Resilience in the Aviation System

Antonio Chialastri[1] and Simone Pozzi[2,3]

[1] Aviation Lab, Rome, Italy
[2] Deep Blue srl, Rome, Italy
[3] Sapienza University of Rome, Department of Psychology of Social and Developmental Processes, Rome, Italy
anto.chialastri@tiscali.it, simone.pozzi@gmail.com

Abstract. This paper presents an overview of the main characteristics of the civil aviation domain and their relation with concepts coming from the approach of resilience engineering. Our objective is to first outline the structural properties of the aviation domain (i.e. regulations, standards, relationships among the various actors, system dynamics), to then present some example processes that bear an effect on the system resilience. We will in particular reason on training and on the role of automation, to discuss how and to what extent they impact on system resilience. We contend that, in a complex system like aviation, resilience engineering is not a matter of simple technical upgrades, rather is about facing contradictory tensions and dynamic system changes. This paper contains a pilot's first-hand reflections, so it aims to stimulate discussion on some issues that are still open, rather than providing solutions.

1 Introduction

Given the unbearable human, economical and legal impact of an air disaster, safety has always been the main concern for airline management. However, technological innovation like the introduction of the so-called glass cockpits in the beginning of the Nineties has questioned well-established safety management methods, calling for the adoption of new safety models. For instance, Leveson [1] mentions how reductionist approaches, which derive the whole system safety from ensuring that each single component is safe, fail to appreciate the systemic dimension of safety. Traditional Probabilistic Risk Assessment focuses on functional failures, i.e. on the non-performance or inability of specific components to perform their intended functions. However the more complex safety critical systems have become, the more accidents have been determined by so-called *dysfunctional interactions*. *Dysfunctional interactions* take place when system elements perform as they are expected (i.e. as specified by requirements) but still the overall system behaviour is unsafe. The increasing role of human and software in supervisory control addresses this issue, as it is quite common to have situations in which a component satisfies its specified requirements, even though the requirements may include behaviour that is undesirable from a larger system context.

A coherent approach with the points raised by Leveson comes from Resilience Engineering [2, 3]. Whereas conventional risk management approaches are based on

M.D. Harrison and M.-A. Sujan (Eds.): SAFECOMP 2008, LNCS 5219, pp. 86–98, 2008.

hindsight and emphasize failure probabilities, Resilience Engineering aims to enhance the ability of organizations to create processes that are robust yet flexible, that can use resources proactively to accommodate for external disruptions or internal ones (e.g. production pressures, human errors). In Resilience Engineering, failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent failure to adapt to the real world complexity. Resilience engineering focuses on the capabilities on all levels of a system to respond to regular and irregular threats in a robust yet flexible manner, and to anticipate the consequences of disruptions. However, all systems to some extent adapt to changes, even if this adaptation might be slow or not apparent. Robustness is provided by specified structures inside the organizations that should respond to intentional attacks or unintentional mishaps, while flexibility is achieved by stretching normal behaviors to cope with situation not previously codified.

Resilience engineering refers to a broader definition of adaptation, whether the system can handle variations that fall outside of the co-called design envelop, that is the variance amplitude as defined in that system. The system should be "designed-for-uncertainties, which defines a 'textbook' performance envelope and how a system recognizes when situations challenge or fall outside that envelope – unanticipated variability or perturbations" [2].

Individuals and organizations 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 organizations to anticipate the changing shape of risk before damage occurs; failure is simply the temporary or permanent absence of that.

Given these definitions of resilience engineering, some problems arise regarding the scope of their applicability in aviation.

According to Erik Hollnagel: "*Safety is something a system or an organisation does, rather than something a system or an organisation has. […] This creates the dilemma that safety is shown more by the absence of certain events – namely accidents – than by the presence of something. Indeed, the occurrence of an unwanted event need not mean that safety as such has failed, but could equally well be due to the fact that safety is never complete or absolute*" [2]. Which begs the question of which is the correct approach to safey in a system such as aviation. The answer depends on how we see the entire system. Fifty years ago, when a reductionist paradigm was dominant, the answer was that safety could be achieved via the engineering approach, by improving onboard technologies. Everything was measurable, predictable, modelled in different shapes to fit for the special field of application. During the eighties, the answer to the same question shifted from engineering to psychology. Following several accidents, due to poor human interaction, the goal was to improve the "liveware" part of the system. Technology was considered safe, while man was not. Today, we recognize that in complex systems we cannot isolate single causes, since every element is interconnected with the other elements.

The approach we propose in this paper is to move away from reductionism and take a philosophical perspective on system dynamics and to address one of the key contradictions at the core of the resilience engineering approach. On the one hand, most of the authors acknowledge that a complex system cannot be reduced to the sum

of single components and are aware of the role played by emergent properties. On the other hand, we need to have better engineering principles, that can be applied by industries. Resilience and engineering do not match. Numbers, graphics and models may give more confidence in the manageability of the system and may reduce the uncertainty given by complexity, but they still cannot address emergent properties. In our opinion, this is the key challenge that resilience engineering should tackle.

2 What Is Resilience in Aviation?

Given this explanation of resilience, we must clarify some concepts that could be misleading for the discussion. From a system's theory point of view, accidents are considered as an unexpected combination of events rather than a single failure or action leading to disaster. In a similar manner resilience is the ability to cope with *unexpected* circumstances that could put in jeopardy the whole system. Accidents in aviation, likewise other domains, show very similar and recurrent patterns of events. That is why we are able to categorize types of accidents by their dynamics and by their shared characteristics, e.g. "controlled flight into terrain" or "loss of control". To overemphasise the point for clarity's sake, in most of the accidents we already know every step leading to the negative outcome before they actually start unfolding. Otherwise even with the benefit of hindsight we would not be able to identify the single links of the event's chain.

To recap, aviation resilience is itself a problematic notion to be analysed deeply, not a simple solution to fix organizational latent failures. This leaves us with some open issues. First, how to define aviation resilience. Ability to cope with unexpected events? Robustness towards ambiguity of information? Functional plasticity and structure remodelling, in order to achieve the same result, namely safety? What do we mean by saying that something is unexpected in aviation? Second, which is the appropriate system level for improving resilience? Who are the stakeholders? Shall we concentrate on the final operator (i.e. pilots, air traffic controllers, etc) or on the organisational level or on international institutions (e.g. ICAO, IATA, etc.)

To further our reflection on resilience engineering and the aviation domain, this paper will present some of the characteristics of the aviation domain, to then describe first-line processes and the way they might impact on the system's resilience.

3 The International Nature of Air Transport: Rules and Regulatory Bodies

The aviation industry has been among the first to go global. Its workplace is the world, so it deeply needs international rules to be enforced worldwide. International organisms and national regulators emit a set of rules regarding the air transport. An airline must comply with the "Airworthiness of operation certificate" criteria. Another institution that sets worldwide rules is the ICAO (International Civil Aviation Organization) agency of the United Nations, who emits, among others, regulations regarding flight procedures (i.e. setting the criteria on the design of instrument approach). The IATA (International Airline Transport Association) is responsible of the rules for passengers and good transportation.

We must mention as well the international agreement signed following some international conference as in Chicago (1944), where the States issued an agreement to create ICAO, together with a series of documents also know as *technical annex*. At the moment, 18 annexes have been issued regulating several aspects of international flight.

From then on, other conventions took place, in Tokyo, in Montreal, and so on.

The United States, the cradle of the aviation industry and the commercial flight on a large scale, often set the pace of air regulation, regulation that is later adopted worldwide. The FAA (Federal Aviation Administration) emitted in the early days of flight a set of rules regarding airplane's manufacturers, pilot training, hiring and scheduling, maintenance action and so forth, in order to guarantee the system reliability to customers and workers in every country adopting those rules. Today, another super-national regulator, the JAA (Joint Aviation Authority) issues its own rules for an European Standard to be applied to airplanes and aircrew flying in Europe.

National regulators should comply with international rules and should implement also other safety measures to ensure safe, smooth and orderly flight operations, They should also take the role of the "system watchdog" whenever required. For this reason, some flight rules are still derived from national legislations, which may sometimes be outdated. For instance, as recently as in 1995, in Italy flight was regulated by the old "Navigation Code", issued some sixty years ago (30/3/1942), thus applying the same measures to ships and airplanes. National legislations is sometimes outdated compared to international rules, because aviation still defines most of its rules and standards at a transnational level. This requires national legislations to quickly comply with international standards, which is not always easily done in the appropriate time frame.

3.1 Main Actors

Having covered the regulatory bodies that set worldwide rules for air transport, we can now move to the core business's actors of air industry and how they interact. Main actors are the manufacturers (i.e. Boeing, Airbus, etc), the operators (airlines, charter companies, cargo, and so on), crews, and auxiliary services. Each actor faces its own peculiar safety challenges and has its own responsibilities.

The *manufacturer* builds a new airplane, according to the rules, and after the flight tests, it sells the aircraft with the relative operation manual to the airline (the operator). The manufacturer usually provides the following information:

- system's limitation
- check list for normal, abnormal and emergency situations
- conditional procedures (a non-routine, but non-dangerous procedures)
- special operation (operation with degraded performance depending either on systems or environment)
- performance tables, including engine(s) out performance
- loading
- MEL (minimum equipment list) enabling the crew to fly with inoperative devices until home base where the repair is made according to a schedule (this deviation must be previously approved by national regulator)

– runways tables that indicate the performances the aircraft can develop on the specified runway: i.e. the maximum weight allowed during takeoff or the flight path to be followed in case of engine failure soon after take off.

The *operator* buys the airplane and plans its operating schedule. In addition to the manufacturer's manual, every major airline provides the crew with rules of conduct either on ground or in flight. This is called *General basic*, and specifies almost every aspects of the crew members' working life.

The *crew* flies according to the national and international rules and laws, it must comply with the procedures specified in the operation manual (i.e. the manufacturer's manual) and the guidelines set by the operator (i.e. airline).

Auxiliary services to air travel include: air traffic management, airport services (catering, fuelling, etc.), maintenance, marketing services. Even if each of these bears a significant effect on aviation resilience, in this paper we will only briefly mention the role of maintenance. Airplane overhauling is regulated by international standards and by strict national rules. Every aircraft should be checked every day, and cyclically after a determined number of flight hours. On the average, airplanes are brought to an hangar every three months to have a complete overhauling, in order to check every system and guarantee safe operations. If the crew experiences any system malfunction during a flight, they file a report. The next flight cannot depart unless the problem has been fixed. Documents proving that the maintenance action has been made are quickly sent to the national regulator who has the right (and duty) of supervision on every repair.

According to Amalberti theory on ultra-safe systems [4] (less than one accident every million take offs), we can point out significant difference in safety records between military and civil flights, and also among civil flights: airline, charter and private flights.

Military flight is made in variable environment that does not allow a strict regulation, leaving room for the pilot to arrange his flight in order to be "combat ready". Often the airplane is flown to its limits, with erosion of the risk margins. Sometimes the enemy is inside the cockpit.

Civil aviation is made of different kind of subjects: airline, charter, private. Airlines are structured in a very organised model that relies on detailed procedures to carry on its activity. Accident rate have been estimated in one accident per ten million take-offs. Crews are trained to comply strictly with these procedures. Charter companies are instead driven by profit in a more aggressive way, so economical pressure on crews could be stronger than in the airlines (estimate rate of accident one per 10^5). Keeping accidents at bay is a serious concern for managers and there is a concrete risk of misperception by employees about the management's real priorities. Private flight are less keen on procedures and mainly relies on pilot's experience, but on the other side, two elements could be critical (the estimated rate of accident is one per 10^4). First, pilots often lack a professional community with whom to share their experience, thus hampering effective proactive learning. Second, maintenance is not often carried out by expert engineers, as maintenance people is hired from big companies on a temporary basis.

4 Resilience between Automation and Training

This section will present some of the processes that the aviation domain has established to increase the resilience of its operations. In the first paragraph, we will outline how pilots are trained to perform with the primary objective of safety. In the second part, we will focus on the role of automation in modern aviation, highlighting a progressive shift in the underlying design philosophy. These two examples will show how resilience engineering is about facing contradictory tensions and dynamic system changes.

4.1 Building a "Safe Crew"

Aviation is a socio-technical system made of men and a variable environment. Everyone working around an airplane plays his role in assuring the final target: safety. In doing so, everyone should be strongly committed to ensure the best performance s/he can in order to avoid a deterioration of safety margins. According to the so-called hologrammatic principle (i.e. every single particle contains the properties of the whole in which it is embedded, e.g. a cell in the human body), in air industry every operator should share the basic approach to safety, since any of her/his action could affect the final result. It is thus crucial to review means and processes that make sure that every operator shares the same approach to safety. Among the main drivers, we may mention training programmes, but also organisational culture and the force of examples.

To tackle this issue, the airline industry adopts a knowledge-based approach to safety, where the system resilience is ensured by appropriate performance at the single operator's level. The result is a bottom up approach to safety in which everyone is strongly committed to safety because s/he shares the same value of the entire organisation. Every area has its own principles and varies from role to role. Selection is very important in hiring pilots, less for ramp agents. Teaching is very important for ramp agents, given their sensitive role in assuring flight balance, less for pilots already hired with a valid license. Given the author's experience, this paper will focus only on the pilot role. The main processes put in place by the aviation industry to ensure a knowledge-based approach are selection, training and checking. In the next part of the paper, we will particularly focus on training.

Selection
Selection is the first "filter" of candidates and it is structured taking into consideration several factors: attitude towards the job, reliability, cognitive skills, social abilities, etc. The performances of the would-be pilots are evaluated by a team made of psychologists, old pilots, managers. The desired profile is set in advance, so that only the suitable candidates are enrolled into the flying school. The other key turning point in a pilot's career is the upgrading to the rank of commander. To achieve this rank, the candidate pilot should be positively assessed by many instructors and check pilots.

Training
Training is a lifelong process that endures till a pilot's retirement. It is based on a series of competences and knowledge pieces, ranging from flying skills, to flight management, to role attitude. Each element is required in the pilot profile. Piloting is

not the sole skill required to be an airline pilot. A pilot also needs to make crucial decisions on the basis of theoretical knowledge, previous experiences, current flight data (which include the present situation, the aircraft status, meteorological conditions). Just like a surgeon, pilots have a strong theoretical knowledge, but they also need experience, which sometimes comes paired with mistakes. Both surgeons and pilots always focus on the same object of operation, a human being for the surgeon and a flight for the pilot, but this object everyday changes in subtle or sharp ways. All the recent technological improvements provide help to carry out simple and repetitive tasks, but in the end a good pilot or a good surgeon are required to exercise their sound judgement to evaluate complex situations, whenever they arise. The core of their profession is the "artfulness of the intelligent worker", that reads reality and puts into connection the single, unique, situations they are living with a set of theoretical tenets.

For instance, if we take the case of procedures, we cannot simply claim they positively contribute to safety. They certainly provide support in routine jobs for smooth, clear, precise operations. However, it is impossible to get a procedure for every aspect of a pilot's job. In a complex environment, threats are too many to be foreseen in advance, thus the safest way to cope with unexpected situation is to provide pilots with the appropriate resources to cope with these variations. Usually a pilot working for an airline is taught to fly well within the safety margins. The safety margins protect the system from technical failures, unexpected circumstances or human errors. But while pilots see the margin area as a buffer over risk, managers tend to see buffers as inefficiencies. While pilots sometimes face the trade-off between money and safety to comply with the company's goals, the managers are oriented to maximize the performances pushing the costs at their lowest edge. To make sure pilots possess the right resources in the right situation, the aviation community has identified four resource categories, also known as the "4 P" approach: Philosophy, Policies, Procedures and Practices.

Philosophy is the guiding principle of airline business. The philosophy of airlines should be *safety first*. Every organizational policy, procedure or practice should be implemented according to this basic principle.

Policies are issued by the management to reach the operational target. They are guidelines concerning a determined area. For instance fuel consumption, given the actual oil cost, is object of a common policy in most of the airline. To minimize fuel consumption a series of measures could be adopted, from avoiding of carrying extra fuel, to requesting air traffic control for higher cruising altitudes, etc.

Procedures details the flow chart required to carry out the user's task. They are designed by the operator (airline) to comply with policies and regulations. They take into consideration several aspects: manufacturer's recommendations on the airplane's management, regulator's criteria on crew composition. In the routine job they ensure a safe and smooth flow of operation.

Practices are what people really do to bridge the gap between procedures and reality demands. There is of course a well known potential mismatch between procedures and practices. Whenever it is impossible to comply with the procedure, the captain has the responsibility to deviate in order to ensure a higher level of safety, in accordance with the philosophy of operations. In these situations, it is essential to

evaluate the attitude towards risk, variable from pilot to pilot according to multiple factors. Such attitude is commonly described as follows:

- risk expectancy: what is the real chance that something happens?
- risk sensitivity: in case something actually happens, which are my effective resources to cope with this new situation?
- risk penalty: which will be the possible consequences in case something actually happens?

For this reason, training programmes include flying skills, flight management skills, role attitudes. Flying skills are the ability to fly an airplane according to basic flight principles, with or without autopilot. They represent the "knowing how-to", cognitive-physical skills on execution tasks requiring coordination of external input perception with actions. This area has a key prominence for a novice pilot, who has to develop familiarity with locating the airplane position in a three-dimensional space and planning/controlling corresponding movements. Flight management skills refer to the ability of managing aircraft systems in order to perform at the requested level of safety. These skills are developed by internalising operating rules and procedures to understand the rationale behind them. In this training phase, pilots should move beyond the mere knowledge of rules to understand how to use rules as resources to ease work and make it safer. Rule should become "safety resources", so that any violation can only be justified if it is clearly required for safety reasons. Role attitudes cover interpersonal skills, like assertiveness, critique, communicativeness, etc.. These are required to perform in coordination with all the crew members, to develop and maintain a shared view on the objectives, to manage the available resources, to handle interpersonal conflicts that might disrupt the team performance. While the former qualities are named technical skills, the latter is a non-technical skill. Leadership, communication, and other non-technical skills can play a major role in many accidents. For instance, a Controlled Flight Into Terrain accident (CFIT) is caused by pilot's misbehaviour or misconduct, as a perfectly efficient airplanes hits an obstacle or overruns the runway end.

Another core area of training programmes deals with error management. Since errors are unavoidable, this area is still an important one, even though state-of-the-art safety literature [5-9] has deeply questioned the assumption that human error causes more than 90% of the accidents. Anyway, pilots are trained in order to be aware of human behaviour in flight. To improve error management, we articulate the training in three levels of error's awareness: avoid, detect, mitigate.

- Avoid: the ability to develop one's own safety net that ensure a smooth, quick and safe way to operate the system. It includes also flight discipline, intended more as a shared value, rather than a rule to comply with.
- Detect: ability in the perception of something deviating from the natural course of action and from intentional input to the system. A key risk area can be found whenever perception does not match the user's expectation, as sometimes expectations can normalise very deviant perception.
- Mitigate: once the deviation is manifest, a quick return to a desired path is a pilot's "must".

Detection can be particularly tricky, as pilots may underestimate a risk on the basis of the lack of negative outcomes in their experience. This phenomenon is commonly known as "drift to danger" [10]. It is an incremental, slow and pervasive attitude toward risk that drives the sharp-end operator to pursue targets even beyond the managers' will. There is, basically, a misperception of the real margin of risk that the organization, as a whole, is ready to accept. This dynamic can be exemplified with a discussion on the fuel policy.[1] Due to the oil price soaring, many airlines are trying to save money, by reducing the fuel consumption. To reach this target, pilots are invited by staff manager to uplift just the minimum fuel required for the flight. Many pilots complied with this policy to eventually find out that they have significantly eroded safety margins, even to a larger extent than they intended to. Recently, there have been several "lack of fuel" emergencies in the United States and in Europe. The CAA (the English regulator) emitted some years ago a recommendation to all crews flying in UK, to consider the right amount of fuel to carry onboard to avoid distress on passengers and special requests to Air Traffic Control units [11]. Even though not every fuel policy critical event is properly detected and reported by crews, there are clear evidences that this area of concern is spreading worldwide, and pilots are struggling between production demands and protection needs. Furthermore, declaring emergency leads to the fear of inter-peers judgement and blaming. A declared emergency with a good functioning aircraft is an ambiguous event, that could be regarded either as a lack of professionalism or as sound judgment. This is a clear example of how economic pressures, organizational climate, raising expectations could impair pilots' day-to-day choices, making the organization unintentionally drift towards the risk area.

Learning in a professional community

The last point we should mention on pilot training is sometimes disregarded, even if it plays a major role in lifelong learning. A pilot should become aware that s/he is part of a professional community, with which s/he can share experiences and discuss problematic issues. Pilots learn from their mistakes, and no pilot can live long enough to commit all the mistakes by her/himself. Pilots see one flight at a time, which does not ensure that they possess an appropriate perception of flight risks. How can a single crew assess if the mistake it has just done is due to poor training, to poor system design or to a coincidence? There are currently no better means to conduct this assessment than by ensuring that the community can openly discuss these events and can share a common interpretation. In this case resilience comes from the cohesion of a community, and not by dynamics strictly related to flight. Though in aviation the informal communication is seen as potentially unsafe, we should point out the paramount importance of peer-to-peer experience sharing, since it provides a valid resource to cope with unexpected events.

Checking programmes

Checking programmes are set by the national and international regulators to define the minimum requirements for licence validation. Big airlines check their pilots on national regulator's behalf.

[1] See "Fuel policy and resilience" by Antonio Chialastri, unpublished manuscript, 2008.

4.2 The Role of Automation: the Tension between Under-Redundancy and Over-Redundancy

About twenty years ago, the air industry, looking for more redundancy in the avionics systems, started introducing automation in flight management. Autopilot and other automatic devices had already been present for some fifty years ago, but that kind of innovation was still guided by the pilots, in the end the final user. The new conception of automation was to provide a whole set of system's redundancies, able to calculate every aspect either of lateral navigation or vertical performances. The pilot was then moved to a monitoring position, rather than being the flight manager. That approach raised questions about the erosion of competence in a pilot (you must know WHAT, not HOW), since the pilot was no longer required to understand the logic of what s/he was using. The basic message was: just use it.

This historical shift in the automation philosophy can be described as a movement from a tactical approach to a strategic one. In the past, every input given to the flight automation (e.g. Flight director, Autopilot, Autothrottle), was immediately visible on a display and pilot's awareness about the mode of automatism was reasonably high. This is called "tactical approach" because input and output were always clear and displayed in cockpit. Nowadays, following the introduction of the Flight Management System (a system that manages and computes several flight aspects in order to minimize pilot's input and provide a protection against flying skills issues, e.g. stall, bank, etc.), a strategic approach is in place. A data (e.g. route deviation, flight level change, etc) inserted now in the computer might be processed hours later, without any displayed information at pilot's reach. If the pilots wants to know which will be the airplane behaviour s/he should review the flight Management System Computer pages.

In the automation case, redundancy is achieved by improving and adding systems in the cockpit, but new risks may arise, as these additional resources contribute to the system resilience only by interacting with human resources, which cannot be considered as a neutral factor. Each situation is exposed to its own peculiar threats. An airplane with few systems (under redundancy) keeps the pilot under stress, fatigue, distraction, information overload, so that workload management is the main area of concern. Such a situation was usual in the middle of 20th century before the introduction of the autopilot, which gave support to pilots during extended operation. Risks were due to flying skills failures, often induced by a too high workload. As automation increasingly supported the pilot's flying skills, the main safety concerns have simply moved to another place. Flight management has become the main risk factor. Over-redundancy has kept the pilot at bay so that s/he lost the basic ability to take over control when needed. Sometimes, pilots cannot understand the system's logic, they lose resources to "fly ahead" of the airplane. Pilots should be a step ahead of the automated flight management system, but as soon as the pilot loses such situation awareness, it should always be possible to revert to basic mode and put back pilot in the position of actually flying the airplane and not merely monitoring automated systems. Nowadays, the primary source of accident has become the *loss of control*, that is the pilot not being able anymore to keep the airplane in a safe flight path. So over-speed, excessive bank angles, stalls, etc, started to show the negative effects of excessive onboard automation. The "erosion of pilot's competence" resulted

in a lack of airmanship, caused by excessive confidence in the flight automation system as the primary resource of flight path and performance management. As a result, few years ago, FAA issued a recommendation to airlines to train pilots *back to basics*, in order to develop the ability to fly regardless of the automated systems.

This discussion shows how in aviation automation often does not increase the margin over risk, instead it keeps the risk ratio constant, allowing the crew (or the system as a whole) to work at the maximum capacity. A similar point comes from the analysis of the development of the instrumental approach to an airport. Ground facilities and onboard receivers allow the pilot to identify the runway to land safely. Before landing s/he must be sure that conditions warrant for a safe approach. It is common, at the operational level, to establish a *decision height* where the crew must positively identify by visual contact the runway and decide if landing is safe or not. If the airplane reaches the *decision height* without getting the runway in sight, the approach must be discontinued. When ground facilities and onboard instruments were not so accurate (i.e. non directional beacon - NDB), the *decision height* was set, say, at 1000 ft above ground and the minimum required visibility was four kilometres. As the technologies improved and the VOR (Very high frequency Omnidirectional Radio) was introduced, the decision height was lowered, say, to 500 ft above ground and the minimum visibility to two kilometres. With the implementation of the Instrument Landing System (ILS – a system that provides the pilot with the correct glide path), the relevant *decision height* was further decreased to 200 ft and minimum visibility required to 600 metres. Nowadays the ILS has been improved to a greater accuracy and the crew may wait 20 ft over the runway before making a decision. That is to say: two eye blinks and you land in the middle of a foggy day with visibility of 125 metres. As we see, gradual introduction of new technologies made the airport operable in almost all weather conditions, but it did not increase safety margins. Safety remained constant, while productivity (operability) of the entire system boosted.

We might discuss other examples, like the introduction of reduced vertical separation minima (RVSM), implemented few years ago, that allowed aircraft flying at cruising level to be spaced vertically of 1000 feet, instead of 2000 feet as before. Even here we see that the system is not safer, but more flight levels become available to let more traffic flow.

This brief excursus shows how resilience engineering is not a matter of simple technical upgrades. We might argue that the introduction of automation has made the 1950 aviation system more resilient (at least under certain conditions), but we would miss the point that automation has also caused the system to change, thus making it more vulnerable to other threats. In a complex system like aviation, resilience engineering is not about increasing the safety level by “solving some issues”, nor by introducing specific technical solutions, rather it should focus on managing changes and studying a problem from various aspects. It should provide the system view, to counter balance excessive specialisation and reductionism.

5 Conclusions

This paper has analysed the aviation system according to the complexity paradigm approach. In doing so, we should drop the old habit used in aviation as far as twenty

years ago to analyse the accident causes: a linear, pre-programmed, highly codified system, made of sub-systems accurately designed by engineers, able to cope with a foreseeable environment. According to this approach, human behaviour is the unique variable, single source of malfunctions leading to disaster. The complexity paradigm invests discipline, from biology to general system theory, to cybernetics, and prompts us not to oversimplify living systems or organization as a whole. It rejects the "standard view" approach based on predictability, verification, measurability, theory of meaning as correspondence, neutral observation, distinction between data and theory. Instead, data are intertwined with theory, observation is never neutral, depending on the observer's light on facts; confutation has replaced verification, and so on.

However, common sense has not followed fully such a paradigm shift. We still see organization as a machine that can be designed, built and checked in every detail, according to the principles of mechanics. For example, in the air industry, quantification is still seen as the main base for decision making. A continuous monitoring activity based on collecting numbers (a huge amount of numbers), followed by scarce analysis and even less synthesis. The loop is not closed with the domain experience, so data remain separated from an overall framework of knowledge.

We have shown in this paper how the concrete mechanisms put in place by the aviation domain to increase its resilience are by far more complex than simple mechanics, as they are multi-faceted, containing inner contradictions and tensions, always developing and subtly changing. Even if we have kept separated the discussion on training and on automation, we eventually have to study the interactions between the two, thus adding further complexity. The lesson we would like to draw from our first-hand experience is that resilience engineering should be a dynamic approach to safety, a never-ending monitoring of the flying activity, which accepts the probable negative outcome and studies all the means to exploit to try and avoid such outcome. An improvement action does not simply fix a safety problem, it also triggers adaptations and interactions. Resilience engineering should be about heightened monitoring of system's changes.

Is it possible to create a model to do it "a priori"? Or should we be satisfied with post-accident analysis that teaches us what went wrong? At the moment, the only sensible answer in aviation is to spread knowledge in order to make people aware of their own behaviour as a single element of the system and as an emergent property, a unique feature, which can contribute to the whole safety. The final question is how to enhance safety via a feed back system that, starting from managers' inputs, collects all the relevant deviation from an ideal centreline accepted as safe. Spontaneous report made by the front line actors (crews, engineers, ramp agents and so on) is vital to detect such a gap between reality and theory. A "no penalty policy" is often endorsed by major airlines in order to encourage people to show their own mistakes, failures in their line operations. At moment this is the only valid approach able to avoid a hidden, and highly dangerous, mismatch between the intended outcome and the actual one.

Acknowledgments. The authors gratefully acknowledge the support provided to this work by the EU project "ReSIST: Resilience for Survivability in IST".

References

1. Leveson, N.G.: A New Accident Model for Engineering Safer Systems. Safety Science 42(4), 237–270 (2004)
2. Hollnagel, E., Woods, D.D., Leveson, N.: Resilience engineering: concepts and precepts. Ashgate, Burlington (2006)
3. Hollnagel, E.: Resilience-The challenge of the unstable. Resilience engineering: concepts and precepts. Ashgate, Aldershot (2006)
4. Amalberti, R.: The paradoxes of almost totally safe transportation systems. Safety Science 37(2-3), 109–126 (2001)
5. Reason, J.T.: Human error. Cambridge University Press, Cambridge (1990)
6. Reason, J.T.: Managing the risks of organizational accidents. Ashgate Publishing Limited, Hampshire (1997)
7. Leveson, N.G.: Safeware. System safety and computers. Addison Wesley Publishing Company, Reading (1995)
8. Dekker, S.: The re-invention of human error. Human Factors and Aerospace Safety 1(3), 247–265 (2001)
9. Dekker, S.: Ten Questions About Human Error: A New View Of Human Factors And System Safety. Lawrence Erlbaum Associates, Mahwah (2005)
10. Dekker, S.: Why we need new accident models. Journal of Human Factors and Aerospace Safety, 2 4(1), 1–18 (in press, 2004)
11. Sindall, T.: Special Objectives Check on air Operator's Fuel Planning Policies. FOCUS on Commercial Aviation Safety 42 (summer, 2000)