diffident quantitativist curtseys, but because "hard" sciences are emphasizing non-linearity over linearity, complexity over simplification, holism over reductionism and qualitative scope over putative quantitative accuracy. And hard sciences too, have had to acknowledge the impossibility to remove the observer from the observation—what was once a time-honored accusation of subjectivity leveled at social science.

This has significant consequences for the role and credibility of social science in safety research. As "hard" sciences become softer and relinquish rigorous determinism and predictability together with other long-held Newtonian-Cartesian notions, social science's status is vicariously rehabilitated, at least as much as its ability to shed new light on the complex, muddled workings of safety-critical organizational-social life. That this produces approximations rather than accurate predictions (e.g. indicators of resilience rather than measures is seen as acceptable, and no longer blamed on the inexactitude of social-scientific knowledge. In fact, it is entirely consistent with natural science working to extend the formulation of laws of dynamics to include emergence, irreversibility and probability so as to be able to better describe events, novelty, and creativity in natural systems, an epistemological commitment not far from the heart of social science. The gap between natural (hard) and social (soft) science, as a result, is shrinking. The opportunities this creates for a new dialogue on safety, or rather, resilience, are numerous, and they are explored in both retrospective and prospective in this report.

Resilience and the legacy of ideas on accidents, human error, and systems

Resilience Engineering is the latest, and in many ways most exciting departure from the popular image in which the typical path to disaster is a single and major failure of a system component—very often the human. In this popular image, which Resilience Engineering tries to attack, "human error" is often seen as a cause, or important contributor, to accidents.

Our understanding of how accidents happen has undergone a dramatic development over the last century (Hollnagel, 2004). Accidents were initially viewed as the conclusion of a sequence of events (which involved "human errors" as causes or contributors). This is now being increasingly replaced by a systemic view in which accidents emerge from the complexity of people's activities in an organizational and technical context. These activities are typically focused on preventing accidents, but also involve other goals (throughput, production, efficiency, cost control) which means that goal conflicts can arise, always under the pressure of limited resources (e.g. time, money, expertise). Accidents emerge from a confluence of conditions and occurrences that are usually associated with the pursuit of success, but in this combination—each necessary but only jointly sufficient—able to trigger failure instead.

In the systemic view, "human errors" are labels for normal, often predictable, assessments and actions that make sense given the knowledge, goals and focus of attention of people at the time;

assessments and actions that make sense in the operational and organizational context that helped bring them forth. "Human error," in other words, is the product of factors that lie deeper inside the operation and organization; and that lie deeper in history too. In this final report, we review a number of ideas of how accidents occur, roughly in historical order, and assess each for their role in helping us understand resilience, or what place they have on or off the historical trajectory leading us to what we today know as Resilience Engineering—the main topic and sole focus of the last part of the report. Indeed, if resilience engineering represents a new direction for measuring and maintaining safety in complex systems, it is important to show how exactly it is "new" and what opportunities for novel ways of approaching safety it offers. Embodied in cases (set in italic font in this report) is a part of the empirical work conducted for this project. Thee empirical encounters, also as detailed in the various progress reports, has been instrumental in informing and shaping the ideas about resilience expressed and collated in this final report.

From stopping linear sequences to the control of complexity

Accidents seem to confront us in their great diversity, yet research into them is marked by an exploration of systematic features and common patterns. In this report, we have divided our treatment of complex system failure into two, based on important assumptions that the models in them make about how accidents happen and, in turn, what implications this has for thinking about resilience. Of course this cut is not entirely clean, as elements from each set of ideas get borrowed and transferred across those conceptual lines. In general, though, a shift can be seen from models that treat accidents as the outcome of a series of events along a linear pathway, to accidents as emergent from the interaction of a multitude of events in a complex system. Different assumptions about the nature of organizations, accidents, about causes and about possible mitigation enter into these two rough categories.

Models in the first category, which are treated in more detail in the next part, are the following:

- The sequence-of-events model
- Man-made disaster theory
- The latent failure model

They have adopted their basic ideas from industrial safety improvements the first half of the twentieth century. Consistent with this lineage, they suggest we think of risk in terms of energy—e.g. a dangerous build-up of energy, unintended transfers, or uncontrolled releases of energy (Rosness, Guttormsen, Steiro, Tinmannsvik & Herrera, 2004). This risk needs containing, and the most popular way is through a system of barriers: multiple layers whose function it is to stop or inhibit propagations of dangerous and unintended energy transfers. This separates the object-to-be-protected from the source of hazard by a series of defenses (which is a basic notion in the latent failure model). Other countermeasures include preventing or improving the recognition of the gradual build-up of dangerous energy (something that inspired Man-made disaster theory), reduce the amount of energy (e.g. reduce vehicle speeds or the available dosage of a particular drug in its packaging), prevent the uncontrolled release of energy or safely distribute its release. Such models are firmly rooted in Newtonian visions of cause, particularly the symmetry between cause and effect. Newton's third law of motion is taken as self-evidently applicable: each cause has an equally large effect (which is in turn embedded in the idea of preservation of energy: energy can never disappear out of the universe, only change form). Yet such presumed symmetry (or cause-consequence equivalence) can mislead human error research and practitioners into believing that really bad consequences (a large accident) must have really large causes (very bad or egregious human errors and violations).

The conceptualization of risk as energy to be contained or managed has its roots in efforts to understand and control the physical (or purely technical) nature of accidents. This also spells out the limits of such conceptualization: it is not well-suited to explain the organizational and socio-technical factors behind system breakdown, nor equipped with a language that can meaningfully handle processes of gradual adaptation, risk management, and decision making. The central analogy used for understanding how systems work is the machine, and the chief strategy reductionism. To understand how something works, these models have typically dismantled it and looked at the parts that make up the whole. This approach assumes that we can derive the macro properties of a system (e.g. safety) as a straightforward function of, or aggregation from, the lower-order components or subsystems that constitute it. Indeed, the assumption is that safety can be increased by guaranteeing the reliability of the individual system components, and that if components (even layers of defense) do not fail, then accidents will not occur.

The accelerating pace of technological change has introduced more unknowns into our safety-critical systems, and made them increasingly complex. Computer technology, and software in particular, has changed the nature of system breakdowns. Accidents can emerge from the complex, non-linear interaction between many reliably operating sub-components. The loss of NASA's Mars Polar Lander, for instance, was related to spurious computer signals when the landing legs were deployed during descent towards the Martian surface. This "noise" was normal; it was expected. The onboard software, however, interpreted it as an indication that the craft had landed (which the software engineers were told it would indicate) and shut down the engines down prematurely. This caused the spacecraft to crash into the Mars surface. The landing leg extension and software all performed correctly (as specified in their requirements), but the accident emerged from unanticipated interactions between leg deployment and descent-engine control software (Leveson, 2002).

Accidents where no physical breakage can be found of course heightens suspicions about human error. Given that no components in the engineered system malfunctioned or broke, the fault must lie with the people operating the system; with the human component, the human factor. This is indeed is what some models tend to do: failures of risk management can get attributed to deficient supervision, ineffective leadership, or lack of appropriate rules and procedures (which points to components that were broken somewhere in the organization). But this just protracts reductive thinking, and it is increasingly questionable whether broken components represent meaningful targets for intervention (by eliminating "errors" in the design or operation or control of a safety-critical process) in highly complex and tightly coupled socio-technical systems. Indeed, more recent accident models attempt to make a break from machinistic, componential images of organizations and risk containment. Instead, they view systems and their behavior as a whole as the unit of interest and analysis. These are the models that will be dealt with in later in the report, leading up to a discussion of resilience engineering:

- Normal accidents theory
- Control theory
- High reliability theory
- Resilience engineering

With it, they abandon Newtonian ideas about the symmetry between cause and effect, instead trying to understand how failure emerges from the normal behaviors of a complex, non-linear system. Inspired by recent developments in science that have embraced such more complex understandings longer since, the most recent addition to thinking about accidents, Resilience Engineering, no longer talks about human error at all. Instead, it focuses on the ability of systems

to recognize, adapt to and absorb disruptions and disturbances, even those that fall beyond the capabilities that the system was trained or designed for. This concern with adaptation as a central capability that allows living systems to survive in a changing world, has been inspired by a number of fields external to the traditional purview of human error research, for example biology, materials science, and physics. Rather than looking for the sorts of negatives (errors, violations, incidents) that point to broken or bad components, and then trying to make them go away ("eliminate" them), resilience engineering sees safety as something positive, as the presence of something, not the absence.

Practitioners and organizations, as adaptive, living 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. This can avoid narrow interpretations of risk and stale strategies.

The principles of organization in a living system are unlike those of machines. In contrast to a machine that either works to specification or does not, 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.

Complex, living systems are dynamically stable, not statically so (which most machines are). Stability and instability emerge 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. To keep a machine working, we want to check the serviceability of its parts and their interactions. Throw out the bad parts, grease the interactions, 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, Woods & Leveson, 2006). The reason for this is that these influences are also ecologically adaptive and help guarantee the system's survival. 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. Failures represent breakdowns in adaptations directed at coping with complexity, which dramatically shifts, and turns into something more positive, the focus of interest for human error research.

Linear thinking and latent failures:
The groundwork from which resilience engineering departs

Accidents as sequences-of-events

Accidents can be seen as (the outcome of) a sequence, or chain, of events. This simple, linear way of conceptualizing how events interact to produce a mishap was first articulated by Heinrich in 1931 and is still dominant in various ways today. According to this model, events preceding the accident happen linearly, in a fixed order, and the accident itself is the last event in the sequence. It has been known too as the domino model, for its depiction of an accident as the endpoint in a string of falling dominoes (Hollnagel, 2004). Consistent with the idea of a linear chain of events is the notion of a root cause—a trigger at the beginning of the chain that sets everything in motion (the first domino that falls and then, one by one, brings down the rest). The sequence-of-events idea is pervasive, even if multiple parallel or converging sequences are sometimes depicted to try to capture some of the greater complexity of the precursors to an accident. The idea forms the basic premise in many risk analysis methods and tools such as fault-tree analysis, probabilistic risk assessment, petri nets, critical path models and more.

Also consistent with a chain of events is the notion of barriers—a separation between the source of hazard and the object or activity that needs protection. Barriers can be seen as blockages between dominoes that prevent the fall of one affecting the next, thereby stopping the chain reaction. From the 1960's to the early 1980's, the barrier perspective gained new ground as a basis for accident prevention. Accidents were typically seen as a problem of uncontrolled transfer of harmful energy, and safety interventions were based on putting barriers between energy source and the object to be protected. The goal was to prevent, modify or mitigate the harmful effects of energy release, and pursuing it was instrumental in improving for example road safety. Strategies there ranged from reducing the amount of energy through speed limits, to controlling its release by salting roads or putting up side barriers, to absorbing energy with airbags (Rosness, Guttormsen, Steiro, Tinmannsvik & Herrera, 2004).

Case: Space Shuttle Columbia break-up
The physical causes of the loss of Space Shuttle Columbia in February 2003 can be meaningfully captured through a series of events that couples a foam strike not long after launch with the eventual breakup sequence during re-entry days later. A piece of insulating foam that had separated from the left bipod ramp section of the External Tank at 81.7 seconds after launch struck the wing in the vicinity of the lower half of the reinforced carbon-carbon panel. This caused a breach in the Thermal Protection System on the leading edge of the left wing. During re-entry this breach in the Thermal Protection System allowed superheated air to penetrate through the leading edge insulation and progressively melt the aluminum structure of the left wing, resulting in a weakening of the structure until increasing aerodynamic forces caused loss of control, failure of the wing, and break-up of the Orbiter. This breakup occurred in a flight regime in which, given the current design of the Orbiter, there was no possibility for the crew to survive.

The sequence-of-events model, and particularly its idea of accidents as the uncontrolled release and transfer of hazardous energy, is a very Newtonian vision of how accidents happen, and how cause and effect relate to each other. Newton's third law of motion (for each action there is an equal and opposite reaction) forms the basis for the idea of preservation of energy in a system: Energy can only change form but there is a fixed amount of it that cannot be changed. In Newtonian thought, there is not only a recursion (each effect is also a cause, and each cause an

effect) but also a symmetry between cause and effect. This cause-consequence equivalence has become an assumption that we often take for granted in our consideration of accidents. People may see as self-evident, for example, that a very big effect (e.g. in numbers of fatalities) must have been due to a very big cause (e.g. really egregious errors) otherwise the implicit understanding of Newton's law would be violated. The cause-consequence equivalence assumption shows up in issues of accountability too, for example in how a judicial system typically assesses a person's liability or culpability on the basis of the gravity of the outcome.

In the Columbia case such cause-consequence symmetry (and the preservation of energy through successive conversions—gravity, speed, friction, heat, breakup) can still meaningfully be used for modeling important aspects of the last few minutes of the Shuttle's re-entry. It even affords the sort of linear depiction of events that could help with the identification of barriers that help in future prevention (from better pre-entry inspection of damage to hull or wings that could promote unwanted energy transfer or release, to separating people from the energy being released by creating a crew escape module). But the contribution of organizational factors to the accident—a normalization of signals of danger, the lack of a safety culture at NASA, organizational turbulence and contractor issues, acute production and budget pressures—are much less amenable, if at all, to being modeled as a linear sequence of events. Instead, these factors require a different kind of analysis and must be thought of as having a much more complex bearing on the eventual accident than a simple, linear cause-effect relationship. The Newtonian symmetry between cause and effect no longer really applies to how accidents are produced in complex systems—generally from the 1950's onward.

Sequences of events and "human error" versus resilience

The idea of separating sources of hazard from objects or processes that must be protected by a linear series of barriers is still popular today. It embodies particular assumptions about the role and nature of human error in accident causation. In particular, the conception of human error in such models is often as a discrete, binary event (the human did or did not do something): a bifurcation or fork in the linear pathway. "Human error" is not really an effect, but still a cause: one of the events that contributes to the eventual outcome of the series.

This of course oversimplifies the situations that people really faced at the time, often boiling them down to a choice between making an error or not making an error. We invoke such thinking when we wonder, "if only they had seen or done this or that, then they could have avoided the outcome." Versions of such thinking often show up in accident reports and remarks by stakeholders after accidents. This is a by-product of the way in which sequences of events are constructed: the accident is not only the actual reason for making them, but also often the starting point. From there, we reason backward in time, arriving rearward at successive branches in the sequence of events that split off towards other outcomes than the one we began from, which of course begs the question why people did not think of that at the time.

Crucially, the outcome we take for granted as the inevitable effect of people's choices wasn't known to those people at the time. This, however, is not the way in which events unfolded around those caught up in them during real-time: for them, choice moments were not likely the binary options that they seem to be in after-the-fact analysis. These choices, such as they were, would have been wrapped in a flow of other activities, surrounded by much more uncertainty, and all of them aimed at maintaining control, at creating resilience.

The relationship between incidents and accidents

An important by-product of the sequence of events model is the perceived difference between incidents and accidents. If an accident is the conclusion of a sequence of events that proceeded all the way to failure, then an incident is a similar progression with one difference—it was stopped in time. This has been an attractive proposition in much safety work. Not only is it cheaper to combat incidents by trying to arrest a causal progression early on; incidents also occur more frequently than accidents, which makes learning from them more efficient (and less costly too). The assumption is that incidents and accidents are similar in substance, but only different in outcome: the same factors contribute to the progression towards failure, but in one case the progression is stopped, in the other it is not (often due to the presence or absence of additional factors). This is where the idea of dress rehearsals comes from: the same problems in for example the operation of a human-machine interface can in some situations combine with other factors that push the system over the brink of failure.

This notion has been taken further still, separating accidents from incidents, and incidents from near misses. A near miss is stopped even earlier in the progression towards failure. Take air traffic control, for example. An accident would be a collision with another aircraft. An incident would be the violation of separation minima (e.g. five nautical miles lateral and one thousand feet vertical) but no physical contact between aircraft. A near miss could be the skirting of those separation minima, but not their actual violation. An even lesser degree than near misses could be unsafe acts, which raise the risk of a near miss or more, but do not actually lead to them. These categories of accidents, incidents, near misses and unsafe acts are used differently in different settings, of course, but they are bound by the assumptions that one category can help produce the next if the progression is not stopped, and that they share a largely common causal pattern.

These assumptions have been popularized in the so-called iceberg model, a classic in safety work (see figure 1). The iceberg model proposes that there are a certain number of incidents for each accident, and a certain number of near misses for each incident, and so forth. The typical ratio used is 1 accident for 10 incidents for 30 near misses for 600 unsafe acts (1:10:30:600). These numbers, to the extent that the various categories are meaningfully measurable at all (which is doubtful for near misses and unsafe acts especially because of typically low reporting rates for them), have achieved almost a mythical status, but reality can be very different. Occupational health and safety statistics in the UK, for example, show 220 fatal injuries in a year, and 28.652 nonfatal ones—a ratio of 1:130. In contrast there were very few near misses, and essentially no unsafe acts reported at all (Hollnagel, 2004).

The iceberg model may have some relevance in simple systems, where the number of possible accidents is very limited (e.g. when standing on a ladder for the painting of a wall) and the incidents, near misses and unsafe acts can all be directly related to the risk that gets its eventual expression in that one accident at the top (falling off the ladder). Yet even in more complex systems (e.g. air traffic control, nuclear power generation, commercial aviation, various branches of medicine), near misses are often used to predict the kinds of incidents that may happen, and incidents are used to predict, and hopefully prevent, accidents. This is the idea behind enormously popular incident reporting systems in many safety-critical worlds—taking those "free lessons" and turning their content into leverage for safety and prevention work.

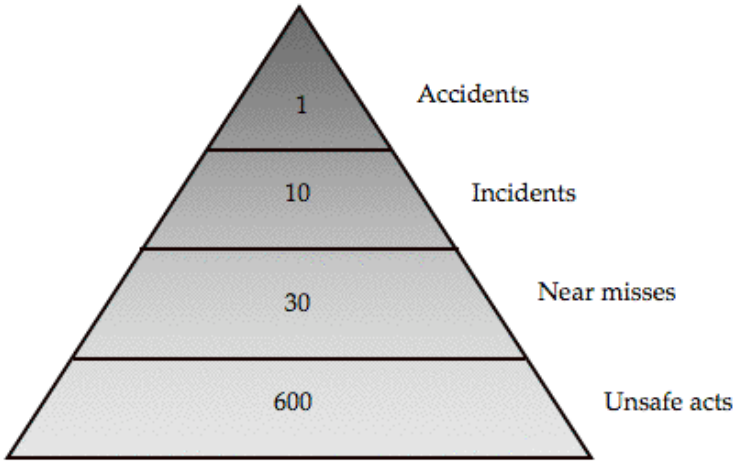


Figure 1. The mythical iceberg model

In more complex systems, however, the relationship between the emergence of accidents and the existence of problems that do not lead to outcome failures (which we variously call incidents, near misses and so forth) is far more complex. And in some cases, there appears to be no substantive relationship at all. This means that incidents in those systems cannot predict accidents, and that collecting data about incidents can help the system, at best, predict and prevent incidents—not accidents (Amalberti, 2001). Data from scheduled airline flying in the US seem to confirm this (see Table 1). The table shows correlations between the number of nonfatal accidents or incidents per 100,000 major carrier departures and their passenger mortality risk. Interestingly, all correlations are negative: carriers with higher rates of non-fatal accidents or non-fatal incidents had lower passenger mortality risks. This directly contradicts the iceberg proposition: the more incidents there are, the fewer fatal accidents. In fact, the table basically inverts the iceberg, because correlations become increasingly negative when the events suffered by the carrier become more severe. If the non-fatal accident that happened to the carrier is more severe, in other words, there is even less chance that a passenger will die onboard that carrier.

Type of non-fatal event	Correlation
Incidents only	-0.10
Incidents and accidents	-0.21
Accidents only	-0.29
Serious accidents only	-0.34

Table 1. Correlation of major US Jet air carrier nonfatal accident/incident rates and passenger-mortality risk, January 1, 1990 to March 31, 1996 (Barnett & Wang, 2000, p. 3).

Statistically, scheduled airline flying in the US is very safe: a single passenger would have to fly 19.000 years on end to die in an airline accident (Barnett & Wang, 2000). This is consistent with Amalberti's (2001) observations of ultra-safe systems: it is particularly in those systems with very low overall accident risk that the predictive value of incidents becomes very small. One reason is that these ultra-safe systems have matured, are typically over-regulated and have learned to operate safely, yet are constantly under resource and production pressures. Working successfully implies working at quasi-incident levels where deviance becomes the standard of normal

operations. That which could be classified as an "incident" no longer is (because it has become normal) and is thus not reported as such either (Dekker, 2005). In such ultra-safe systems,

> "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)

This means that before an accident, proponents of safety measures can find themselves in a difficult position. What they see as warning signals are things that do not usually herald a specific failure. Because of this, it can be hard to get the attention of responsible people, and efforts to improve safety come across to them as diffuse and general. Paradoxically, the costs of these measures are easily calculated while their potential benefits remain unknown and unknowable. Together, these characteristics tend to channel organizational work on safety towards low cost ventures that do not affect production. Because failure is rare, warning signals may be separated from overt accidents by long periods of time. This may have the effect of making the warning signals seem uninformative. System managers may come to believe that dismissing these warning signals reflects good judgment rather than successful gambling. It is easy to rationalize away warnings, especially when the system itself is operating near the margins of economic failure (as many airlines do, and healthcare systems, for that matter).

Detailed investigations of accidents thus frequently show that the system was managed towards catastrophe, often for a long while. Accidents are not anomalies that arise from isolated human error. Instead, accidents are "normal" events that arise from deeply embedded features of the systems of work (Perrow, 1984). Complex systems have a tendency to move incrementally towards unsafe operations (Rasmussen, 1997). Because they are expensive to operate, there is a constant drive to make their operations cheaper or more efficient. Because they are complex, it is difficult to project how changes in the operations will create opportunities for new forms of failure. Because many of the changes are difficult to reverse (e.g. when they involve new technology or significant organizational change) there may be little opportunity to return to the old ways of doing things.

Case: Texas A&M University bonfire

The Texas A&M University bonfire tragedy is a case in point. The accident revealed a system that was profoundly out of control and that had, over a long period, marched towards disaster (see Petroski, 2000). On November 18, 1999, a multi-story stack of logs that was to be burned in a traditional football bonfire collapsed while being built by students at the Texas A&M University. Twelve students working on the structure were crushed to death as the structure collapsed. Twenty-seven others were injured. It was the worst such disaster at a college campus in the United States and was devastating within the tight knit community that prided itself on its engineering college. An independent commission was established to investigate the causes of the collapse. Extensive and expensive engineering studies were conducted that showed that the collapse was the result of specific aspects of the structural design of the bonfire. It revealed that the collapse happened because the bonfire had evolved from being a conventional bonfire into a large scale construction project. That project had never been competently designed or analyzed and was largely carried out by unsupervised amateurs.

The bonfire was a Texas A&M football tradition that extended over many years. It began in 1928 as a haphazard collection of wooden palettes. It grew gradually, increasing in scale and complexity each year until the 1990's when it required a crane to erect. In 1994 a partial collapse occurred but was attributed to shifting ground

underneath the structure rather than structural failure per se. The catastrophe five years later overwhelmed the medical facilities of the area. The response to the failure made it clear that no one imagined that this sort of disaster was possible, let alone likely. In hindsight, it seems incredible that this should be the case. Even here hindsight misleads us into believing that the inevitability of this particular sort accident should have been apparent. It was not at all obvious before the fact. The relative lack of failure over many years produced a sense that failure was unlikely, even through the growing structure over the years was taking the system in that direction. Each increment in complexity and scale was too small to signal that the system was becoming dangerous in new ways. The bonfires of the late 1990's reached new heights without anyone understanding what those heights meant. The inability to recognize that the system was unsafe was a property of the system itself, a property essential to the development of the accident situation.

Against the backdrop of success, warning signals like the partial collapse could be discounted. The partial collapse was treated as an incident. It was not large enough to garner the sort of attention needed for the kind of detailed examination that would show how dangerous these new bonfires were. Only a truly catastrophic failure was enough to produce a new look at what the bonfire had become. The group managing the bonfire had marched into tragedy with their eyes open but unable to interpret what they were seeing.

The sequence-of-events model no longer really applies to how things go wrong in such situations. The slow but steady drift towards safe operating margins that typically marks the period before an eventual accident is characterized by what everybody sees as normal work under normal everyday pressures, expectations or demands. And historical success provides a basis for confidence in future results. With rising expectations of system performance because of historical success, risk rises too—but invisibly so because of the signals people in the system are attuned to, what they know what to look for.

Accidents, then, are the result of normal people doing normal work, and bear no semblance to the kinds of problems that would still be reported as incidents. And the psychological and organizational processes that form the engine behind such drift and its gradual loosening of safety constraints, can really not be modeled meaningfully as a causal series, instead demanding a much more dynamic and complex depiction (Leveson, 2002). The Newtonian assumption of symmetry between cause and effect no longer applies either. Very small changes in starting conditions can lead to devastatingly huge consequences—in ultra-safe systems, the causes, banally embedded as they are in normal work done by normal people in efforts to handle normal, everyday pressures, are rarely as big as the effects that are made visible in an accident. Some of these ideas have been captured more effectively by what is now known as man-made disaster theory.

Man-made disaster theory

In 1978, Barry Turner offered one of the first accounts of accidents as a result of normal, everyday organizational decision making. Accidents, Turner concluded, are neither chance events, nor acts of God, nor triggered by a few events and unsafe human acts immediately before they occur. Nor is it useful to describe accidents in purely technological terms (Pidgeon and O'Leary, 2000). Turner's idea was that "man-made disasters" often start small, with seemingly insignificant operational and managerial decisions. From then, there is an incubation period. Over a long time, problems accumulate and the organization's view of itself and how it manages its risk grows increasingly at odds with the real state of affairs, until this mismatch actually explodes into the open in the form of an accident (Turner, 1978). Man-made disaster theory preserved important notions of the sequence-of-events model (e.g. problems at the root that served to trigger others

over time) even if the sequence spread further into the organization and deeper into history than in any model before then. Yet the theory added a new focus and language to the arsenal of safety thinking.

An important post-accident discovery highlighted by man-made disaster theory is that innocuous organizational decisions turned out to interact, over time, with other contributory preconditions in complex and unintended ways. None of those contributors alone is likely to trigger the revelatory accident, but the way they interact and add up falls outside the predictive scope of people's model of their organization and its hazard control up to that moment. Turner's account was innovative because he did not define accidents in terms of their physical impact (e.g. uncontrolled energy release) or as a linear sequence of events. Rather, he saw accidents as sociological phenomena. Accidents represent a disruption in how people believe their system operates; a collapse of their own norms about hazards and how to manage them.

An accident, in other words, comes as a surprise, as a shock to the image that the organization has of itself, of its risks and of how to contain them. The developing vulnerability has long been concealed by the organization's belief that it has risk under control, a belief that it is entitled to according to its own model of risk and the imperfect organizational cognitive processes that help keep it alive. Vaughan (1996) would later use this notion to shed new light on the Challenger Launch disaster, showing how "structural secrecy" (broken information links as a result of organizational structures) across the NASA and contractor bureaucracies attenuated evaluations of blow-by risk in the Shuttle's solid rocket boosters. Such blow-by (hot propellant gases squirting through the joints in the solid rocket boosters) was found to be the major factor in the breakup of Space Shuttle Challenger not long after it was launched.

Already in 1979, Stech saw how this idea applied to the failure of Israeli intelligence organizations to foresee what would become known as the Yom Kippur war, even though all necessary data that pointed in that direction was available somewhere across the intelligence apparatus. Reflecting in part on the same events, Lanir (1986) used the term "fundamental surprise," to capture this sudden revelation that one's perception of the world is entirely incompatible with reality. In the wake of accidents, however, there is often pressure to convert fundamental surprises into local ones, as it is psychologically easier and economically cheaper to correct a local "human error" than it is to re-asses the entire groundwork of assumptions governing the control of hazard in an industry.

Interestingly, the surprise in man-made disaster theory is not that a system that is normally successful suddenly suffers a catastrophic breakdown. Rather, the surprise is that a successful system produces failure as a normal, systematic by-product of its creation of success. An accident potential does not build up at random, as if it were some abnormal, irrational growth alongside and independent from 'normal' organizational processes. On the contrary, man-made disaster theory suggests how the potential for an accident accumulates precisely because it is able to make opportunistic, non-random use of organized systems of production that until then are responsible for organizational success and safety.

Take the processing of food in one location. This offers greater product control and reliability (and thus, according to current ideas about food safety, better and more stringent inspection and uniform hygiene standards). Such centralized processing, however, also allows effective, fast, and wide-spread distribution of unknowingly contaminated food to many people at the same time precisely thanks to the existing systems of production. This happened during the outbreaks of food poisoning from the E-coli bacterium in Scotland during the 1990's (Pidgeon and O'Leary, 2000). This same centralization of food preparation, now regulated and enforced as being the

safest in many Western military forces, also erodes cooks' expertise at procuring and preparing local foods in the field when on missions outside the distribution reach of centrally prepared meals. As a result of centralized control over food preparation and safety, the incidence of food poisoning in soldiers on such missions typically goes up rather than down.

Case: Boeing 757 landing incident

On the evening of December 24, 1997, the crew of a Boeing 757 executed an autopilot-coupled approach to a southerly runway at Amsterdam (meaning the autopilot was flying the aircraft down the electronic approach path toward the runway). The wind was very strong and gusty out of the south-west. The pilot disconnected the autopilot at approximately 100 ft above the ground in order to make a manual landing. The aircraft touched down hard with its right main wheels first. When the nose gear touched down hard with the aircraft in a crab angle (where the airplane's body is moving slightly sideways along the runway so as to compensate for the strong crosswind), the nose wheel collapsed, which resulted in serious damage to the electric/electronic systems and several flight- and engine control cables. The aircraft slid down the runway, was pushed off to the right by the crosswind and came to rest in the grass next to the runway. All passengers and crew were evacuated safely and a small fire at the collapsed nose wheel was quickly put out by the airport fire brigade (Dutch Safety Board, 1999).

In an effort to reduce the risks associated with hard landings, runway overruns and other approach and landing accidents, the aviation industry has long championed the idea of a "stabilized approach" whereby no more large changes of direction, descent rate, power setting and so forth should be necessary below a particular height, usually 500 feet above the ground. Should such changes become necessary, a go-around is called for. Seeing a stabilized approach as "the accepted airmanship standard" (Sampson, 2000), many airline safety departments have taken to stringent monitoring of electronic flight data to see where crews may not have been stabilized (yet "failed" to make a go-around). One operational result (even promoted in various airlines' company procedures) is that pilots can become reluctant to fly approaches manually before they have cleared the 500 ft height window: they rather let the automation fly the aircraft down to at least that height. This leads to one of the ironies of automation (Bainbridge, 1987): an erosion of critical manual control skills that are still called for in case automation is unable to do the job (as it would have been unable to land the aircraft in a crosswind as strong as at Amsterdam at the time). Indeed, the investigation concluded how there would have been very little opportunity from 100 ft on down for the pilot to gain effective manual control over the aircraft in that situation (Dutch Safety Board, 1999).

Some would call this "pilot error." In fact, one study cited in the investigation concluded that most crosswind-related accidents are caused by improper or incorrect aircraft control or handling by pilots (van Es, van der Geest and Nieuwpoort, 2001). But this pilot error, man-made disaster theory could say, was actually the non-random effect of a system of production that helped the industry achieve success according to its dominant model of risk: Make sure approaches are stabilized, because non-stabilized approaches are seen as a major source of hazard. Yet this seemingly sensible and safe strategy incubated an unintended vulnerability at the same time—a vulnerability that would not become obvious until triggered by local circumstances. Consistent with Turner's ideas, the accident revealed the limits of the model of success and risk the organization (and by extension, the industry) had entertained up until that time.

Also, consistent with the fundamental surprise error, the industry is reluctant to revise its model of risk and interprets fundamental evidence that its model is wrong or only partially right (or at least that it produces hazardous side-effects) as only a local problem of "human error." With the information of recent accidents in its hands, it regresses to its idea of pilot error as their cause ("perfectly functioning airplanes in relatively good weather crashed during a failed go-around," (Sampson, 2000, p. 1)). The alternative would be to go behind the label "human error" to uncover the second story: a complex organizational, administrative and cultural story, where hazard is incubated through the unintended side-effects of adherence to a partial model of risk and strategy for containing it (unstabilized approaches are risky, we need more stringent monitoring to make sure approaches are stabilized).

Man-made disaster theory, "human error" and resilience

Man-made disaster theory holds that accidents are administrative and managerial in origin—not just technological. A field that had been dominated by languages of energy transfers and barriers was thus re-invigorated with a new longer-term perspective that stretched people's focus across the softer, social-organizational incubation of disaster over longer periods. Any "human errors" that may have finally triggered the accident are themselves the result of problems that have been brewing inside the organization much longer. No serious accident inquiry since Turner has been able to do without taking such organizational incubation into account and pointing to the wider context from which "errors" stem (under whatever label; e.g. "latent failures," "holes in defense layers"). The theory was the first to put issues of company culture and institutional design (which determines organizational cognition, which in turn governs information exchange) at the heart of the safety question (Pidgeon and O'Leary, 2000). Basically all organizational accident thinking developed since the seventies owe intellectual debt to Turner and his contemporaries (Reason, Hollnagel & Pariès, 2006), even if most of those models are quite poor at illuminating the processes by which such incubation occurs, or, conversely, how resilience is maintained (Dekker, 2005).

There is an unresolved position on human error in man-made disaster theory that reverberates even through the subsequent models it has inspired. The theory posits that "despite the best intentions of all involved, the objective of safely operating technological systems could be subverted by some very familiar and 'normal' processes of organizational life" (Pidgeon and O'Leary, 2000, p. 16). Such "subversion" occurs through usual organizational phenomena such as information not being fully appreciated, information not correctly assembled, or information conflicting with prior understandings of risk. Turner noted that people were prone to discount, neglect or not take into discussion relevant information, even when available, if it mismatched prior information, rules or values of the organization. Thus, entire organizations could fail to take action on danger signals because of what he called "decoy" phenomena that distracted from the building hazard (Rosness et al., 2004).

One problem with a theory that relies both on the best intentions of all involved and on the misunderstanding or wrong appreciation of phenomena, needs to explain why these interpretations seemed right at the time, given the goals, knowledge and mindset of the decision makers involved. To this, man-made disaster theory doesn't really offer a solution, nor do its offshoots (e.g. Reason, 1997). The problem it runs into is one of normativism: "not fully" appreciating information implies a norm of what "fully" would have been. Not "correctly" assembling information implies a norm of what "correct" assembly would be—relative to which people fell short at the time. These norms, however, are left unexpressed in the theory. The reason is that it is only in hindsight, from the point of view of an omniscient retrospective observer, that one could point to what information should not have been discounted and instead appreciated better, or how exactly it should have been appreciated to qualify as "fully" or "correctly."

It is not, of course, that there is no variation in how teams or organizations deal with information, or that many of the processes by which they do this have no improvement potential. Westrum (1993) identified three organizational ideal types, whose cultures shape the way people respond to evidence of problems and other information:

- Pathological culture. Suppresses warnings and minority opinions, responsibility is avoided and new ideas actively discouraged. Bearers of bad news are "shot," failures are punished or covered up.
- Bureaucratic culture. Information is acknowledged but not dealt with. Responsibility is compartmentalized. Messengers are typically ignored because new ideas are seen as problematic. People are not encouraged to participate in improvement efforts.
- Generative culture. Is able to make use of information, observations or ideas wherever they exist in the system, without regard to the location or status of the person or group having such information, observation or ideas. Whistleblowers and other messengers are trained, encouraged and rewarded.

Westrum's generative culture points to some of the activities that can make teams and organizations resilient—able to remain sensitive to the possibility of failure and constantly updating their models of risk so they can adapt effectively under pressure, even in the face of novelty.

The other problem in man-made disaster theory is that of recursion. In some sense, it does not explain the problem of human error, but relocates its source up the causal pathway, further away from the place and time of the accident, by invoking new kinds of errors by other people there. It lifts the explanatory burden for an accident from the sharp-end operators (who inherit the accident rather than causing it) but then displaces the burden onto other humans (e.g. managers who failed to appreciate earlier on) to whose information processing errors the incubation of an accident can then be attributed instead. Again, man-made disaster theory does not go much further in showing light on why those assessments and actions made sense at the time, or why particular versions of risk could have become dominant through political processes and power relationships and structural secrecy common to any organization at the expense of other interpretations (Vaughan, 1996; Pidgeon and O'Leary, 2000). This problem of recursion (explaining one human error by referring to another and then stopping there) is something that afflicts similar theories of organizational accidents (see e.g. the latent failure model further below). It is also a risk that needs to be dealt with in explanations of design-induced errors later on in this book.

Latent Failures

The idea of latent failures is an evolution and combination of ideas from preceding theories and models on accident causation, particularly the sequence-of-events model and man-made disasters theory. According to the latent failure model, which first appeared in developed form in Reason (1990), disasters are characterized by a concatenation of several small failures and contributing events—rather than a single large failure (e.g., Pew et al., 1981; Reason, 1990). Multiple contributors are all necessary but individually insufficient for the disaster to occur. For example, the combination of multiple contributing events is seen in virtually all of the significant nuclear power plant incidents, including Three Mile Island, Chernobyl, the Brown's Ferry fire, the incidents examined in Pew et al. (1981), the steam generator tube rupture at the Ginna station and others. In the near miss at the Davis-Besse nuclear station (NUREG-1154), about ten machine failures and several erroneous human actions were identified that initiated the loss-of-feedwater accident and determined how it evolved.

Some of the factors that combine to produce a disaster are latent in the sense that they were present before the incident began. Turner (1978) discussed this in terms of the incubation of factors prior to the incident itself, and Reason (1990) refers to hidden pathogens that build in a

system in an explicit analogy to viral processes in medicine. Reason (1990) uses the term resident pathogen, or latent failure, to refer to errors or failures in a system that produce a negative effect but whose consequences are not revealed or activated until some other enabling condition is met. A typical example is a failure that makes safety systems unable to function properly if called on, such as the maintenance failure that resulted in the emergency feedwater system being unavailable during the Three Mile Island incident. Latent failures require a trigger, i.e., an initiating or enabling event, that activates its effects or consequences. For example in the Space Shuttle Challenger disaster, the decision to launch in cold weather was the initiating event that activated the consequences of the latent failure in booster seal design.

The concatenation of factors in past disasters includes both human and machine elements intertwined as part of the multiple factors that contribute to incident evolution. One cannot study these as separate independent elements, but only as part of the dynamics of a human-machine operational system that has adapted to the demands of the field of activity and to the resources and constraints provided by the larger organizational context (Rasmussen, 1986). The latent failure model thus distinguishes between active and latent failures:

Active failures are "unsafe acts" whose negative consequences are immediately or almost immediately apparent. These are associated with the people at the "sharp end," that is, the operational personnel who directly see and influence the process in question.
Latent failures are decisions or other issues whose adverse consequences may lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach the system's defenses (Reason, 1990). Some of the factors that serve as "triggers" may be active failures, technical faults, or atypical system states. Latent failures are associated with managers, designers, maintainers, or regulators—people who are generally far removed in time and space from handling incidents and accidents.

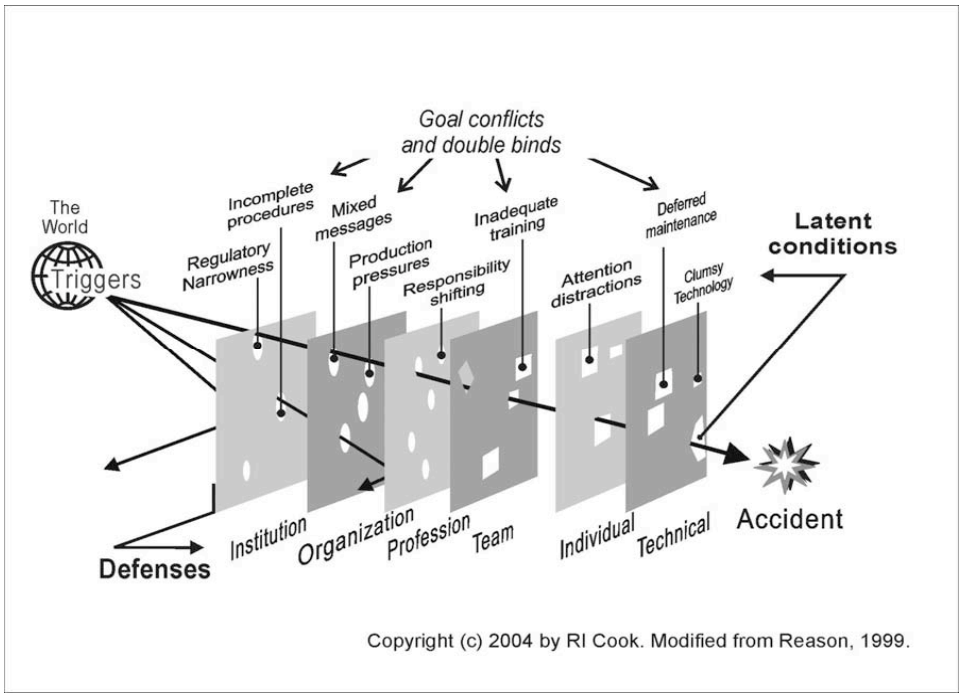


Figure 2. Complex systems failure according to the latent failure model. Failures in these systems require the combination of multiple factors. The system is defended against failure but these defenses have defects or "holes" that allow accidents to occur.

Case: The Air Ontario flight 1363 accident at Dryden, Canada

On Friday, March 10, 1989, a Fokker F-28 commuter jet aircraft took off from Dryden, Ontario on the last leg of a series of round trips between Winnepeg, Manitoba and Thunder Bay, Ontario. During the brief stopover in Dryden, the aircraft had been refueled. The temperature was hovering near freezing and it had been raining or snowing since the aircraft had landed. Several passengers and at least one crew member had noticed that slush had begun to build up on the wings. Flight 1363 began its takeoff roll but gathered speed slowly and only barely cleared the trees at the end of the runway. The Fokker never became fully airborne but instead crashed less than 1 km beyond the end of the runway. The aircraft, loaded with fuel, was destroyed by fire. Twenty-four people on board, including the pilot and co-pilot, were killed.

The initial assessment was that pilot error, specifically the decision to take off despite the icy slush forming on the wings, was the cause of the accident. The inexplicable decision to attempt takeoff was not in keeping with the pilot's record or reputation. The pilot was experienced and regarded by others as a thoughtful, cautious, and competent man who operated "by-the-book." Nevertheless, it was immediately obvious that he had chosen to take off in the presence of hazardous conditions that a competent pilot should have known were unacceptable. The reactions to this particular accident might well have ended there. Human error by practitioners is well known to be the proximate cause of 80% of accidents. At first, the Dryden Air Ontario crash seemed to be just another instance of the unreliability of humans in technological settings. If the pilot had been inexperienced or physically or mentally impaired (e.g. drinking alcohol before the crash), it is likely that attention would have turned away and the crash would today be remembered only by the survivors and families of those who died.

Instead, the Canadian Federal government commissioned an unprecedented investigation, under the direction of retired Supreme Court Justice Moshansky into all the factors surrounding the accident. Why it did so is not entirely clear but at least three factors seem to have played roles. First, the scale of the event was too large to be treated in ordinary ways. Images of the charred wreckage and the first-hand accounts of survivors captivated the entire country. The catastrophe was national in scale. Second, the accident "fit" hand-in-glove into a set of concerns about Canadian aviation, concerns that had been growing slowly over several years. These years had seen substantial change in Canadian commercial aviation. Airline deregulation had produced a significant increase in airline operations. New aircraft were being brought into service and new routes were being opened. In addition, the aviation industry itself was in turmoil. Once-small companies were expanding rapidly and larger companies were buying up smaller ones. Significantly, instead of keeping pace with the growth of commercial aviation, the Canadian government's aviation regulatory oversight body was shrinking as the government sought to reduce its budget deficit. There was no obvious connection between any of these large scale factors and the accident at Dryden, Ontario. But the small waves of concern about aviation safety that had been rippling across the surface of the country now appeared to be harbingers of the large wave that came from the accident.

The investigation took almost two years to complete and became the most exhaustive, most extensive examination of an aviation accident ever conducted. Well over 200,000 pages of documents and transcripts were collected and analyzed. The investigators explored not just the mechanics of flight under icing conditions but details about the running of the airport, the air transportation system, its organization, and its regulation. All these factors were linked together in the Commission's four volume report. The Report does not identify a single cause or even multiple causes of the accident. Instead, it makes clear that the aviation system contained many faults that together created an environment that would eventually produce an accident – if not on the 10th day of March in Dryden, Ontario, then on some other day in some other place (Maurino et al., 1999).

Bad weather at the Dryden airport was just one of many problems that came together on March 10, 1989. The airline itself was a family operation without strong management. It had traditionally relied on smaller, prop aircraft and had only recently begun jet operations. The operating manual for the Fokker F-28 had not yet been approved by Canadian regulators. The company's safety manager, an experienced pilot, had recently resigned because of disputes with management. There were 'deferred' maintenance items, among them fire sensors in the small engine

the Fokker carried that would allow it to start its main engines. Company procedures called for the engines to be shut down for deicing of the wings but there was no convenient way to restart them at Dryden: the company did not have ground starting equipment for its new jet aircraft at the Dryden airport. To deice the aircraft would have required turning off the engines but once they were turned off there was no way to restart them (The F-28 aircraft had an auxiliary starting engine located in the tail to allow the aircraft to start its own jet engines using internal power. This engine was believed by the pilots to be unusable because certain sensors were not working. In fact, the auxiliary engine was operable). Bad weather at Dryden caused snow and ice to build up on the aircraft wings. The Dryden refueling was necessary because the airline management had required the pilots to remove fuel before taking off on from Thunder Bay, Ontario for the trip to Winnipeg. The pilot had wanted to leave passengers behind in Thunder Bay to avoid the need to refuel but management had ordered him to remove fuel instead, creating the need for refueling in Dryden (The situation was even more complex than indicated here and involves weather at expected and alternate airports, the certification of the pilot for operation of the Fokker, and detailed characteristics of the aircraft. The takeoff of Flight 1363 from Dryden was further delayed when a single engine airplane's urgently requested use of the one runway in order to land because the snow was making visibility worse. Ultimately, over thirty contributing factors were identified, including characteristics of the deregulation of commercial aviation in Canada, management deficiencies in the airline company, and lack of maintenance and operational equipment.

No single one of these problems was sufficient in itself to cause a crash. Only in combination could these multiple latent conditions create the conditions needed for the crash. In hindsight, there were plenty of opportunities to prevent the accident. But the fact that the multiple flaws are necessary to create disaster has the paradoxical effect of making each individual flaw seem insignificant. Seen in isolation, no flaw appears dangerous. As a result, many such flaws may accumulate within a system without raising alarm. When they do they present the operators with a situation that teeters on the very edge of catastrophe. This was the situation in the case of Flight 1363.

The pilots were not so much the instigators of the accident as the recipients of it. Circumstances had combined (some would say conspired) to create a situation that was rife with pressures, uncertainty, and risk. The pilots were invited to manage their way out of the situation but were offered no attractive opportunities to do so. Rather than being a choice between several good alternatives, the system produced a situation where the pilots were forced to choose between bad alternatives under conditions of uncertainty. They made an effort to craft a safe solution but were obstructed by managers who insisted that they achieve production goals.

Unlike many post-accident inquiries, the investigation of the crash of Flight 1393 was detailed and broad enough to show how the situation confronting the pilots had arisen. It provided a fine-grain picture of the kinds of pressures and difficulties that operators at the sharp end of practice confront in daily work. It showed how the decisions and actions throughout the aviation system had brought these pressures and difficulties together in the moments before the crash. This is now recognized as a "systems view" of the accident. It is a picture of the system that shows, in detail, how the technical characteristics of the workplace, the technical work that takes place there, and the pressures and difficulties that the workers experience combine to create the situation that produced the accident. Rather than attributing the accident to a discrete cause or causes, the investigation works towards providing a detailed account of the interactions between the factors that created the situation. In itself, the latent failure model could not capture all this, but it has been a very important contribution to making many more stakeholders think more critically about the rich context that surrounds and helps produce accidents.

Latent failures, "human error" and resilience

The latent failure model has helped redirect the focus away from front-line operators and towards the upstream conditions that influenced and constrained work. As Reason put it in 1990:

> "Rather than being the main instigators of an accident, operators tend to be the inheritors of system defects created by poor design, incorrect installation, faulty maintenance and bad management decisions. Their part is usually that of adding the final garnish to a lethal brew whose ingredients have already been long in the cooking." (p. 173)

According to the latent failure model, we should think of accident potential in terms of organizational processes, task and environmental conditions, individual unsafe acts, and failed defenses (see Figure 2.). A safety-critical system is surrounded by defenses-in-depth (as depicted by the various layers between hazards and the object or process to be protected in the figure). Defenses are measures or mechanisms that protect against hazards or lessen the consequences of malfunctions or erroneous actions. Some examples include safety systems or forcing functions such as interlocks. According to Reason (1990), the "best chance of minimizing accidents is by identifying and correcting these delayed action failures (latent failures) before they combine with local triggers to breach or circumvent the system's defenses." This is consistent with original 1960's ideas about barriers and the containment of unwanted energy release: It is best to stay as close to the source as possible, rather than trying to stop a concatenation downstream (Hollnagel, 2004; Rosness et al., 2005).

None of these layers are perfect, however, and the "holes" in them represent those imperfections. The organizational layer, for example, involves such processes as goal setting, organizing, communicating, managing, designing, building, operating, and maintaining. All of these processes are fallible, and produce the latent failures that reside in the system. This is not normally a problem, but when combined with other factors, they can contribute to an accident sequence. Indeed, according to the latent failure model, accidents happen when all of the layers are penetrated (when all their imperfections or "holes" line up). Incidents, in contrast, happen when the accident progression is stopped by a layer of defense somewhere along the way. This idea is carried over from the earlier sequence-of-events model, as is the linear depiction of a failure progression. Again, the latent failure model implicitly sustains the notion that an accident involves the unwanted or uncontrolled release of energy, which needs to be contained by several linearly stacked layers of defense.

Case: Eastern Airlines L1011 from Miami to Nassau, May 1983.

The aircraft lost oil pressure in all three of its engines in mid-flight. Two of the engines stopped, and the third gave out at about the time the crew safely landed the aircraft. The proximal event was that O-rings, which normally should be attached to an engine part, were missing from all three engines (It is interesting to note that from the perspective of the pilot, it seemed impossible that all three should go out at once. There must have been a common mode failure -- but what was it? The only thing they could think of was that it must be an electrical system problem. In actuality, it was a common mode failure, though a different one than they hypothesized). A synopsis of relevant events leading up to the incident is given below, based on the National Transportation Safety Board report (NTSB, 1984) and on Norman's commentary on this incident (Norman, 1992).

One of the tasks of mechanics is to replace an engine part, called a master chip detector, at scheduled intervals. The master chip detector fits into the engine and is used to detect engine wear. O-rings are used to prevent oil leakage when the part is inserted. The two mechanics for the flight in question had always gotten replacement master chip detectors from their foreman's cabinet. These chip detectors were all ready to go, with new O-rings installed. The mechanics' work cards specified that new O-rings should be installed with a space next to this instruction for their initials when the task was completed. However, their usual work situation meant that this step was unnecessary, because someone else (apparently their supervisor) was already installing new O-rings on the chip detectors.

The night before the incident, an unusual event occurred. When the mechanics were ready to replace master chip detectors, they found there were no chip detectors in the foreman's cabinet. The mechanics had to get the parts from the stockroom. The chip detectors were wrapped in a "semi-transparent sealed plastic package with a serviceable parts tag." The mechanics took the packages to the aircraft and replaced the detectors in low light conditions. It turned out the chip detectors did not have O-rings attached. The mechanics had not checked for them, before installing them. There was a check procedure against improper seals: motoring the engines to see if oil leaked. The technicians did this, but apparently not for a long enough time to detect oil leaks.

One might argue that the technicians should have checked the O-rings on the part, especially since they initialed this item on the work card. But consider that they did not strictly work from the work card—the work card said that they should install a new seal. But they never needed to; someone else always took care of this, so they simply checked off on it. Also, they could not work strictly from procedure; for example, the work card read "motor engine and check chip detector for leaks" but it didn't specify how long. The mechanics had to fill in the gap, and it turned out the time they routinely used was too short to detect leaks (a breakdown in the system for error detection).

Even without these particular technicians, the system held the potential for breakdown. Several problems or latent failures existed. The unusual event (having to get the part from supply) served as a trigger. (These latent failures are points where a difference might have prevented this particular incident.) Some of these were:

(a) The fact that someone other than the technicians normally put the O-rings on the chip detectors left in the cabinet and yet did not initial the workcard, effectively leaving no one in charge of O-ring verification (There would have been no place to initial since the task of using a new seal was a subtask of the larger step which included replacing the chip detector).
(b) The fact that the chip detectors from supply were not packed with O-rings.
(c) Personnel did not know what was a sufficient length of time to run the engines to see if their tasks had been carried out successfully.

Other factors that may have played a role include:

(a) Low lighting conditions and the necessity of working by feel when inserting the part made it unlikely that the lack of O-rings would have been detected without explicitly checking for them.
(b) Special training procedures concerning the importance of checking O-rings on the chip detectors were posted on bulletin boards and kept in a binder on the general foreman's desk. Theoretically, the foremen were supposed to ensure that their workers followed the guidance, but there was no follow-up to ensure that each mechanic had read these.
(c) The variation from a routine way of doing something (opening up the potential for slips of action).

The latent factors involved multiple people in different jobs and the procedures and conditions established for the tasks at the sharp end. Notice how easy it is to miss or rationalize the role of latent factors in the absence of outcome data. In this case, the airline had previous O-ring problems, but these were attributed to the mechanics. According to the NTSB report, the propulsion engineering director of the airline, after conferring with his counterparts, said that all the airlines were essentially using the same maintenance procedure but were not experiencing the same in-flight shutdown problems. Hence, it was concluded that the procedures used were valid, and that the problems in installation were due to personnel errors. Also, in reference to the eight incidents that occurred in which O-rings were defective or master chip detectors were improperly installed (prior to this case), the "FAA concluded that the individual mechanic and not Eastern Air Lines maintenance procedures was at fault" (National Transportation Safety Board, 1984).

As Norman (1992) points out, these are problems in the system. These latent failures are not easy to spot; one needs a systems view (i.e., view of the different levels and their interactions) as well as knowledge of how they hold the potential for error. Because of how difficult it is to see these, and how much easier it is to focus on the

individual and the actions or omissions that directly impacted the event, the tendency is to attribute the problem to the person at the sharp end. But behind the label "human error" is another story that points to many system-oriented deficiencies that made it possible for the faulty installation to occur and to go undetected.

The idea of latent failures has broadened the story of error. It has popularized the notion that is not enough to stop with the attribution that some individual at the sharp end erred. The concept of latent failures highlights the importance of organizational factors. It shows how practitioners at the sharp end can be constrained or trapped by larger factors. Even though it throws the net much wider, encompassing a larger number than factors than may have been usual, the latent failure model holds on to a broken-component explanation of accidents. The latent failures themselves are, or contribute to, (partially) broken layers of defense, for example. The model proposes that latent failures can include organizational deficiencies, inadequate communications, poor planning and scheduling, inadequate control and monitoring, design failures, unsuitable materials, poor procedures (both in operations and maintenance), deficient training, and inadequate maintenance management (Reason, 1993). The problem is that these are all different labels for "human error," even if they refer to other kinds of errors by other people inside or outside the organization. Explaining operator error by referring to errors by other people is the problem of recursion that dogs man-made disaster theory and the imperfect information processing notion of failure that it, in turn, is based on too (Rosness et al., 2005). Recursion makes that a "human error" is not really explained, but rather displaced.

The latent failure model also reserves a special place for violations. These, according to the model, are deviations from some code of practice or procedure. Stakeholders often hugely overestimate the role of such "violations" in their understanding of accidents ("if only operators followed the rules, then this would never have happened") and can presume that local adaptations to rules or other written guidance were unique to that situation, the people in it or the outcome it produced. This is not often the case: written guidance is always underspecified relative to the actual work-to-be-performed, as well as insensitive to many changes in context, so people always need to bridge the gaps by interpreting and adapting. To understand failure and success in safety-critical worlds where multiple goals compete for people's attention and resources are always limited, it may not be helpful to see adaptations in such a strong normative light, where the rule is presumed right and the violator wrong. "Violations" are but one way to characterize adaptation, a characterization that depends critically on an externally imposed norm against which the behavior is judged deficient or deviant.

The best chance of minimizing accidents is by learning how to detect and appreciate the significance of latent failures before they combine with other contributors to produce disaster (Reason, 1990). But this is where the depiction of a complex system as a static set of layers presents problems. It does not explain how such latent failures come into being, nor how they actually combine with active failures. Also, the model does not tell how layers of defense are gradually eroded, for example under the pressures of production and resource limitations and confidence based on successful past outcomes. It helps stakeholders focus on a larger set of deficient components, but the linear, componential approach limits analytical access to the complex interactions and cross-adaptations between the layers, components, and people inside and outside an organization. These, however, are responsible for the waxing and waning of defense layers, and the erosion of holes in them. While the latent failure model is able to portray the latent failures that contributed to an accident after-the-fact, it is a static model that helps stakeholders depict a resulting imperfect organizational form, but it does not help them understand or describe the processes of formation and erosion.

Complexity and resilience

Normal Accident Theory

Highly technological systems such as aviation, air traffic control, telecommunications, nuclear power, space missions, and medicine include potentially disastrous failure modes. These systems, consistent with the barrier idea in the previous part, usually have multiple redundant mechanisms, safety systems, and elaborate policies and procedures to keep them from failing in ways that produce bad outcomes. The results of combined operational and engineering measures make these systems relatively safe from single point failures; that is, they are protected against the failure of a single component or procedure directly leading to a bad outcome. But the paradox, says Perrow (1984), is that such barriers and redundancy can actually add complexity and increase opacity so that, when even small things start going wrong, it becomes exceptionally difficult to get off an accelerating pathway to system breakdown. The need to make these systems reliable, in other words, also makes them very complex. They are large systems, semantically complex (it generally takes a great deal of time to master the relevant domain knowledge), with tight couplings between various parts, and operations are often carried out under time pressure or other resource constraints.

Perrow (1984) promoted the idea of system accidents. Rather than being the result of a few or a number of component failures, accidents involve the unanticipated interaction of a multitude of events in a complex system—events and interactions whose combinatorial explosion can quickly outwit people's best efforts at predicting and mitigating disaster. The scale and coupling of these systems creates a different pattern for disaster where incidents develop or evolve through a conjunction of several small failures. Yet to Normal Accidents Theory, analytically speaking, such accidents need not be surprising at all (not even in a fundamental sense). The central thesis of what has become known as normal accident theory (Perrow, 1984) is that accidents are the structural and virtually inevitable product of systems that are both interactively complex and tightly coupled. Interactive complexity and coupling are two presumably different dimensions along which Perrow plotted a number of systems (from manufacturing to military operations to nuclear power plants). This separation into two dimensions has spawned a lot of thinking and discussion (including whether they are separable at all), and has offered new ways of looking at how to manage and control complex, dynamic technologies, as well as suggesting what may lie behind the label "human error" if things go wrong in a tightly coupled, interactively complex system. Normal accident theory predicts that the more tightly coupled and complex a system is, the more prone it is to suffering a "normal" accident.

Interactive complexity refers to component interactions that are non-linear, unfamiliar, unexpected or unplanned, and either not visible or not immediately comprehensible for people running the system. Linear interactions are those in expected and familiar production or maintenance sequences, and those that are quite visible and understandable even if unplanned. Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible (Perrow, 1984). An electrical power grid is an example of an interactively complex system. Failures, when they do occur, can cascade through these systems in ways that may confound the people managing them, making it difficult to stop the progression of failure. Table 2 shows the contrast between linear and complex systems.

Complex systems	Linear systems
Tight spacing of equipment	Equipment spread out
Proximate production steps	Segregated production steps
Many common-mode connections of components not in production sequence	Common-mode connections limited to power supply and environment
Limited isolation of failed components	Easy isolation of failed components
Personnel specialization limits awareness of dependencies	Less personnel specialization
Limited substitution of supplies and materials	Extensive substitution of supplies and materials
Unfamiliar and unintended feedback loops	Few unfamiliar and unintended feedback loops
Many control parameters with potential interactions	Control parameters few, direct, segregated
Indirect or inferential information sources	Direct, on-line information sources
Limited understanding of some processes	Extensive understanding of all processes

Table 2: Complex versus linear systems (from Perrow, 1984).

In addition to being either linearly or complexly interactive, systems can be loosely or tightly coupled. They are tightly coupled if they have more time-dependent processes (meaning they can't wait or stand by until attended to), sequences that are invariant (the order of the process cannot be changed) and little slack (e.g. things cannot be done twice to get it right). Dams, for instance, are rather linear systems, but very tightly coupled. Rail transport is too. In contrast, an example of a system that is interactively complex but not very tightly coupled is a university education. It is interactively complex because of specialization, limited understanding, number of control parameters and so forth. But the coupling is not very tight. Delays or temporary halts in education are possible, different courses can often be substituted for one another (as can a choice of instructors), and there are many ways to achieving the goal of getting a degree.

Tight coupling	Loose coupling
Delays in processing not possible	Processing delays possible
Invariant sequences	Order of sequences can be changed
Only one method to achieving goal	Alternative methods available
Little slack possible in supplies, equipment or personnel	Slack and substitution in resources possible
Buffers and redundancies exist but are limited to what has been deliberately designed in	Buffers and redundancies available

Table 3. Tight versus loose coupling tendencies (from Perrow, 1984)

Case: A coffee maker onboard a DC-8 airliner

During a severe winter in the US (1981-1982), a DC-8 airliner was delayed at Kennedy airport in New York (where the temperature was a freezing 2°F or minus 17°C) because mechanics needed to exchange a fuel pump (they received frost bite, which caused further delay) (Perrow, 1984, p. 135)

After the aircraft finally got airborne after midnight, headed for San Francisco, passengers were told that there would be no coffee because the drinking water was frozen. Then the flight engineer discovered that he could not control the cabin pressure (which is held at a higher pressure than the thin air the aircraft is flying in so as to make the air breathable). Later investigation showed that the frozen drinking water had cracked the airplane's water tank. Heat from ducts to the tail section of the aircraft then melted the ice in the tank, and because of the crack in the tank, and the pressure in it, the newly melted water near the heat source sprayed out. It landed on the outflow valve that controls the cabin pressurization system (by allowing pressurized cabin air to vent outside). Once on the valve, the water turned to ice again because of the temperature of the outside air (minus 50°F or minus 45°C), which caused the valve to leak. The compressors for the cabin air could not keep up, leading to depressurization of the aircraft.

The close proximity of parts that have no functional relationship, packed inside a compact airliner fuselage, can create the kind of interactive complexity and tight coupling that makes it hard to understand and control a propagating failure. Substituting broken parts was not possible (meaning tight coupling): the outflow valve is not reachable when airborne and a water tank cannot be easily replaced either (nor can a leak in it be easily fixed when airborne). The crew response to the pressurization problem, however, was rapid and effective—independent of their lack of understanding of the source of their pressurization problem. As trained, they got the airplane down to a breathable level in just three minutes and diverted to Denver for an uneventful landing there.

To Perrow, the two dimensions (interactive complexity and coupling) presented a serious dilemma. A system with high interactive complexity can only be effectively controlled by a decentralized organization. The reason is that highly interactive systems generate the sorts of non-routine situations that resist standardization (e.g. through procedures, which is a form of centralized control fed forward into the operation). Instead, the organization has to allow lower-level personnel considerable discretion and leeway to act as they see fit based on the situation, as well as encouraging direct interaction among lower-level personnel, so as to bring together the different kinds of expertise and perspective necessary to understand the problem.

A system with tight couplings, on the other hand, can in principle only be effectively controlled by a highly centralized organization, because tight coupling demands quick and coordinated responses. Disturbances that cascade through a system cannot be stopped quickly if a team with the right mix of expertise and backgrounds needs to be assembled first. Centralization, for example through procedures, emergency drills, or even automatic shut-downs or other machine interventions, is necessary to arrest such cascades quickly. Also, a conflict between different well-meaning interventions can make the situation worse, which means that activities oriented at arresting the failure propagation need to be extremely tightly coordinated.

To Perrow, an organization cannot be centralized and decentralized at the same time. So a dilemma arises if a system is both interactively complex and tightly coupled (e.g. nuclear power generation). A necessary conclusion for normal accidents theory is that systems that are both tightly coupled and interactively complex can therefore not be controlled effectively. This, however, is not the whole story. In the tightly coupled and interactively complex pressurization case above, the crew may not have been able to diagnose the source of the failure (which would indeed have involved decentralized multiple different perspectives, as well as access to various systems and components). Yet through centralization (procedures for dealing with pressurization problems are often trained, well-documented, brief and to the point) and extremely tight

coordination (who does and says what in an emergency depressurization descent is very firmly controlled and goes unquestioned during execution of the task), the crew was able to stop the failure from propagating into a real disaster. Similarly, even if nuclear power plants are both interactively complex and tightly coupled, a mix of centralization and decentralization is applied so as to make propagating problems more manageable (e.g. thousands of pages of procedures and standard protocols exist, but so does the co-location of different kinds of expertise in one control room, to allow spontaneous interaction; and automatic shut-down sequences that get triggered in some situations can rule out the need for human intervention for up to thirty minutes).

Normal accident theory, "human error" and resilience

At the sharp end of complex systems, normal accidents theory sees human error as a label for some of the effects of interactive complexity and tight coupling. Operators are the inheritors of a system that structurally conspires against their ability to make sense of what is going on and to recover from a developing failure. Investigations, infused with the wisdom of hindsight, says Perrow (1984) often turn up places where human operators should have zigged instead of zagged, as if that alone would have prevented the accident. Perrow invokes the idea of the fundamental surprise error when he comments on official inability to deal with the real structural nature of failure (e.g. through the investigations that are commissioned). The cause they find may sometimes be no more than the "cause" people are willing or able to afford. Indeed, to Perrow, the reliance on labels like "human error" has little to do with explanation and more with politics and power, something even formal or independent investigations are not always immune to:

> "Formal accident investigations usually start with an assumption that the operator must have failed, and if this attribution can be made, that is the end of serious inquiry. Finding that faulty designs were responsible would entail enormous shutdown and retrofitting costs; finding that management was responsible would threaten those in charge, but finding that operators were responsible preserves the system, with some soporific injunctions about better training." (1984, p. 146)

Human error, in other words, can be a convenient and cheap label to use so as to control sunk costs and avoid having to upset elite interests. Behind the label, however, lie the real culprits: structural interactive complexity and tight coupling—features of risky technological systems such as nuclear power generation that society as a whole should be thinking critically about (Perrow, 1984).

That said, humans can hardly be the recipient victims of complexity and coupling alone—that indeed would be a foreign idea to anything resilient. The very definition of Perrowian complexity actually involves both human and system, to the point where it becomes hard to see where one ends and the other begins. For example, interactions cannot be unfamiliar, unexpected, unplanned, or not immediately comprehensible in some system independent of the people who need to deal with them (and to whom they are either comprehensible or not). One hallmark of expertise, after all, is a reduction of the degrees of freedom that a decision presents to the problem-solver (Jagacinski and Flach, 2002), and an increasingly refined ability to recognize patterns of interactions and knowing what to do primed by such situational appreciation (Klein, Orasanu & Calderwood, 1993). Perrowian complexity can thus not be a feature of a system by itself, but always has to be understood in relation to the people (and their expertise) who have to manage that system (e.g., Pew et al., 1981). This also means that the categories of complexity and coupling are not as independent as normal accident theory suggests.

Another problem arises when complexity and coupling are treated as stable properties of a system, because it misses the dynamic nature of much safety-critical work and the ebb and flow of cognitive and coordinative activity to manage it. During periods of crisis, or high demand, a system can become more difficult to control as couplings tighten and interactive complexity momentarily deepens. It renders otherwise visible interactions less transparent, less linear, creating interdependencies that are harder to understand and more difficult to correct. This can become especially problematic when important routines get interrupted, coordinated action breaks down and misunderstandings occur (Weick, 1990). The opposite goes too. Contractions in complexity and coupling can be met in centralized and de-centralized ways by people responsible for the safe operation of the system, creating new kinds of coordinated action and newly invented routines.

Case: The MAR knockout case

During the Friday night shift in a large, tertiary care hospital, a nurse called the pharmacy technician on duty to report a problem with the medications just delivered for a ward patient in the unit dose cart. The call itself was not usual; occasionally there would be a problem with the medication delivered to the floor, especially if a new order was made after the unit dose fill list had been printed. In this case, however, the pharmacy had delivered medicines to the floor that had never been ordered for that patient. More importantly, the medicines that were delivered to the floor matched with the newly printed medication administration record (MAR). This was discovered during routine reconciliation of the previous day's MAR with the new one. The MAR that had just been delivered was substantially different than the one from the previous day but there was no indication in the patient's chart that these changes had been ordered. The pharmacy technician called up a computer screen that showed the patient's medication list. This list corresponded precisely to the new MAR and the medications that had been delivered to the ward.

While trying to understand what had happened to this patient's medication, the telephone rang again. It was a call from another ward where the nurses had discovered something wrong. For some patients, the unit dose cart contained drugs their patients were not taking, in others the cart did not contain drugs the patients were supposed to get. Other calls came in from other areas in the hospital, all describing the same situation. The problem seemed to be limited to the unit dose cart system; the intravenous medications were correct. In each case, the drugs that were delivered matched the newly printed MAR, but the MAR itself was wrong. The pharmacy technician notified the on-call pharmacist who realized that, whatever its source, the problem was hospital-wide. The MAR as a common mode created the kind of Perrowian complexity that made management of the problem extremely difficult: its consequences were showing up throughout the entire hospital, often in different guises and with different implications.

Consistent with normal accident theory, a technology that was introduced to improve safety, such as the dose checking software in this case, actually made it harder to achieve safety, for example, by making it difficult to upgrade to new software. Information technology makes it possible to perform work efficiently by speeding up much of the process. But the technology also makes it difficult to detect failures and recover from them. It introduces new forms of failure that are hard to appreciate before they occur. These failures are foreseeable but not foreseen. This was an event with system-wide consequences required decisive and immediate action to limit damage and potential damage. This action was expensive and potentially damaging to the prestige and authority of those who were in charge. The effective response required simultaneous, coordinated activity by experienced, skilled people.

Like many accidents, it was not immediately clear what had happened, only that something was wrong. It was now early Saturday morning and the pharmacy was confronting a crisis. First, the pharmacy computer system was somehow generating an inaccurate fill list. Neither MARs nor the unit dose carts already delivered to the wards could be trusted. There was no pharmacy computer generated fill list that could be relied upon. Second, the wards

were now without the right medications for the hospitalized patients and the morning medication administration process was about to begin. No one yet knew what was wrong with the pharmacy computer. Until it could be fixed, some sort of manual system was needed to provide the correct medications to the wards. Across the hospital, the unit dose carts were sent back to the pharmacy.

A senior pharmacist realized that the previous day's hard copy MARs as they were maintained on the wards were the most reliable available information about what medicines patients were supposed to receive. By copying the most recent MARs, the pharmacy could produce a manual fill list for each patient. For security reasons, there were no copying machines near the wards. There was a fax machine for each ward, however, and the pharmacy staff organized a ward-by-ward fax process to get hand updated copies of each patient's MAR. Technicians used these faxes as manual fill lists to stock unit dose carts with correct medications. A decentralized response, in other words, that coordinated different kinds of expertise and background, making fortuitous use of substitutions (fax machines instead of copiers) helped people in the hospital manage the problem. A sudden contraction in interactive complexity through a common mode failure (MAR in this case) with a lack of centralized response capabilities (no central back-up) did not lead to total system breakdown because of the spontaneously organized response of practitioners throughout the system.

Ordinarily, MARs provided a way to track and reconcile the physician orders and medication administration process on the wards. In this instance they became the source of information about what medications were needed. Because the hospital did not yet have computer-based physician order entry, copies of handwritten physician orders were available. These allowed the satellite pharmacies to interact directly with the ward nurses to fill the gaps. Among the interesting features of the event was the absence of typewriters in the pharmacy. Typewriters, discarded years before in favor of computer label printers, would have been useful for labeling medications. New technology displaces old technology, making it harder to recover from computer failures by reverting to manual operations.

The source of the failure remained unclear, as it often does, but that does not need to hamper the effectiveness of the coordinated response to it. There had been some problem with the pharmacy computer system during the previous evening. The pharmacy software detected a fault in the database integrity. The computer specialist had contacted the pharmacy software vendor and they had worked together through a fix to the problem. This fix proved unsuccessful so they reloaded a portion of the database from the most recent backup tape. After this reload, the system had appeared to work perfectly. The computer software had been purchased from a major vendor. After a devastating cancer chemotherapy accident in the institution, the software had been modified to include special dose checking programs for chemotherapy. These modifications worked well but the pharmacy management had been slow to upgrade the main software package because it would require rewriting the dose checking add-ons. Elaborate backup procedures were in place, including both frequent "change" backups and daily "full" backups onto magnetic tapes.

Working with the software company throughout the morning, the computer technicians were able to discover the reason that the computer system had failed. The backup tape was incomplete. Reloading had internally corrupted the database The backup was corrupted because of a complex interlocking process related to the database management software that was used by the pharmacy application. Under particular circumstances, tape backups could be incomplete in ways that remained hidden from the operator). problem was not related to the fault for which the backup reloading was necessary. The immediate solution to the problem facing the pharmacy was to reload the last "full" backup (now over a day and a half old) and to re-enter all the orders made since that time. The many pharmacy technicians now collected all the handwritten order slips from the past 48 hours and began to enter these (The process was actually considerably more complex. For example, to bring the computer's view of the world up to date, its internal clock had to be set back , the prior day's fill list regenerated, the day's ordered entered, the clock time set forward and the current day's morning fill list re-run). The manual system was used all Saturday. The computer system was restored by the end of the day. The managers and technicians examined the fill lists produced for the nightly fill closely and found no errors. The system was back "on-line".

As far as pharmacy and nursing management could determine, no medication misadministration occurred during this event. Some doses were delayed, although no serious consequences were identified. Several factors contributed to the hospital's ability to recover from the event. First, the accident occurred on a Friday night so that the staff had all day Saturday to recover and all day Sunday to observe the restored system for new failures. Few new patients are admitted on Saturday and the relatively slow tempo of operations allowed the staff to concentrate on recovering the system. Tight coupling, in other words, was averted fortuitously by the time of the week of the incident. Second, the hospital had a large staff of technicians and pharmacists who came in to restore operations. In addition, the close relationship between the software vendor and hospital information technical staff made it possible for the staff to diagnose the problem and devise a fix with little delay. The ability to quickly bring a large number of experts with operational experience together was critical to success, as normal accidents theory predicts is necessary in highly interactively complex situations. Third, the availability of the manual, paper records allowed these experts to "patch-up" the system and make it work in an unconventional but effective way. The paper MARs served as the basis for new fill lists and the paper copies of physician orders provided a "paper trail" that made it possible to replay the previous day's data entry, essentially fast forwarding the computer until it's "view" of the world was correct. Substitution of parts, in other words, was possible, thereby reducing coupling and arresting a cascade of failures. Fourth, the computer system and technical processes contributed. The backup process, while flawed in some ways, was essential to recovery: it provided the "full" backup needed. In other words, a redundancy existed that had not been deliberately designed-in (as is normally the case in tightly coupled systems according to normal accident theory).

The ability of organizations to protect themselves against system accidents (such as the MAR knockout came close to being) can, in worse cases than the one described above, fall victim to the very interactive complexity and tight coupling it must contain. Plans for emergencies, for example, are intended to help the organization deal with unexpected problems and developments for which are designed to be maximally persuasive to regulators, board members, surrounding communities, lawmakers and opponents of the technology, and as a result can become wildly unrealistic. Clarke and Perrow (1996) call them "fantasy documents," that fail to cover most possible accidents, lack any historical record that may function as a reality check, and are quickly based on obsolete contact details, organizational designs, function descriptions and divisions of responsibility. The problem with such fantasy documents is that they can function as an apparently legitimate placeholder that suggests that everything is under control. It inhibits the organization's commitment to continually reviewing and re-assessing its ability to deal with hazard. In other words, fantasy documents can impede organizational learning as well as organizational preparedness.

Control theory: Sketching the outlines of resilience

Accident models based on control theory explicitly look at accidents as emerging from interactions among system components. They usually do not identify single causal factors, but rather look at what may have gone wrong with the system's operation or organization of the hazardous technology that allowed an accident to take place. Safety, or risk management, is viewed as a control problem (Rasmussen, 1997), and accidents happen when component failures, external disruptions or interactions between layers and components are not adequately handled; when safety constraints that should have applied to the design and operation of the technology have loosened, or become badly monitored, managed, controlled. Control theory tries to capture these imperfect processes, which involve that include people, societal and organizational structures, engineering activities, and physical parts. It sees the complex interactions between those—as did man-made disaster theory—as eventually resulting in an accident (Leveson, 2002).

Control theory sees the operation of hazardous technology as a matter of keeping many interrelated components in a state of dynamic equilibrium (which means that control inputs, even if small, are continually necessary for the system to stay safe: it cannot be left on its own as could a statically stable system). This is an essential basis for resilience thinking. Keeping a dynamically stable system in equilibrium happens through the use of feedback loops of information and control that stem not only from the system's own behavior and evolution but also very much from its interaction with its changing environment. Accidents are not the result of an initiating (root cause) event that triggers a series of events, which eventually leads to a loss. Instead, accidents result from interactions among components that violate the safety constraints on system design and operation, by which feedback and control inputs can grow increasingly at odds with the real problem or processes to be controlled. Unsurprisingly, concern with those control processes (how they evolve, adapt and erode) forms the heart of control theory as applied to organizational safety, and is highly important for resilience as well (Rasmussen, 1997; Leveson, 2002).

Degradation of the safety-control structure over time can be due to asynchronous evolution, where one part of a system changes without the related necessary changes in other parts. Changes to subsystems may have been carefully planned and executed in isolation, but consideration of their effects on other parts of the system, including the role they play in overall safety control, may remain neglected or inadequate. Asynchronous evolution can occur too when one part of a properly designed system deteriorates independent of other parts. In both cases, erroneous expectations of users or system components about the behavior of the changed or degraded subsystem may lead to accidents (Leveson, 2002). The more complex a system (and, by extension, the more complex its control structure), the more difficult it can become to map out the reverberations of changes (even carefully considered ones) throughout the rest of the system. Control theory embraces a much more complex idea of causation, taken from complexity (or chaos) theory. Small changes somewhere in the system, or small variations in the initial state of a process, can lead to huge consequences elsewhere. The Newtonian symmetry between cause and effect (still assumed in other models discussed in this part) no longer applies.

Case: The Lexington Comair 5191 accident (see Nelson, 2008)

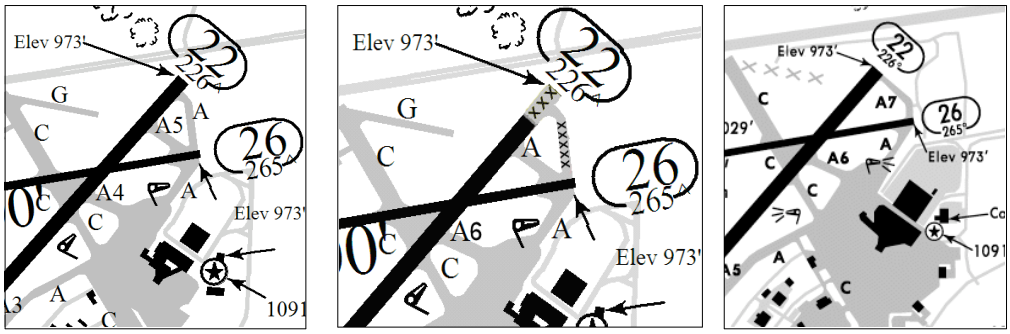
Flight 5191 was a scheduled passenger flight from Lexington, Kentucky to Atlanta, Georgia, operated by Comair. On the morning of August 27, 2006, the Regional Jet that was being used for the flight crashed while attempting to take off. The aircraft was assigned runway 22 for the takeoff, but used runway 26 instead. Runway 26 was too short for a safe takeoff. The aircraft crashed just past the end of the runway, killing all 47 passengers and two of the three crew. The flight's first officer was the only survivor. At the time of the 5191 accident the LEX airport was in the final construction phases of a five year project. The First Officer had given the takeoff briefing and mentioned that "lights were out all over the place" (NTSB, 2007, p. 140) when he had flown in two nights before. He also gave the taxi briefing, indicating they would take taxiway Alpha to runway 22 and that it would be a short taxi. Unbeknownst to the crew, the airport signage was inconsistent with their airport diagram charts as a result of the construction. Various taxiway and runway lighting systems were out of operation at the time.

After a short taxi from the gate, the captain brought the aircraft to a stop short of runway 22, except, unbeknownst to him, they were actually short of runway 26. The control tower controller scanned runway 22 to assure there was no conflicting traffic, then cleared Comair 191 to take off. The view down runway 26 provided the illusion of some runway lights. By the time they approached the intersection of the two runways, the illusion was gone and the only light illuminating the runway was from the aircraft lights. This prompted the First Officer to comment "weird with no lights" and the captain responded "yeah" (NTSB, 2007, p. 157). During the next 14 seconds, they traveled the last 2500 ft of remaining runway. In the last one hundred feet of runway, the captain

called "V1, Rotate, Whoa." The jet became momentarily airborne but then impacted a line of oak trees approximately 900 feet beyond the end of runway 26. From there, the aircraft erupted into flames and came to rest approximately 1900 feet off the west end of runway 26.

Runway 26 was only 3500 feet long and not intended for aircraft heavier than 12,000 pounds. Yet each runway had a crossing runway located approximately 1500 feet from threshold. They both had an increase in elevation at the crossing runway. The opposite end of neither runway was visible during the commencement of the takeoff roll. Each runway had a dark-hole appearance at the end, and both had 150 foot wide pavement (runway 26 was edge striped to 75 feet). Neither runway had lighting down the center line, as that of runway 22 had been switched off as part of the construction (which the crew knew). Comair had no specified procedures to confirm compass heading with the runway. Modern Directional Gyros (DG) automatically compensate for precession, so it is no longer necessary to cross-check the DG with runway heading and compass indication. Many crews have abandoned the habit of checking this, as airlines have abandoned procedures for it. The 5191 crew was also fatigued, having accumulated sleep loss over the preceding duty period.

Comair had operated accident-free for almost 10 years when the 5191 accident occurred. During those 10 years, Comair approximately doubled its size, was purchased by Delta Air Lines Inc., became an all jet operator and, at the time of the 5191 accident, was in the midst of its first bankruptcy reorganization. As is typical with all bankruptcies, anything management believed was unnecessary was eliminated, and everything else was pushed to maximum utilization. In the weeks immediately preceding the 5191 accident, Comair had demanded large wage concessions from the pilots. Management had also indicated the possibility of furloughs and threatened to reduce the number of aircraft, thereby reducing the available flight hours and implying reduction of work force.



Crew's chart | Accurate Chart depiction | NFDC data chart

Figure 3. The difference between the crew's chart on the morning of the accident, the actual situation (center) and the eventual result of the reconstruction (NFDC or National Flight Data Center chart to the right). From Nelson, 2008.

Data provided by Jeppesen, a major flight navigation and chart company. for NOTAM's (Notices to Airmen), did not contain accurate local information about the closure of taxiway Alpha North of runway 26. Comair, nor the crew, had any other way to get this information other than a radio broadcast at the airport itself, but there was no system in place for checking the completeness and accuracy of these either. According to the airport, the last phase of construction did not require a change in the route used to access runway 22; Taxiway A5 was simply renamed Taxiway A, but this change was not reflected on the crew's chart (indeed, asynchronous evolution). It would eventually become Taxiway A7.

Several crews had acknowledged difficulty dealing with the confusing aspects of the north end taxi operations to runway 22, following the changes which affected a seven day period prior to the 5191 accident. One captain, who flew in and out of LEX numerous times a month, stated that after the changes "there was not any clarification

about the split between old alpha taxiway and the new alpha taxiway and it was confusing." A First Officer, who also regularly flew in and out of LEX, expressed that on their first taxi after the above changes, he and his captain "were totally surprised that taxiway Alpha was closed between runway 26 and runway 22." The week before, he used taxiway Alpha (old Alpha) to taxi all the way to runway 22. It "was an extremely tight area around runway 26 and runway 22 and the chart did not do it justice." Even though these and, undoubtedly, other instances of crew confusion occurred during the seven day period of August 20-27, 2006, there were no effective communication channels to provide this information to LEX, or anyone else in the system. After the 5191 accident, a small group of aircraft maintenance workers expressed concern that they, too, had experienced confusion when taxiing to conduct engine run-up's. They were worried that an accident could happen, but did not know how to effectively notify people who could make a difference.

The regulator had not approved the publishing of interim airport charts that would have revealed the true nature of the situation. It had concluded that changing the chart over multiple revision cycles would create a high propensity for inaccuracies to occur, and that, because of the multiple chart changes, the possibilities for pilot confusion would be magnified.

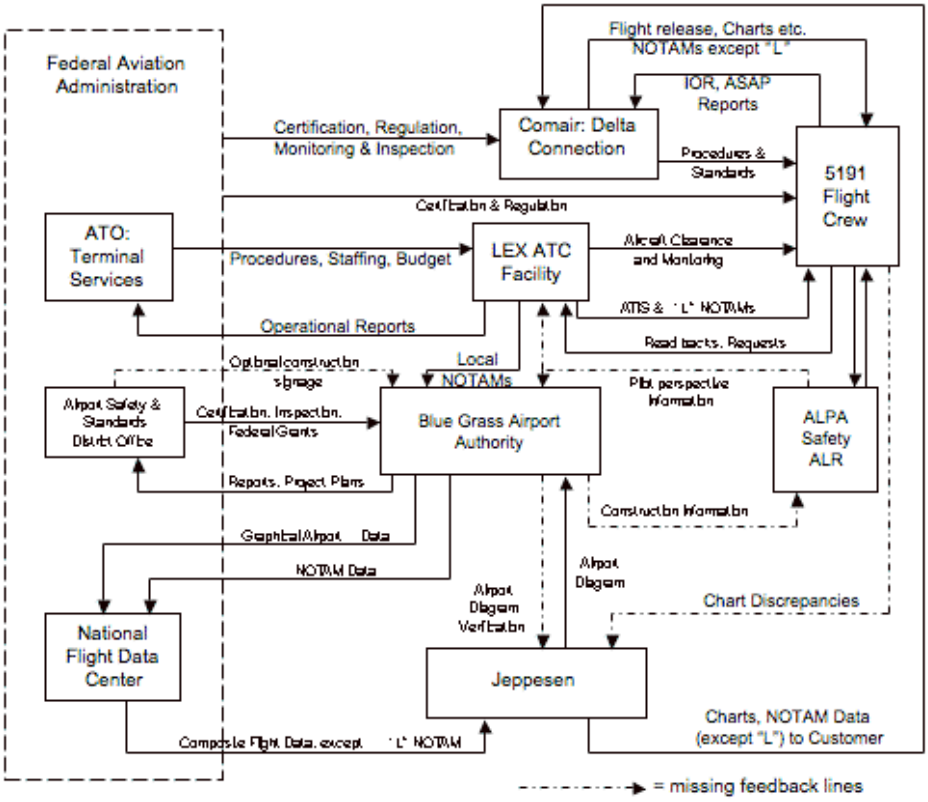


Figure 4. The structure responsible for safety-control during airport construction at Lexington, and how it had become eroded. Lines going into the left of a box represent control actions, lines from the top or bottom represent feedback.

Control theory has part of its background in control engineering, which helps the design of control and safety systems in hazardous industrial or other processes, particularly with software applications (e.g. Leveson & Turner, 1993). The models, as applied to organizational safety, are concerned with how a lack of control allows a migration of organizational activities towards the boundary of acceptable performance, and there are several ways to represent the mechanisms by

which this occurs. Systems dynamics modeling does not see an organization as a static design of components or layers. It readily accepts that a system is more than the sum of its constituent elements. Instead, they see an organization as a set of constantly changing and adaptive processes focused on achieving the organization's multiple goals and adapting around its multiple constraints. The relevant units of analysis in control theory are therefore not components or their breakage (e.g. holes in layers of defense), but system constraints and objectives (Rasmussen, 1997; Leveson, 2002):

Human behavior in any work system is shaped by objectives and constraints which must be respected by the actors for work performance to be successful. Aiming at such productive targets, however, many degrees of freedom are left open which will have to be closed by the individual actor by an adaptive search guided by process criteria such as workload, cost effectiveness, risk of failure, joy of exploration, etc. The work space within which the human actors can navigate freely during this search is bounded by administrative, functional and safety-related constraints. The normal changes found in local work conditions lead to frequent modifications of strategies and activity will show great variability… During the adaptive search the actors have ample opportunity to identify 'an effort gradient' and management will normally supply an effective 'cost gradient'. The result will very likely be a systematic migration toward the boundary of functionally acceptable performance and, if crossing the boundary is irreversible, an error or an accident may occur (Rasmussen, 1997, p. 189).

The dynamic interplay between these different constraints and objectives is illustrated in figure 5.

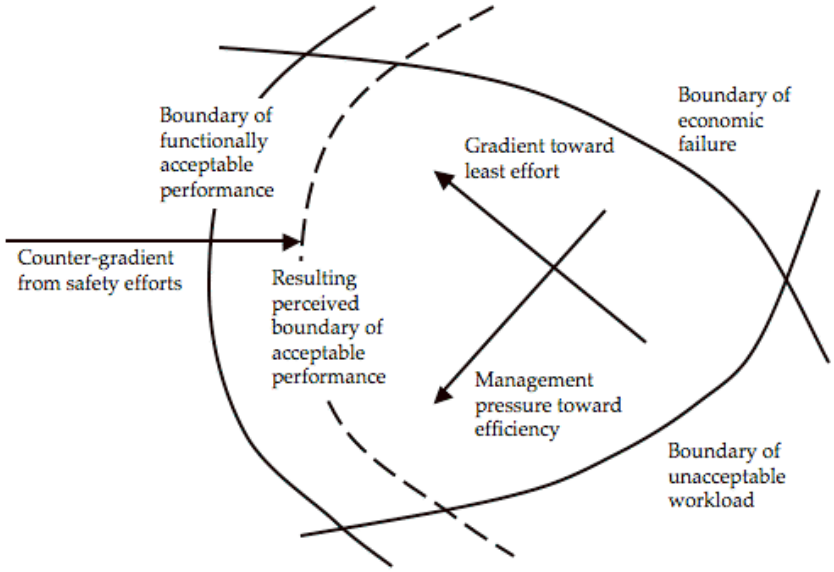


Figure 5. A space of possible organizational action is bounded by three constraints: safety, workload and economics. Multiple pressures act to move the operating point of the organization in different directions (after Rasmussen, 1997)

Control theory sees accidents as the result of normal system behavior, as organizations try to adapt to the multiple, normal pressures that operate on it every day. Reserving a place for "inadequate" control actions, as some models do, of course does re-introduce human error under a new label (accidents are not the result of human error, but the result of inadequate control—what exactly is the difference then?). Systems dynamics modeling must deal with that problem by recursively modeling the constraints and objectives that govern the control actions at various

hierarchical levels, thereby explaining the "inadequacy" as a normal result of normal pressures and constraints operating on that level from above and below, and in turn influencing the objectives and constraints for other levels. Rasmussen (1997) does this by depicting control of a hazardous technology as a nested series of reciprocally constraining hierarchical levels, down from the political and governmental level, through regulators, companies, management, staff, all the way to sharp-end workers. This nested control structure is also acknowledged by Leveson, 2002).

In general, systems dynamics modeling is not concerned with individual unsafe acts or errors, or even individual events that may have helped trigger an accident sequence. Systems dynamics modeling also rejects the depiction of accidents in the traditionally physical way as the latent failure model does, for example. Accidents are not about particles, paths of traveling or events of collision between hazard and process-to-be-protected (Rasmussen, 1997). The reason for rejecting such language (even visually) is that removing individual unsafe acts, errors or singular events from a presumed or actual accident sequence only creates more space for new ones to appear if the same kinds of systemic constraints and objectives are left similarly ill-controlled in the future. The focus of control theory is therefore not on erroneous actions or violations, but on the mechanisms that help generate such behaviors at a higher level of functional abstraction—mechanisms that turn these behaviors into normal, acceptable and even indispensable aspects of an actual, dynamic, daily work context.

Fighting violations or other deviations from presumed ways of operating safely—as implicitly encouraged by other models discussed above—is not very useful according to control theory. A much more effective strategy for controlling behavior is by making the boundaries of system performance explicit and known, and to help people develop skills at coping with the edges of those boundaries. Ways proposed by Rasmussen (1997) include increasing the margin from normal operation to the loss-of-control boundary. This, however, is only partially effective because of risk homeostasis—the tendency for a system to gravitate back to a certain level of risk acceptance, even after interventions to make it safer. In other words, if the boundary of safe operations is moved further away, then normal operations will likely follow not long after—under pressure, as they always are, from the objectives of efficiency and less effort.

Case: Risk homeostasis

One example of risk homeostasis is the introduction of anti-lock brakes and center-mounted brake lights on cars. Both these interventions serve to push the boundary of safe operations further out, enlarging the space in which driving can be done safely (by notifying drivers better when a preceding vehicle brakes, and by improving the vehicle's own braking performance independent of road conditions). However, this gain is eaten up by the other pressures that push on the operating point: drivers will compensate by closing the distance between them and the car in front (after all, they can see better when it brakes now, and their own braking performance has improved). The distance between the operating point and the boundary of safe operations is once again the same because of risk homeostasis.

Another way is to increase people's awareness that the system may be drifting towards the boundary, and then launching safety campaign to push back in the opposite direction (Rasmussen, 1997).

Case: Take-off checklists and the pressure to depart on-time

Airlines frequently struggle with on-time performance, particularly in heavily congested parts of the world, where so-called slot times govern when aircraft may become airborne. Making a slot time is critical, as it can be hours for a new slot to open up if the first one is missed. This push for speed can lead to problems with for example pre-take off checklists, and airlines regularly have problems with attempted take-offs in airplanes that are not correctly configured (particularly the wing flaps which help the aircraft fly at slower speeds such as in take-off and landing). One airline published a flight safety news letter that was distributed to all its pilots. The letter counted seven such configuration events in half a year, where aircraft did not have wing flaps selected before taking off, even when the item "flaps" on the before take-off checklist was read and responded to by the pilots. Citing no change in procedures (so that could not be the explanation), the safety letter went on to speculate whether stress or complacency could be a factor, particularly as it related to the on-time performance goals (which are explicitly stated by the airline elsewhere). Slot times played a role in almost half the events. While acknowledging that slot times and on-time performance were indeed important goals for the airline, the letter went on to say that flight safety should not be sacrificed for those goals. In an attempt to help crews develop their skills at coping with the boundaries, the letter also suggested that crew members should act on 'gut' feelings and speak out loudly as soon as something was detected that was amiss, particularly in high workload situations.

Leaving both pressures in place (a push for greater efficiency and a safety campaign pressing in the opposite direction) does little to help operational people (pilots in the case above) cope with the actual dilemma at the boundary. Also, a reminder to try harder and watch out better, particularly during times of high workload, is a poor substitute for actually developing skills to cope at the boundary. Raising awareness, however, can be meaningful in the absence of other possibilities for safety intervention, even if the effects of such campaigns tend to wear off quickly. Greater safety returns can be expected only if something more fundamental changes in the behavior-shaping conditions or the particular process environment (e.g. less traffic due to industry slow-down, leading to less congestion and fewer slot times). In this sense, it is important to raise awareness about the migration toward boundaries throughout the organization, at various managerial levels, so that a fuller range of countermeasures is available beyond telling front-line operators to be more careful. Organizations that are able to do this effectively have sometimes been dubbed high-reliability organizations.

High reliability versus resilience

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. Through a series of empirical studies, high reliability organizational (HRO) researchers 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 could achieve the consistency and stability required to effect failure-free operations (LaPorte & Consolini, 1991). Some of these categories were very much inspired by the worlds studied—naval aircraft carriers, for example (Rochlin, LaPorte & Roberts, 1987). There, in a relatively self-contained and disconnected closed system, systematic learning was a 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 multi-skilling.

When HRO researchers first set out to examine how safety is created and maintained in such complex systems, 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 was 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 picture. Operational safety—how it is created, maintained, discussed, mythologized—is 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."

The creation of safety, in other words, involves a belief about the possibility to continue operating safely. 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. It is a belief punctuated by encounters with risk, but it can become sluggish by overconfidence in past results, blunted by organizational smothering of minority viewpoints, and squelched by acute performance demands or production concerns. But that also makes it a belief that is, in principle, open to organizational or even regulatory intervention so as to keep it curious, open-minded, complexly sensitized, inviting of doubt, and ambivalent toward the past (e.g. Weick, 1993).

High reliability, resilience and "human error"

An important point for the role of "human error" in high reliability theory is that safety is not the same as reliability. A part can be reliable, but in and of itself it can't 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 is expressed as a component's failure rate over a period of time. In other words, it addresses the question of whether a component lives up to its pre-specified performance criteria. Organizationally, reliability is often associated with a reduction in variability, and 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 "human errors" and technical breakdowns.

In moderately safe systems, such as chemical industries or 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 cut down on the number of errors and incidents.

The monitoring of performance through operational safety audits, error counting, process data collection, and incident tabulations has become institutionalized and in many cases required by legislation or regulation. As long as an industry can assure that components (parts, people, companies, countries) can comply with pre-specified and auditable criteria, it affords the belief that it has a safe system. Quality assurance and safety management within an 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.

Such beliefs may well have been sustained by models such as the latent failure model discussed above, which posited that accidents are the result of a concatenation of factors, a combination of active failures at the sharp end with latent failures from the blunt end (the organizational, regulatory, societal part) of an organization. Accidents represent opportunistic trajectories through imperfectly sealed or guarded barriers that had been erected at various levels (procedural, managerial, regulatory) against them. This structuralist notion plays into the hand of reliability: the layers of defense (components) should be checked for their gaps and holes (failures) so as to guarantee reliable performance under a wide variety of conditions (the various line-ups of the layers with holes and gaps). People should not violate rules, process parameters should not exceed particular limits, acme nuts should not wear beyond this or that thread, a safety management system should be adequately documented, and so forth.

This model also sustains decomposition assumptions that are not necessarily applicable to complex systems (see Leveson, 2002). For example, it suggests that each component or sub-system (layer of defense) operates reasonably independently, so that the results of a 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 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 elimination of residual "noise" (e.g. errors, other kinds of performance variability) that stands between the current situation and perfect reliability is still a widely-pursued goal, as if industries are the custodian of an already safe system that merely needs protection from unpredictable, erratic components that are the remaining sources of unreliability. This common sense approach, says Amalberti (2001), which indeed may have helped some systems progress to their safety levels of today, is beginning to lose its traction. 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."

Many systems, even after progressing beyond being moderately safe, are still embracing this notion of reliability with vigor—not just to maintain their current safety level (which would

logically be non-problematic, in fact, it would even be necessary) but also as a basis for increasing safety even further. But as progress on safety in more mature systems (e.g. commercial 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 5x10-7 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."

The accident described below illustrates how the reductionist reliability model applied to understanding safety and risk (taking systems apart and checking whether individual components meet prespecified criteria) may no longer work well, and may in fact have contributed to the accident. 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 non-linear dynamics where new system behaviors emerge that cannot be anticipated using reductive logic, and negate the Newtonian assumption of symmetry between cause and consequence.

Case: Helios Airways B737, August 2005

On 13 August 2005, on the flight prior to 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).

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 take-off configuration horn (which warns pilots that the aircraft is not configured properly for take-off, 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.

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.

Helios 522 is unsettling and 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 accelerated the effects of hypoxia. And while there are variations in what JAR-compliant means as one travels 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 UK 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.

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 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).

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 the 14th of August 2005, this certified and certifyable system was not 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 sub-systems predicts little about how they can stochastically and non-linearly recombine to outwit our best efforts at anticipating pathways to failure.

The case above represents the temporary inability to cope effectively with complexity. This is true, of course, for the cockpit crew after climbing out from Larnaca, but it is even more interesting at a 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 European 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, Woods & Leveson, 2006) that put

together this crew, from this airline, in this airframe, with these system anomalies, on this day, outsmarted how the industry had learned to adapt, create and maintain safety in an already very safe activity.

Resilience engineering

Resilience Engineering represents a way of thinking about safety that departs from conventional risk management approaches based on componential approaches (e.g. error tabulation, violations, calculation of failure probabilities), Resilience Engineering looks for ways to enhance the ability of organizations to monitor and revise risk models, to create processes that are robust yet flexible, and to use resources proactively in the face of disruptions or ongoing production and economic pressures. Accidents, according to Resilience Engineering do not represent a breakdown or malfunctioning of normal system functions, but rather represent the breakdowns in the adaptations necessary to cope with the real world complexity. As control theory suggested with its emphasis on dynamic stability, individuals and organizations must always adjust their performance to current conditions; and because resources and time are finite it is inevitable that such adjustments are approximate. Success has been ascribed to the ability of groups, individuals, and organizations to anticipate the changing shape of risk before damage occurs; failure is the temporary or permanent absence of that.

Case: NASA organizational drift into the Columbia accident

While the final breakup sequence of the Space Shuttle Columbia could be captured by a sequence-of-events model (see the first case description in the beginning of this report), the organizational background behind it takes a whole different form of analysis, and has formed a rich trove of inspiration for thinking about how to engineer resilience into organizations.

A first, very critical shift was the re-classification of foam events from in-flight anomalies to maintenance and turn-around issues, something that significantly degraded the safety status of foam strikes. Foam loss was increasingly seen as an accepted risk or even, as one pre-launch briefing put it, "not a safety of flight issue" (CAIB, 2003, p. 126). This shift in the status of foam events is an important part of explaining the limited and fragmented evaluation of the Columbia foam strike and how analysis of that foam event never reached the problem-solving groups that were practiced at investigating anomalies, their significance and consequences, i.e., Mission Control.

What was behind this reclassification, how could it make sense for the organization at the time? First, pressure on schedule issues produced a mindset centered on production goals. There are several ways in which this could have played a role: first, schedule pressure magnifies the importance of activities that affect turnaround; second, when events are classified as in-flight anomalies a variety of formal work steps and checks are invoked; third, the work to assess anomalies diverts resources from the tasks to be accomplished to meet turnaround pressures. Second, a breakdown or absence of cross-checks on the rationale for classifying previous foam loss events as not an in-flight safety issue. In fact the rationale for the reclassification was quite weak, and flawed. The CAIB's examination reveals that no cross-checks were in place to detect, question, or challenge the specific flaws in the rationale. Third, the use of what on the surface looked like technical analyses to justify previously reached conclusions, rather than using technical analyses to test tentative hypotheses.

It would be very important to know more about the mindset and stance of different groups toward this shift in classification. For example, one would want to consider: Was the shift due to the salience of the need to improve maintenance and turnaround? Was this an organizational structure issue (which organization focuses on what aspects of problems)? What was Mission Control's reaction to the reclassification? Was it heard about by other groups? Did reactions to this shift remain underground relative to formal channels of communication?

Interestingly, the organization had three categories of risk: in-flight anomalies, accepted risks, and non-safety issues. As the organization began to view foam events as an accepted risk, there was no formal means for follow-up with a re-evaluation of an "accepted" risk to assess if it was in fact acceptable as new evidence built up or as situations changed. For all practical purposes, there was no difference between how the organization was handling non-safety issues and how it was handling accepted risks (i.e., accepted risks were being thought of and acted on no differently than non-safety issues). Yet the organization acted as if items placed in the accepted risk category were being evaluated and handled appropriately (i.e., as if the assessment of the hazard was accurate and up to date and as if the countermeasures deployed were still shown to be effective).

*Foam events were only one source of debris strikes that threaten different aspects of the orbiter structure. Debris strikes carry very different risks depending on where and what they strike. The hinge in considering the response to the foam strike on STS-107 is that the debris struck the leading-edge structure (*RCC panels and seals*) and not the tiles. Did concern and progress on improving tiles block the ability to see risks to other structures? Did NASA regard the leading edge as much less vulnerable to damage than tiles? This is important because the damage in STS-45 provided an opportunity to focus on the leading-edge structure and reconsider the margins to failure of that structure given strikes by various kinds of debris. Did this mission create a sense that the leading-edge structure was less vulnerable than tiles? Did this mission fail to revise a widely held belief that the RCC leading-edge panels were more robust to debris strikes than they really were? Who followed up the damage to the RCC panel and what did they conclude? Who received the results? How were risks to non-tile structures evaluated and considered -- including landing gear door structures? More information about the follow-up to leading-edge damage in STS-45 would shed light on how this opportunity was missed.*

A management stance emerged early which downplayed significance of the strike. The initial and very preliminary assessments of the foam strike created a stance toward further analysis that this was not a critical or important issue for the mission. The stance developed and took hold before there were results from any technical analyses. This indicates that preliminary judgments were biasing data evaluation, instead of following a proper engineering evaluation process where data evaluation points teams and management to conclusions.

Indications that the event was outside of boundary conditions for NASA's understanding of the risks of debris strikes seemed to go unrecognized. When events fall outside of boundaries of past data and analysis tools and when the data available includes large uncertainties, the event is by definition anomalous and of high risk. While personnel noted the specific indications in themselves, no one was able to use these indicators to trigger any deeper or wider recognition of the nature of the anomaly in this situation. This pattern of seeing the details but being unable to recognize the big picture is commonplace in accidents.

As the Debris Assessment Team (DAT) was formed after the strike was detected and began to work, the question arose: "Is the size of the debris strike 'out-of-family' or 'in-family' given past experience?" While the team looked at past experience, it was unable to get a consistent or informative read on how past events indicated risk for this event. It appears no other groups or representatives of other technical areas were brought into the picture. This absence of any cross-checks is quite notable and inconsistent with how Mission Control groups evaluate in-flight anomalies. Past studies indicate that a review or interaction with another group would have provided broadening checks which help uncover inconsistencies and gaps as people need to focus their analysis, conclusions, and justifications for consideration and discussion with others.

Evidence that the strike posed a risk of serious damage kept being encountered -- RCC panel impacts at angles greater than 15 degrees predicted coating penetration (CAIB, 2003, p. 145), foam piece 600 times larger than ice debris previously analyzed (CAIB, 2003, p. 143), models predicting tile damage deeper than tile thickness (CAIB, 2003, p. 143). Yet a process of discounting evidence discrepant with the current assessment went on several times (though eventually the DAT concerns seem to focus on the landing gear doors rather than the leading-edge structure).

Given the concerns about potential damage that arose in the DAT and given its desire to determine the location more definitively, the question arises: did the team conduct contingency analyses of damage and consequences across the different candidates sites -- leading edge, landing gear door seals, tiles? Based on the evidence compiled in the CAIB report, there was no contingency analysis or follow through on the consequences if the leading-edge structure (RCC) was the site damaged. This is quite puzzling as this was the team's first assessment of location and in hindsight their initial estimate proved to be reasonably accurate.

This lack of follow-through, coupled with the DAT's growing concerns about the landing gear door seals, seems to indicate that the team may have viewed the leading-edge structures as more robust to strikes than other orbiter structures. The CAIB report fails to provide critical information about how different groups viewed the robustness or vulnerability of the leading-edge structure to damage from debris strikes (of course, post-accident these beliefs can be quite hard to determine, but various memos/analyses may indicate more about the perception risks to this part of the orbiter). Insufficient data is available to understand why RCC damage was under-pursued by the Debris Assessment Team.

There was a fragmented view of what was known about the strike and its potential implications over time, people, and groups. There was no place, artifact, or person who had a complete and coherent view of the analysis of the foam strike event (note a coherent view includes understanding the gaps and uncertainties in the data or analysis to that point). This contrasts dramatically with how Mission Control works to investigate and handle anomalies where there are clear lines of responsibility to have a complete, coherent view of the evolving analysis vested in the relevant flight controllers and in the flight director. Mission Control has mechanisms to keep different people in the loop (via monitoring voice loops, for example) so that all are up to date on the current picture of situation. Mission Control also has mechanisms for correcting assessments as analysis proceeds, whereas in this case the fragmentation and partial views seemed to block reassessment and freeze the organization in an erroneous assessment. As the DAT worked at the margins of knowledge and data, its partial assessments did not benefit from cross-checks through interactions with other technical groups with different backgrounds and assumptions. There is no report of a technical review process that accompanied its work. Interactions with people or groups with different knowledge and assumptions is one of the best ways to improve assessments and to aid revision of assessments. Mission Control anomaly response includes many opportunities for cross-checks to occur. In general, it is quite remarkable that the groups practiced at anomaly response -- Mission Control -- never became involved in the process.

The process of analyzing the foam strike by the DAT broke down in many ways. The fact that this group also advocated steps that we now know would have been valuable (the request for imagery to locate the site of the foam strike) leads us to miss the generally fragmented distributed problem-solving process. The fragmentation also occurred across organizational levels (DAT to Mission Management Team (MMT)). Effective collaborative problem-solving requires more direct participation by members of the analysis team in the overall decision-making process. This is not sufficient of course; for example, the MMT's stance already defined the situation as, "Show me that the foam strike is an issue" rather than "Convince me the anomaly requires no response or contingencies." Overall, the evidence points to a broken distributed problem-solving process -- playing out in between organizational boundaries. The fragmentation in this case indicates the need for a senior technical focal point to integrate and guide the anomaly analysis process (e.g., the flight director role). And this role requires real authority. The MMT and the MMT chair were in principle in a position to supply this role, but:

Was the MMT practiced at providing the integrative problem-solving role? Were there other cases where significant analysis for in flight anomalies was guided by the MMT or were they all handled by the Mission Control team? The problem-solving process in this case has the odd quality of being stuck in limbo: not dismissed or discounted completely, yet unable to get traction as an in-flight anomaly to be thoroughly investigated with contingency analyses and re-planning activities. The dynamic appears to be a management stance that puts the event outside of safety of flight (e.g., conclusions drove, or eliminated, the need for analysis and investigation, rather than investigations building the evidence from which one would draw conclusions). Plus, the DAT exhibited a fragmented problem-

solving process that failed to integrate partial and uncertain data to generate a big picture -- i.e., the situation was outside the understood risk boundaries and carried significant uncertainties.

The Columbia case reveals a number of classic patterns that have helped shape the ideas behind resilience engineering—some of these patterns have their basis in the earlier models described in this part of the report:

- Drift toward failure as defenses erode in the face of production pressure.
- An organization that takes past success as a reason for confidence instead of investing in anticipating the changing potential for failure.
- Fragmented distributed problem-solving process that clouds the big picture.
- Failure to revise assessments as new evidence accumulates.
- Breakdowns at the boundaries of organizational units that impede communication and coordination.

The Columbia case provides an example of a tight squeeze on production goals, which created strong incentives to downplay schedule disruptions. With shrinking time/resources available, safety margins were likewise shrinking in ways which the organization couldn't see. Goal tradeoffs often proceed gradually as pressure leads to a narrowing of focus on some goals while obscuring the tradeoff with other goals. This process usually happens when acute goals like production/efficiency take precedence over chronic goals like safety. The dilemma of production/safety conflicts is this: if organizations never sacrifice production pressure to follow up warning signs, they are acting much too riskily. On the other hand, if uncertain "warning" signs always lead to sacrifices on acute goals, can the organization operate within reasonable parameters or stakeholder demands? It is precisely at points of intensifying production pressure that extra safety investments need to be made in the form of proactive searching for side-effects of the production pressure and in the form or reassessing the risk space -- safety investments are most important when least affordable. This raises the following questions:

- How does a safety organization monitor for drift and its associated signs, in particular, a means to recognize when the side-effects of production pressure may be increasing safety risks?
- What indicators should be used to monitor the organization's model of itself, how it is vulnerable to failure, and the potential effectiveness of the countermeasures it has adopted?
- How does production pressure create or exacerbate tradeoffs between some goals and chronic concerns like safety?
- How can an organization add investment in safety issues at the very time when the organization is most squeezed? For example, how does an organization note a reduction in margins and follow through by rebuilding margin to boundary conditions in new ways?

Another general pattern identified in Columbia is that an organization takes past success as a reason for confidence instead of digging deeper to see underlying risks. During the drift toward failure leading to the Columbia accident a misassessment took hold that resisted revision (that is, the misassessment that foam strikes pose only a maintenance problem and not a risk to orbiter safety). It is not simply that the assessment was wrong; what is troubling is the inability to re-evaluate the assessment and re-examine evidence about the vulnerability.

The absence of failure was taken as positive indication that hazards are not present or that countermeasures are effective. In this context, it is very difficult to gather or see if evidence is

building up that should trigger a re-evaluation and revision of the organization's model of vulnerabilities. If an organization is not able to change its model of itself unless and until completely clear-cut evidence accumulates, that organization will tend to learn late, i.e., it will revise its model of vulnerabilities only after serious events occur. On the other hand, high reliability organizations assume their model of risks and countermeasures is fragile and even seek out evidence about the need to revise and update this model (Rochlin, 1999). They do not assume their model is correct and then wait for evidence of risk to come to their attention, for to do so will guarantee an organization that acts more risky riskier than it desires.

The missed opportunities to revise and update the organization's model of the riskiness of foam events seem to be consistent with what has been found in other cases of failure of foresight. This discounting of evidence can be described as "distancing through differencing," whereby those reviewing new evidence or incidents focus on differences, real and imagined, between the place, people, organization, and circumstances where an incident happens and their own context. By focusing on the differences, people see no lessons for their own operation and practices (or only extremely narrow, well-bounded responses). This contrasts with what has been noted about more effective safety organizations which proactively seek out evidence to revise and update this model, despite the fact that this risks exposing the organization's blemishes (Rochlin, 1999).

The distancing through differencing that occurred throughout the build-up to the final Columbia mission can be repeated in the future as organizations and groups look at the analysis and lessons from this accident and the CAIB report. Others in the future can easily look at the CAIB conclusions and deny their relevance to their situation by emphasizing differences (e.g., my technical topic is different, my managers are different, we are more dedicated and careful about safety, we have already addressed that specific deficiency). This is one reason avoiding hindsight bias is so important. When we start with the question, "How could they have missed what is now obvious?," we are enabling future distancing through differencing rationalizations. The distancing through differencing process that contributes to this breakdown also indicates ways to change the organization to promote learning. One general principle which could be put into action is this: do not discard other events because they appear on the surface to be dissimilar. At some level of analysis all events are unique, while at other levels of analysis they reveal common patterns. Every event, no matter how dissimilar to others on the surface, contains information about underlying general patterns that help create foresight about potential risks before failure or harm occurs. To focus on common patterns rather than surface differences requires shifting the analysis of cases from surface characteristics to deeper patterns and more abstract dimensions. Each kind of contributor to an event can then guide the search for similarities.

This suggests that organizations need a mechanism to generate new evaluations that question the organization's own model of the risks it faces and the countermeasures deployed. Such review and reassessment can help the organization find places where it has underestimated the potential for trouble and revise its approach to create safety. A quasi-independent group is needed to do this -- independent enough to question the normal organizational decision-making but involved enough to have a finger on the pulse of the organization (keeping statistics from afar is not enough to accomplish this).

Another general pattern identified in Columbia is a fragmented problem-solving process that clouds the big picture. During Columbia there was a fragmented view of what was known about the strike and its potential implications. There was no place or person who had a complete and coherent view of the analysis of the foam strike event including the gaps and uncertainties in the data or analysis to that point. It is striking that people used what looked like technical analyses to

justify previously reached conclusions, instead of using technical analyses to test tentative hypotheses.

Discontinuities and internal handovers of tasks increase risk of fragmented problem-solving (Patterson, Roth, Woods, Chow, & 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. High reliability organization 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, Roth, Woods, Chow, & Gomez, 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:

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

Such problems could also have played a role in the Helios accident, described above. In Columbia, the breakdown or absence of cross-checks between disjointed departments and functions is also striking. Cross-checks on the rationale for decisions is a critical part of good organizational decision-making. Yet no cross-checks were in place to detect, question, or challenge the specific flaws in the rationale, and no one noted that cross-checks were missing. The breakdown in basic engineering judgment stands out as well. The initial evidence available already placed the situation outside the boundary conditions of engineering data and analysis. The only available analysis tool was not designed to predict under these conditions, the strike event was hundreds of times the scale of what the model is designed to handle, and the uncertainty bounds were very large with limited ability to reduce the uncertainty (CAIB, 2003).

Being outside the analyzed boundaries should not be confused with not being confident enough to provide definitive answers. In this situation basic engineering judgment calls for large efforts to extend analyses, find new sources of expertise, and cross-check results as Mission Control both practices and does. Seasoned pilots and ship commanders well understand the need for this ability to capture the big picture and not to get lost in a series of details. The issue is how to train for this judgment. For example, the flight director and his or her team practice identifying and handling anomalies through simulated situations. Note that shrinking budgets led to pressure to reduce training investment (the amount of practice, the quality of the simulated situations, and the number or variety of people who go through the simulations sessions can all decline).

What about making technical judgments? Relevant decision-makers did not seem able to notice when they needed more expertise, data, and analysis in order to have a proper evaluation of an issue. NASA's evaluation prior to STS-107 that foam debris strikes do not pose risks of damage to the orbiter demands a technical base. Instead their "resolution" was based on very shaky or absent technical grounds, often with shallow, offhand assessments posing as and substituting for careful analysis.

The fragmentation of problem-solving also illustrates Weick's points about how effective organizations exhibit a "deference to expertise," "reluctance to simplify interpretations," and "preoccupation with potential for failure," none of which was in operation in NASA's organizational decision-making leading up to and during Columbia (Weick et al., 1999). A safety organization must ensure that adequate technical grounds are established and used in organizational decision-making. To accomplish this, in part, the safety organization will need to define the kinds of anomalies to be practiced as well as who should participate in simulation training sessions. The value of such training depends critically on designing a diverse set of anomalous scenarios with detailed attention to how they unfold. By monitoring performance in these simulated training cases, safety personnel will be better able to assess the quality of decision-making across levels in the organization.

The fourth pattern in Columbia is a failure to revise assessments as new evidence accumulates. The accident shows how difficult it is to revise a misassessment or to revise a once plausible assessment as new evidence comes in. This finding has been reinforced in subsequent studies in different settings (Feltovich et al., 1997; Johnson et al., 1991). Research consistently shows that revising assessments successfully requires a new way of looking at previous facts. Organizations can provide this "fresh" view:

- By bringing in people new to the situation;
- Through interactions across diverse groups with diverse knowledge and tools;
- Through new visualizations which capture the big picture and reorganize data into different perspectives.

One constructive action is to develop the collaborative interchanges that generate fresh points of view or that produce challenges to basic assumptions. This cross-checking process is an important part of how NASA Mission Control and other organizations successfully respond to anomalies (for a case where these processes break down see Patterson et al., 2004). One can also capture and display indicators of safety margin to help people see when circumstances or organizational decisions are pushing the system closer to the edge of the safety envelope. (this idea is something that Jens Rasmussen, one of the pioneers of the new results on error and organizations, has been promoting for two decades (Rasmussen, 1997).

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 completely clear-cut evidence. If revision only occurs when evidence is overwhelming, there is a grave risk of an organization acting too riskily and finding out only from near-misses, serious incidents, or even actual harm. Instead, the practice of revising assessments of risk needs to be an ongoing process. In this process of continuing re-evaluation, the working assumption is that risks are changing or evidence of risks has been missed.

What is particularly intresting about NASA's organizational decision-making is that the correct diagnosis of production/safety tradeoffs and useful recommendations for organizational change were noted in 2000. The Mars Climate Orbiter report of March 13, 2000 depicts how the pressure for production and to be "better" on several dimensions led to management accepting riskier and riskier decisions. This report recommended many organizational changes similar to those in the CAIB report. A slow and weak response to the previous independent board report was a missed opportunity to improve organizational decision-making in NASA. The lessons of Columbia should lead organizations of the future to develop a safety organization that provides "fresh" views on risks to help discover the parent organization's own blind spots and question its conventional assumptions about safety risks.

Finally, the Columbia accident brings to the fore another pattern: Breakdowns at the boundaries of organizational units. The CAIB analysis notes how a kind of Catch-22 was operating in which the people charged to analyze the anomaly were unable to generate any definitive traction and in which the management was trapped in a stance shaped by production pressure that views such events as turnaround issues. This effect of an "anomaly in limbo" seems to emerge at the boundaries of different organizations that do not have mechanisms for constructive interplay. It is here that we see the operation of the generalization that in risky judgments of risk we have to defer to those with technical expertise and the necessity to set up a problem-solving process that engages those practiced at recognizing anomalies in the event.

This pattern points to the need for mechanisms that create effective overlap across different organizational units and the need to avoid simply staying inside the chain-of-command mentality (though such overlap can be seen as inefficient when the organization is under severe cost pressure). This issue is of particular concern to many organizations as communication technology has linked together disparate groups as a distributed team. This capability for connectivity is leading many to work on how to support effective coordination across these distributed groups, e.g., in military command and control. A safety organization must have the technical expertise and authority to enhance coordination across the normal chain of command.

Engineering Resilience in Organizations

The insights derived from the above five patterns and other research results on safety in complex systems point to the need to monitor and manage risk continuously throughout the life-cycle of a system, and in particular to find ways of maintaining a balance between safety and the often considerable pressures to meet production and efficiency goals (Adamski and Westrum, 2003; Reason, 1997; Weick et al., 1999). These results indicate that safety management in complex systems should focus on resilience -- the ability to adapt or absorb disturbance, disruption, and change. A system's resilience captures the result that failures are breakdowns in the normal adaptive processes necessary to cope with the complexity of the real world (Rasmussen, 1990; Rasmussen et al., 1994; Sutcliffe and Vogel, 2003; Woods and Cook, 2004).

A system's resilience includes properties such as:

- buffering capacity: the size or kinds of disruptions the system can absorb or adapt to without a fundamental breakdown in performance or in the system's structure;
- flexibility: the system's ability to restructure itself in response to external changes or pressures;
- margin: how closely the system is currently operating relative to one or another kind of performance boundary;
- tolerance: whether the system gracefully degrades as stress/pressure increase, or collapses quickly when pressure exceeds adaptive capacity.

Cross-scale interactions are another important factor, as the resilience of a system defined at one scale depends on influences from scales above and below: downward in terms of how organizational context creates pressures/goal conflicts/dilemmas and upward in terms of how adaptations by local actors in the form of workarounds or innovative tactics reverberate and influence more strategic issues. Managing resilience, or resilience engineering, then, focuses on what sustains or erodes the adaptive capacities of human-technical systems in a changing environment (Hollnagel et al., 2006). The focus is on monitoring organizational decision-making

to assess the risk that the organization is operating nearer to safety boundaries than it realizes (or, more generally, that the organization's adaptive capacity is degrading or lower than the adaptive demands of its environment).

Resilience engineering seeks to develop engineering and management practices to measure sources of resilience, provide decision support for balancing production/safety tradeoffs, and create feedback loops that enhance the organization's ability to monitor/revise risk models and to target safety investments. For example, resilience engineering would monitor evidence that effective cross-checks are well integrated when risky decisions are made, or would serve as a check on how well the organization prepares to handle anomalies by checking on how it practices handling of simulated anomalies (what kind of anomalies, who is involved in making decisions). The focus on system resilience emphasizes the need for proactive measures in safety management: tools to support agile, targeted, and timely investments to defuse emerging vulnerabilities and sources of risk before harm occurs.

To achieve resilience, organizations need support for decisions about production/safety tradeoffs. Resilience engineering should help organizations decide when to relax production pressure to reduce risk, or, in other words, develop tools to support sacrifice decisions across production/safety tradeoffs. When operating under production and efficiency pressures, evidence of increased risk on safety may be missed or discounted. As a result, organizations act in ways that are riskier than they realize or want, until an accident or failure occurs. This is one of the factors that creates the drift toward failure signature in complex system breakdowns.

To make risk a proactive part of management decision-making means knowing when to relax the pressure on throughput and efficiency goals, i.e., make a sacrifice decision; how to help organizations decide when to relax production pressure to reduce risk. These tradeoff decisions can be referred to as sacrifice judgments because acute production- or efficiency-related goals are temporarily sacrificed, or the pressure to achieve these goals is relaxed, in order to reduce risks of approaching too near to safety boundary conditions. Sacrifice judgments occur in many settings: when to convert from laparoscopic surgery to an open procedure (e.g., Cook et al., 1998), when to break off an approach to an airport during weather that increases the risk of wind shear, or when to have a local slowdown in production operations to avoid risks as complications build up. Ironically, it is at the very times of higher organizational tempo and focus on acute goals that we require extra investment in sources of resilience to keep production/safety tradeoffs in balance -- valuing thoroughness despite the potential for sacrifices on efficiency required to meet stakeholder demands.

Over the past two decades, 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.

Resilience Engineering, the latest addition to thinking about safety and human performance in complex organization, is built on insights derived in part from HRO work, control theory, Perrowian complexity and even man-made disaster theory. It is concerned with assessing organizational risk, that is the risk that 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 would serve as a check on how well the organization is practicing the handling of simulated anomalies (what kind of anomalies, who is involved in making decisions).

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 include:

- Preparedness/Anticipation: is the organization proactive in picking up on evidence of developing problems versus only reacting after problems become significant?
- 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?
- Flexibility/Stiffness—how does the organization adapt to change, disruptions, and opportunities?

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

- detecting signs of increasing organizational risk, especially when production pressures are intense or increasing;
- having the resources and authority to make extra investments in safety at precisely these times when it appears least affordable;
- having a means to recognize when and where to make targeted investments tocontrol rising signs of organizational risk and re-balance the safety and production tradeoff.

These resilience-enhancing mechanisms may help produce an organization that creates foresight about changing risks before failures occur, by offering new directions for measuring and maintaining safety in complex systems.

Resilience — summary of its cornerstones and considerations for implementation

As the practical interest for resilience engineering continues to grow, so does the need of a clear definition and of practical methods. The purpose of this short chapter is to propose a working definition of resilience and analyse it in some detail. The working definition, based on the work in the project described here, is as follows:

> A resilient system is able effectively to adjust its functioning prior to, during, or following changes and disturbances, so that it can continue to perform as required after a disruption or a major mishap, and in the presence of continuous stresses.

The key term of this definition is the ability of a system to *adjust* its functioning. (The terms system and organisation are used interchangeably in this chapter.) This makes clear that resilience is more than the ability to *continue* functioning in the presence of stress and disturbances. While the ability of a system or an organisation to preserve and sustain its primary functions is important, this can be achieved by other and more traditional means. Continued functioning can for instance be achieved by isolating the system from the environment, or by making it impervious to exogenous disturbances. An example of that, which we covered in detail earlier in the report, is the *defence-in-depth* principle, which means that there are multiple layers of barriers between the system and the environment in which it exists. The *defence-in-depth* solution can, of course, serve to protect either the system, the environment, or both. In the field of nuclear power generation, *defence-in-depth* is defined as:

> "... a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant." (INSAG-10)

To maintain functioning despite external disturbances and disruptions clearly has a cost, since it is expensive to build and maintain defences and inefficient to keep too many resources and supplies ready for deployment without actually using them. It is therefore not a universally applicable solution, and is sometimes sacrificed in the name of productivity improvements or cost reductions.

Considerations before the implementation of resilience engineering

As the key term emphasizes, the ability to go on functioning is a result of the ability to *adjust* the functioning, rather than to maintain it unchanged. This adjustment can in principle take place either after something has happened (be reactive) or something happens (be proactive). Reactive adjustment is by far the most common. For instance, if there is a major accident in a community, such as a large fire or an explosion, local hospitals will change their state of functioning to be prepared for a rush of people that have been hurt. (For a more extreme case see the description of the responses to a bus bombing by Cook & Nemeth, 2006.) Responding when something happens may, however, be insufficient to guarantee the system's safety and survivability. One reason is that a system can only be ready to respond to a limited set of events or conditions, either in the sense that it only recognises a limited set of symptoms or in the sense that it only has the resources needed for certain kinds of events – and usually only for a limited duration. Vivid examples of that can be found in everyday events, the most conspicuous case in recent years being the (lack of) response by the Federal Emergence Management Agency (FEMA) to the Hurricane Katrina in 2005 (e.g., Comfort & Haase, 2006). In the world of business, the failure of Airbus company to recognise and effectively respond to the problems with the production of the A380 in the June 2006, and the later failure of the Boeing company to do the same with the production of the 787 in September 2007, suggest that limited readiness is not an unusual

phenomenon at all.

Going further into the proposed definition of resilience, a second key phrase is that the system must be able to adjust its functioning *prior to, during,* or *following* changes and disturbances. The ability to make adjustments prior to an event means that the system can change from a state of normal functioning to a state of heightened readiness *before* something happens. A state of readiness means that resources are allocated to match the needs of the expected event, that special functions are activated, and that defences are increased. A trivial example is to batten down the hatches to prepare for stormy weather, either literally or metaphorically. An everyday example from the world of aviation is to secure the seat belts before start and landing or during turbulence. In these cases the criteria for when to go from a normal state to a state of readiness are clear. In other cases it may be less obvious either because of a lack of experience or because the validity of indicators is questionable. An increased state of alertness should, of course, not last longer than necessary since it may consume resources that otherwise could be used for normal performance. An example of failing to re-adjust is the alert level for air travel in the US, which was raised from the yellow (elevated) level to the orange (high) level on August 10 2006, and has remained there ever since (at least at the time of writing this, May 2008).

The ability to adjust *during* changes and disturbances, to respond when something happens, has already been mentioned and will be elaborated further below. The ability to adjust *following* changes and disturbances means that the experiences from events of the past are used to make decisions about structural or functional changes so that the system it is better prepared for what may happen in the future. These changes are often focused on the causes, as determined by accident investigations, although such causes and explanations always must be seen relative to the accident models and the investigation methods that were used (Hollnagel, 2004 & 2008a). The working definition of resilience can be made more detailed by noticing that it implies four cornerstones of resilience, each representing an essential system capability. The four cornerstones, or four essential capabilities are:

• Knowing what to *do*, i.e., how to respond to regular and irregular disruptions and disturbances by adjusting normal functioning. This is the ability to address the *actual*.
• Knowing what to *look for*, i.e, how to monitor that which is or could become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, i.e., its own performance. This is the ability to address the *critical*.
• Knowing what to *expect*, i.e., how to anticipate developments and threats further into the future, such as potential disruptions, pressures, and their consequences. This is the address to address the *potential*.
• Knowing what *has happened*, i.e., how to learn from experience, in particular to learn the right lessons from the right experience. This is the ability to address the *factual*.

What resilient systems are actually able to do

No system – be it an individual, a group, or an organization – can sustain its functioning and continue to exist unless it is able to respond to what happens. The response must furthermore be effective in the sense that it helps bring about a desired change. As described above, a resilient system responds by adjusting its functioning so that it better matches the new conditions. Other responses are to mitigate the effects of an adverse event, to prevent a further deterioration or spreading of effects, to restore the state that existed before the event or to resume the functioning that existed before, to change to stand-by conditions, etc.

In order to respond when something happens the system must be able to *detect* that something has happened. Second, it must be able to *identify* the event and *recognise* or *rate* it as being so serious that a response is necessary. Third, the system must know how to *respond* and be capable of responding, in particular it must have or be able to command the required resources long enough for the response to have an effect. The detection that something has happened is not entirely passive but depends on what the system looks for – on what its pre-defined categories of critical events or threats are. If the system looks for the wrong events or threats it may either fail to recognise some threats (false negatives or a Type II error) or respond to situations where a response was not actually needed (false positives or a Type I error). The former will leave the system vulnerable to unexpected events. The latter may be harmful both because the system may transition to a state that is not easily reversible, and because it wastes resources and reduces readiness. Some events may be so obvious that they cannot be missed, yet without any response being ready – or even without a clear idea of what should be done. (The subprime crisis of 2007 was an example of that.) In such cases there may also be an urgency of the situation, i.e., an immediate pressure to act, which by its very nature limits the ability to consider what the proper response should be. A tragic example of that is the not infrequent situation when people get caught in a nightclub fire. Under such conditions the system, or in this case the individuals, may easily lose control by responding in an opportunistic or scrambled rather than in a more orderly mode (Hollnagel, 1998).

Rating or deciding whether an event or a threat is so serious that a response must be made can refer either to the establishing of a level of readiness, or to taking action in the concrete situation. In the first case, deciding that a response capability is needed depends on a number of factors, cultural, organisational, and situational. The dilemma is nicely captured by the common definition of safety as the freedom from unacceptable risks, which forces the question of when a risk is considered acceptable – and by whom. A common solution is to rely on probability calculations, and accept all risks where the probability is lower than some numerically defined limit (e.g., Amalberti, 2006). This, however, does not solve the problem of how the limit is set. Another solution is to invoke the *As Low As Reasonably Practicable* (ALARP). A risk is ALARP if the cost of any reduction in that risk is grossly disproportionate to the benefit obtained from the reduction. This links the acceptability of risks, and therefore also the decision of whether a response capability is necessary, to economical criteria. This becomes even more obvious in the UK Offshore Installations Regulations' clarification of the ALARP principle: "If a measure is practicable and it cannot be shown that the cost of the measure is grossly disproportionate to the benefit gained, then the measure is considered reasonably practicable and should be implemented."

The second case is how to decide whether a response should be activated in a given situation. As long as the activation of the response depends on technology, including software, the problem is in principle solvable. But in cases where the decision depends on humans – at any level of an organisation – the problem is more difficult. Deciding whether to do something, and when to do it, depends to a considerable extent on the competence of the people involved, and on the situation in which they find themselves (e.g., Dekker & Woods, 1999). Finally, having the resources necessary for the chosen response is also essential. This is not only a question of having prepared resources, which really only makes sense for regular threats (cf., below), but also a question of whether the system is flexible enough to make the necessary resources available when needed. The ability to address the actual can also be seen in relation to the various types of threats that may exist. Westrum (2006) has proposed a characterisation of threats in terms of their predictability, their potential to disrupt the system, and their origin (internal vs. external). He further proposed to make a distinction among three types of threats:

1. Regular threats that occur so often that it is both possible and cost-effective for the system to develop a standard response and to set resources aside for such situations.
2. Irregular threats or one-off events, for which it is virtually impossible to provide a standard response. The very number of such events also makes the cost of doing so prohibitive.
3. Unexampled events, which are so unexpected that they push the responders outside of their collective experience envelope. For such events it is utterly impracticable to consider a prepared response, although their possible existence at least should be recognised.

The ability to address the actual depends on whether threats or events can be imagined, on whether it is possible to prepare a response, and on whether it is cost effective to do so. Referring to the three categories listed above, it is clear that such readiness only is feasible for regular threats. That does, however, not mean that irregular threats and unexampled events can be disregarded. They must, however, be dealt with in a different manner.

Focusing on the critical

A resilient system must be able flexibly to monitor what is going on, including its own performance. The ability to monitor enables the system to cope with that which could become critical in the near term. The flexibility means that the monitoring basis must be assessed from time to time, so that the monitoring does not become constrained by routine and habits. As argued above, it is in practice only possible for a system to be ready to respond to regular threats, or even just to a subset of these. It is nevertheless a potential risk if the readiness to respond is limited to a small number of events or conditions. The solution is to monitor for what may become critical, and use that to change from a state of normal operation to a state of readiness when the conditions indicate that a crisis, disturbances, or failure is imminent. Such as two-step approach will be more cost effective. If a system can make itself ready when something is going to happen, rather than remain in a state of readiness more or less permanently, then resources may be freed for more productive purposes. The difficulty is, of course, to be able to decide that something may go wrong so early that there is sufficient time to change to a state of readiness. It is also necessary that the identification of the impending event is so reliable that preparations are not made in vain.

Monitoring normally looks for certain conditions or relies on certain indicators. These are by definition called leading indicators, because they indicate what may happen *before* it happens. Everyday life is replete with examples, as the indicators for the weather tomorrow or for the coming winter (or summer). While meteorologists today are very good at predicting the weather, risks analysts are less successful in predicting when something will go wrong. (It is a sobering thought that economists and politicians seem to be even less capable of foreseeing financial and political crises.) In the case of the weather there are good leading indicators because we have an accurate understanding of the phenomenon, i.e., of how the (weather) system functions. In other cases, and particularly in safety related cases, we only have weak or incomplete descriptions of what goes on and therefore have no effective way of proposing or defining valid leading indicators. Because of this, most systems rely on lagging indicators instead, such as accident statistics. While many lagging indicators have a reasonable face validity, they are only known with a delay that often may be quite considerable (e.g., annual statistics). The dilemma of lagging indicators is that while the likelihood of success increases the smaller the lag is (because early interventions are more effective than late ones), the validity or certainty of the indicator increases the longer the lag (or sampling period) is.

According to the proposed definition, resilience is the ability of a system effectively to adjust its

functioning prior to an event. As argued above, this can only be done if attention is paid to that which may become critical in the short term. For a system to do so requires that the effort is deemed worthwhile, that the necessary investment in resources (time and money) is made, and that the monitoring focuses on the right indicators or symptoms. Failing that the system will sometimes be caught unprepared when it should have been ready. There will always be situations that completely defy both preparations and monitoring – the dreaded unexampled events – but more can be done to reduce their number and frequency of occurrence than established safety practices allow.

Looking out for the potential

While looking for what may go wrong in the immediate future generally makes sense, it may be less obvious that there is an advantage to look very far ahead as well, to look at what could possibly happen in the more distant future. The difference between monitoring and looking ahead is not just that the time horizons are different (short versus long), but also that it is done in different ways. In monitoring, a set of pre-defined cues or indicators are checked to see if they change, and if it happens in a way that demands a readiness to respond. In looking for the potential, the goal is to identify possible future events, conditions, or state changes – internal or external to the system – that should be prevented or avoided. While monitoring tries to keep an eye on the regular threats, looking for the potential tries to identify the most likely irregular threats.

Already, risk assessment already does look for the potential. In principle, that is. But risk assessment is constrained because it relies on representations and methods that focus on linear combinations of discrete events, such as event trees and fault trees. Established risk assessment methods are developed for tractable systems where the principles of functioning are known, where descriptions do not contain too many details, where descriptions can be made relatively quickly, and where the system does not change while the description is being made (Hollnagel, 2008b). For such systems it may be acceptable to look for the failure potential in simple combinations of discrete events or linear extrapolations of the past. Many present day systems of major interest for industrial safety are unfortunately intractable rather than tractable. This means that the principles of functioning are only partly or incompletely known, that the description is elaborate and contains many details, that it takes a long time to make, and that the system therefore changes while the description is made. In consequence of that there will never be a complete description of the system and it is therefore ill advised to rely on established risk assessment methods.

Looking for the potential requires requisite imagination or the ability to imagine key aspects of the future (Westrum, 1993). As described by Adamski & Westrum (2003), requisite imagination is needed to know from which direction trouble is likely to arrive and to explore those factors that can affect outcomes in future contexts. The relevance of doing that is unfortunately not always obvious as the following example illustrates. In a recent discussion about whether it was safe to use meat from cloned animals for human consumption, the chief food expert of the US Food and Drug Administration claimed that it was beyond his imagination to even find a theory that would cause the food to be unsafe. This categorical rejection of the possibility that something could go wrong obviates any need to look to the potential, and perhaps also to monitor for the critical.

Even if the possibility that something could go wrong is acknowledged, thinking about the potential is fraught with difficulties. Many studies have, for instance, shown that human thinking

makes use of a number of simplifying heuristics such as representativeness, recency, and anchoring (Tversky & Kahneman, 1974). While these may improve efficiency in normal working conditions, they severely restrict the more open-minded thinking that is necessary to look at the possible. Looking for the potential is also difficult because it requires a disciplined combination of individual or collective imagination. It can also be costly, both because it cannot be hurried but must take its time and because it deals with something that may happen so far into the future that benefits are rather uncertain. Relatively few organisations therefore allocate sufficient resources to look at the potential. However, a truly resilient organization realises the need at least to do something.

Learning from experience

A resilient system must be able to learn from experience. Although this is mentioned last, it is in many ways the basis for the ability to respond, to monitor, and to look ahead. (The four cornerstones are actually equally important, and it is only the limitations of a written text that forces one to be mentioned before the other.) To learn from experience sounds rather straightforward and few safety managers, administrators, or regulators will willingly disagree with that. Yet if it is to be done in an efficient and systematic manner, it requires careful planning and ample resources. The effectiveness of learning depends on what the basis for the learning is, i.e., which events or experiences are taken into account; on how the events are analysed and understood; and on when and how often the learning takes place. This can be elaborated as follows (for a more detailed discussion, see Hollnagel, 2008a):

• Which events should be investigated and which should not? Since human, material, and temporal resources always are limited, it is necessary to separate the wheat from the chaff, to focus on what is important and to disregard what is unimportant. One common bias is to focus on failures and disregard successes, on the mistaken assumption that the two outcomes represent different underlying "processes." Investigations may further be limited to look only at events with serious outcomes (accidents) and disregard other adverse events such as incidents and unsafe acts. Another bias is to focus on adverse events that happen locally and to disregard experiences that could be learned from other places. Resilience engineering tries to overcome all of these biases.

• How should events be described? Anyone who has been involved in accident investigation or risk assessment knows that there are no objective or true descriptions of events. The description depends on which data are collected, how they are coded or categorised, and not least how they are analysed. The latter is perhaps the most important factor since the assumptions behind the chosen analysis method to a large degree determines the result (Hollnagel, 2004). In accident investigation, as in most other human endeavours, *What You Look For Is What You Find.* A root cause analysis will, for example, not give the same results as an epidemiological analysis, and the learning will therefore be different in the two cases.

• When and how should learning take place? This is primarily a question of whether learning should be discrete or continuous, i.e., whether should it be done whenever something has happened or on a more regular basis? If it only takes place after "important" events, then nothing is learned from "unimportant" events, which are by far the more frequent. If learning is more regular, then how often should it be done and how many resources should be allocated to do it?

• What should the locus of learning be, individual or organisational? In any given situation, performance is determined by a combination of three things. First, individual knowledge and

skills – as well as the individual's perception and assessment of the situation. Second, institutionalised knowledge, usually expressed by means of rules, regulations, procedures, policies, and norms. Third, the attitudes to which knowledge to use and how to behave, whether to comply with rules or rely on "common sense," whether to prioritise own achievements or the group, etc. Learning from experience can be directed at any of these, but the "mechanisms" must be appropriate for the locus.

In learning from experience it is important to separate what is easy to learn from what is meaningful to learn. Experience is often couched in terms of the number or frequency of occurrence of some event or other, usually ones that are negative (accidents, incidents, loss time, etc.). But counting is not the same as learning. In order for a measure to be useful, it must be meaningful, hence refer to a principle, a model, or some king of conceptual basis. While compiling extensive accident statistics may seem impressive it is not tantamount to learning and it does not mean that the system actually learns anything. Knowing how many accidents have occurred says nothing about why they have occurred, nor anything about the many situations when accidents did not occur. And without knowing *why* accidents occur, as well as knowing why they do *not* occur, it is impossible to propose effective ways to improve safety.

The difference between resilience engineering and the traditional view on safety can be summarised by looking at how the three questions above should be approached.

• A resilient system tries to understand how it functions, not just how it fails. Resilience is the ability to sustain normal functioning, not just to prevent failures. A resilient system should therefore not limit learning to specific categories of events and certainly not to failures rather than successes.
• A resilient system does not limit descriptions of events to their causes, as in the classical approach. Instead of looking for relations between causes and effects, resilience engineering looks for dependencies among functions and for the typical or representative variability of functions.
• In a resilient system, learning should be continuous rather than discrete, and should be driven by a plan or strategy rather than by events. One way of facilitating that is to try to learn from everyday situations and not just from situations where something has gone wrong. Indeed, if the focus is to learn from situations that turn out right, then learning will almost automatically become continuous. Learning from experience should also cover different spans of time. The lessons to be learned from short term changes are not the same as the lessons to be learned from long term trends, neither statistically nor causally.

Finally, that which already has been learned should be revisited and revised because learning in itself will change the basis for learning and improve analysis methods. Lessons learned are never facts, they are interpretations that may have been valid when they were made, but where the validity is not guaranteed to last forever.

How To Engineer Resilience

If a resilient system is to be able to pay attention to the actual, the critical, the potential, and the factual, an obvious question is how this can be brought about. This is really the question of how resilience can be engineered or the question of what resilience engineering is in practice. While a detailed answer cannot be given here, a start will be made by considering each of the four cornerstones from a more operational perspective. This will give rise to a number of issues that in turn can serve as the starting point for more concrete measures.

• In order to address *the actual*, in order to know what to do, a system must have a clearly defined set of events to which it is ready to respond. So one step towards resilience is to develop or produce this set in a systematic manner. It is necessary to know why events are included in the set, both to be able to develop effective responses and in order to judge whether the events are still relevant. Failing to do that the system may waste efforts in being prepared for events that should be of no concern, at the same time as it may be unable to respond to events that should be of concern. A second issue is how the readiness is established, i.e., how effective responses are formulated and how they are verified or ensured. A third issue is how the readiness is maintained. Keeping a system in a state of readiness is essential but costly. The resources needed may be manpower (e.g., staff on stand-by), knowledge (training and requalification), materials (energy, mass, and information), etc. Maintaining readiness is not just a technical but also a management issue, and should therefore be addressed explicitly at the appropriate levels. The failure to verify and maintain an existing response capability is one of the ways in which latent conditions can arise.

• In order to address the *critical*, in order to know what to look for, the most important thing is a set of valid and reliable indicators. One question is how to define these indicators. The best solution is to base indicators on an articulated model of the critical processes of the system. Such models are, however, only feasible for pure technological systems. Another, more common, solution is to choose indicators that correspond to a tradition within an organisation or a field of activity. A third solution, to choose indicators only because everyone else seems to use them ('*cosi fan tutte*'), should be avoided. A second question is how often this list is revised, and on what grounds. There should be clear guidelines for how to revise the indicators, how often, and on which basis. Quite often a revision takes place when something unexpected has happened, i.e., when the indicators have failed. But such a reaction is inappropriate both because it is unreasonable to expect the indicators to be complete and foretell everything, and because the revision will be hasty and superficial, putting more weight on face validity than content validity. A third question, already mentioned, is whether the indicators are leading or lagging, where leading indicators clearly are to be preferred. A fourth question is how measurements actually are made. Since most indicators will refer to some kind of aggregated measure, combining data sources of different quality, it is also here important that the rules and criteria are clear. A fifth question is whether the measurements refer to transient or stable changes, where the latter obviously is to be preferred. There should therefore be some way to determine whether a measured change is transient or stable.

• In looking at the *potential*, in looking towards the future, the most important issue is probably what the model of the future is. In other words, what are the assumptions used to consider long term developments? The simplest assumption is that the future will be a repetition of the past, i.e., that one should look out for a recurrence of past events, perhaps embellished with some degree of uncertainty. A less simple-minded assumption is that what can potentially happen can be found by an extrapolation of the past. This may even be developed into a formal model of the past that is used to calculate the future; most risk models fall within that category. A more realistic assumption is that what can potentially happen will be an emergent rather than a resultant phenomenon because the systems we deal with are only "nearly decomposable" (Simon, 1962). This means that every component of the system has a direct or indirect interaction with, in principle, every other component. Looking into the future must therefore be based on methods that go beyond cause-effect relations. A final issue is that looking at the potential in itself requires taking a risk, in the sense that it may lead to an investment in something that is not certain to happen. This again means that it is a management (blunt end) issue as much as an operational (sharp end) issue and that it should be treated as such.

• Finally, in looking at the *factual*, in trying to learn from the past, it is important to learn from successes as well as from failures. Successes are not just the near-misses or the spontaneous recoveries, but rather the normal functioning. If the focus is on accidents and adverse events, it means that only 1 out of 10.000 – or even 1 out of 100.000 – events will be considered. This is an enormous waste of opportunity unless, of course, it is assumed that successes and failures are the result of different underlying processes so that there is nothing to learn from the former. Resilience engineering strongly rejects this assumption. In consequence of that, leaning should be continuous rather than discrete. It is of course not feasible to try to learn from every event or every situation, both because it will impede productive work and because many of them are highly similar. But learning should follow a regular scheme rather than be part of the reaction when something goes wrong. Learning should also be both qualitative and quantitative. Quite apart from the fact that quantification is impossible without a prior qualitative analysis, more is usually learned by understanding what went on than by tallying specific outcome types, such as counting 'human errors.' A qualitative lesson will also be easier to communicate that numbers orstatistics. Finally, learning should improve both individual and institutionalized knowledge.

The focus on the issues arising from each of the four cornerstones demonstrate how it is possible to think about resilience engineering in in a practical manner. Starting from the level of the system as a whole this soon leads to the development of operational details and specific steps to be taken on a concrete level. This can, however, only be done by referring to a specific domain or field of activity, or even to a specific organization at a certain point in time. Much of that may obviously make use of existing methods and techniques, although seen from a resilience perspective and in some cases supplemented by new methods and techniques. For any given domain or organization it will also be necessary to determine the relative weight or importance of the four main abilities, i.e., how much of each is needed. The right proportion cannot be determined analytically, but must be based on expert knowledge of the system under considerations and with due consideration of the characteristics of the core business. Yet the minimum requirement is that none of them can be left out if a system wants to call itself resilient.

References

Adamski, A. & Westrum, R. (2003). Requisite imagination. The fine art of anticipating what might go wrong. In E. Hollnagel (Ed.), *Handbook of cognitive task design* (pp. 193-220). Mahwah, NJ: Lawrence Erlbaum Associates.

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

Amalberti, R. (2006). Optimum system safety and optimum system resilience: Agonistic or antagonistic concepts? In E. Hollnagel, D. D. Woods & N. G. Leveson (Eds.), *Resilience engineering: Concepts and precepts* (p. 253-271). Aldershot, UK: Ashgate.

Barnett, A., & Wang, A. (2000, April). Passenger mortality risk estimates provide perspectives about flight safety. *Flight Safety Digest, 19*(4), 1-12. Washington, DC: Flight Safety Foundation.

Comfort, L. K. & Haase, T. W. (2006). Communication, coherence and collective action: the impact of Hurricane Katrina on communications infrastructure. *Public Works Management & Policy*, 11(1), 6-16.

Cook, R. I. (2006). Being bumpable. In D. D. Woods & E. Hollnagel, *Joint cognitive systems: Patterns in cognitive systems engineering.* Boca Raton, FL: CRC Press, Francis & Taylor.

Cook, R. I. & Nemeth, C. (2006). Taking things in one's stride: Cognitive features of two resilient performances. In Hollnagel, E., Woods, D. D. & Leveson, N. (Eds.), *Resilience engineering: Concepts and precepts.* Aldershot, UK: Ahsgate.

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. & Woods, D. D. (1999). To intervene or not to intervene: The dilemma of management by exception. *Cognition, Technology & Work*, *1*(2), 86-96.

Dutch Safety Board (1999). *Final report 97-75/A-26, PH-TKC Boeing 757, 24 December 1997 Amsterdam Airport Schiphol.* The Hague, NL: Author.

Es, G. W. H. van, Geest, P. J. van der, & Nieuwpoort, T. M. H. (2001). *Safety aspects of aircraft operations in crosswind (NLR-TP-2001-217).* Amsterdam, NL: National Aerospace Laboratory NLR.

Hollnagel, E. (2004). *Barriers and accident prevention.* Aldershot, UK: Ashgate Publishing Co.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method.* London, UK: Elsevier.

Hollnagel, E. (2004). *Barriers and accident prevention.* Aldershot, UK: Ashgate.

Hollnagel, E. (2008a). Investigation as an impediment to learning. In: E. Hollnagel, C. P. Nemeth & S. Dekker, S. (Eds.), *Remaining sensitive to the possibility of failure.* Aldershot, UK: Ashgate.

Hollnagel, E. (2008b). *From protection to resilience: Changing views on how to achieve safety.* Proceedings of the 8th International Symposium of the Australian Aviation

Psychology Association, April 8-11, Sydney, Australia.

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

INSAG (1995). *Defence in depth in nuclear safety* (INSAG-10). Vienna: International Atomic Energy Agency.

Jagacinski, R. J., & Flach, J. M. (2002). *Control theory for humans: Quantitative approaches to modeling performance*. Mahwah, NJ: Lawrence Erlbaum Associates.

Klein, G. A., Orasanu, J., and Calderwood, R. (Eds.) (1993). *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex.

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. (2002). *System safety engineering: Back to the future*. Boston: MIT Aeronautics and Astronautics.

National Transportation Safety Board. (1984). *Eastern Air Lines Lockheed L-1011, N334EA Miami International Airport, FL, 5/5/83. Report no. AAR 84/04,* Springfield, VA: National Technical Information Service.

Nelson, P. S. (2008). *STAMP Analysis of the Lexington Comair 5191 accident*. Lund University, Sweden: Unpublished MSc thesis.

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

Petroski H, 2000. Vanities of the Bonfire. *American Scientist* 88:486-490.

Pew, R. W. , Miller, D. C. and Feehrer, C. E. (1981). *Evaluation of proposed control room improvements through analysis of critical operator decisions*. Palo Alto, CA: Electric Power Research Institute NP-1982.

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science, 34*, 15-30.

Rasmussen, J. (1986). *Information processing and human-machine interaction: An approach to cognitive engineering*. New York: North-Holland.

Rasmussen, J. (1997). Risk management in a dynamic society: A modeling problem. *Safety Science, 27*(2/3), 183-213.

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

Reason, J. (1993). The identification of latent organizational failures in complex systems. In J. A. Wise, V. D. Hopkin and P. Stager (Eds.), *Verification and Validation of Complex Systems: Human Factors Issues*. Springer-Verlag: Berlin. NATO ASI Series.

Reason, J. (1997). *Managing the risks of organizational Accidents*. Aldershot, UK: Ashgate Publishing Co.

Reason, J. T., Hollnagel, E., & Pariès, J. (2006). *Revisiting the "Swiss Cheese" model of accidents (EEC Note No. 13/06)*. Brussels: Eurocontrol.

Rochlin, G., LaPorte, T. R. and Roberts, K. H. (1987). The self-designing high reliability organization: Aircraft carrier flight operations at sea. *Naval War College Review, (Autumn)*, 76-90.

Rochlin, G. (1991). Iran Air Flight 655 and the USS Vincennes. In LaPorte, T. (Ed.), *Social responses to large technical systems*. The Netherlands: Kluwer Academic.

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.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K., & Herrera, I. A. (2004). *Organisational accidents and resilient organizations: Five perspectives (Revision 1), Report no. STF38 A 04403*. Trondheim, Norway: SINTEF Industrial Management.

Sampson, J. (2000). The accepted airmanship standard is the stabilized approach. *Air Safety Week*, 13 November 2000.

Simon, H. A. (1962). The architecture of complexity. *Proceedings of the American Philosophical Society*, *106*(6), 467-482.

Turner, B. A. (1978). *Man-Made Disasters*. London: Wykeham.

Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*, 1124-1131.

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

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

Weick, K. E. (1990): The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management, 16* (3), 571-593.

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

Weick, K. E. and Roberts, K. H. (1993). Collective mind and organizational reliability: The case of flight operations on an aircraft carrier deck. *Administration Science Quarterly, 38*, 357--381.

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

Westrum, R. (1993). Cultures with requisite imagination. In J. A. Wise, V. D. Hopkin and P. Stager (Eds.), *Verification and validation of complex systems: Human factors issues*. Springer-Verlag: Berlin. NATO ASI Series.

Westrum, R. (2006). A typology of resilience situations. In E. Hollnagel, D. D. Woods & N. Leveson (Eds.) *Resilience engineering. Concepts and precepts*. Ashgate: Aldershot, UK

Appendix: Scientific production of the project

The scientific production that has flowed out of the Resilience project has become significant and wide-spread across multiple application domains (e.g. aviation, healthcare, processing industry). Publications range from peer-reviewed journal articles to book chapters, to edited books, and cover a number of the domains empirically studied for this project. This range of publications has allowed us to reach different audiences with the results of this project:

Hollnagel, E., Nemeth, C., & Dekker, S. W. A. (Eds.) (2009). *Resilience Engineering: Preparation and restoration.* Aldershot, UK: Ashgate Publishing Co. In press.

Hollnagel, E. (2008). The cost of safety: As high as reasonably practicable?. *6th International Conference on Occupational Risk Prevention.* A Coruna, Spain.

Hollnagel, E. (2008). Critical information infrastructures: Should models represent structures or functions? *Lectures notes in computer science: Computer safety, reliability, and security.* Berlin /Heidelberg: Springer. (pp 1-4)

Hollnagel, E., Pruchnicki, S., Woltjer, R. & Etcher, S. (2008). Analysis of Comair flight 5191 with the functional resonance accident model. *8th International Symposium of the Australian Aviation Psychology Association Sydney, Australia*

Hollnagel, E. (2008). From protection to resilience: Changing views on how to achieve safety. *8th International Symposium of the Australian Aviation Psychology Association Sydney, Australia.*

Hollnagel, E., Nemeth, C., & Dekker, S. W. A. (Eds.) (2008). *Resilience Engineering: Remaining sensitive to the possibility of failure.* Aldershot, UK: Ashgate Publishing Co.

Nijhof, M., & Dekker, S. W. A. (In press). Restoration through preparation, is it possible? Analysis of a low-probability/high-consequence event. In, C. Nemeth (Ed.) *Resilience Engineering: Preparation and restoration.* Aldershot, UK: Ashgate Publishing Co.

Hollnagel, E. (2008). Safety management – looking back or looking forward. In, E. Hollnagel, C. Nemeth, & S. W. A. Dekker (Eds.). *Resilience Engineering: Remaining sensitive to the possibility of failure.* Aldershot, UK: Ashgate Publishing Co.

Dekker, S. W. A. (2008). Risky business or resilient business? Paper presented at *Risky Business: An International Patient Safety Conference.* Great Ormond Street Childrens Hospital, London UK, 16 May 2008.

Huber, S., van Wijgerden, I. J., de Witt, A., & Dekker, S. W. A. (submitted). Learning from organizational incidents: Resilience engineering for high-risk process environments. *Process Safety Progress.* Manuscript under review.

Van Winsen, R., Dahlström, N., Dekker, S. W. A., & Nyce, J. M. (submitted). "Rule- and Role-Retreat: An Empirical Study of Procedures and Resilience. *Journal of Cognitive Engineering and Decision Making.* Manuscript under review.

Dekker S. W. A., Jonsén, M., Bergström, J., & Dahlström N. (submitted). Learning from failures in emergency response: Two empirical studies. *Journal of Emergency Management*. Manuscript under review.

Dahlström N., van Winsen, R., Dekker S. W. A., & Nyce, J. M. (submitted). Regimes of control and resilience in escalating situations. *Safety Science Monitor*. Manuscript under review.

Dekker, S. W. A. (2008). Reporting and investigating events. In: P. Croskerry, K. Cosby, & R. Wears (2008). *Patient safety in emergency medicine*. Philadelphia, PA: Lippincott, Williams & Wilkins.

Cook, R. I., Nemeth, C., & Dekker S. W. A. (2008). What went wrong at the Beatson Oncology Centre? In: In: E. Hollnagel, C. Nemeth, & S. W. A. Dekker (Eds.) (2008). *Resilience Engineering Perspectives: Remaining sensitive to the possibility of failure*. Aldershot, UK: Ashgate Publishing Co.

Dekker, S. W. A., Dahlström, N., van Winsen, R., & Nyce, J. M. (2008). Crew resilience and simulator training in aviation. In: E. Hollnagel, C. Nemeth, & S. W. A. Dekker (Eds.). *Resilience Engineering Perspectives: Remaining sensitive to the possibility of failure*. Aldershot, UK: Ashgate Publishing Co.

Amer-Wåhlin, I., & Dekker, S. W. A. (2008). Fetal monitoring: A risky business for the unborn and the personnel. *Journal of Obstetrics and Gynaecology*, in press.

Dekker, S. W. A. (2008). Into thin air. In: Houle, T. (Ed). *Crew Resource Management*. In press.

Dekker, S. W. A., & Lundström, J. T. (2007). From threat and error management (TEM) to resilience. *Human Factors and Aerospace Safety, 6*(3), 261-274.

Dekker, S. W. A. & Laursen, T. (2007). From punitive action to confidential reporting: A longitudinal study of organizational learning. *Patient Safety & Quality Healthcare,* 5, 50-56.