Human-centred design in aviation

Antonio Chialastri (anto.chialastri@tiscali.it)
Aviationlab, Rome

Abstract

This paper focuses on the next challenges that, in the near future, ergonomics has to cope with in the aviation domain. After a short excursus, showing the accidents dynamics along the years and pointing out the relative causes, the paper illustrates the difference between two different conception of automation: a generic human (user) friendly versus a specific pilot-friendly concept. This is useful to evaluate the impact on operational life of the introduction of new technologies onboard in the next generation of airplanes. Some case-studies are shown to give an example of the hidden threats, invisible at the design stage, disseminated through the entire innovation process.

Introduction

Since the beginning of flight, Human Factor specialists have striven to improve the environment in which pilots work. Initially, the upgrading of this environment was made following the accidents' investigation. Air safety was then conceived in a reactive mode; ameliorations and improvements were implemented in the entire system only after a severe mishap and were aimed at avoiding similar accidents.

Safety is conceived today in another way, called "proactive approach". This approach aims at avoiding future accidents, preventing mishap with timely interventions on the areas where possible threats lie, even if no accident occurs. The detection of weak signals helps to understand the menaces' nature, to conceive a set of countermeasures in order to achieve a safer system.

Preliminarily, it is essential to point out which is the safety paradigm that includes our point of view. In fact, during the last seventy years, the safety paradigm changed several times and also the actions taken to achieve risk-free systems, even if a zero accident system has never been experienced. Some conceptions will be briefly discussed as the linear conception, the systemic one and the complex ones (normal accident theory, HRO, resilience engineering).

After having set the frame to our discussion, it will be then described the accidents' dynamics in the aviation domain, to show how the accidents' causes shifted along the years and eventually we describe the macro-area which, according to this paper, represents the next challenge for air safety: ergonomics.

Some case studies will be shown to describe accidents really happened, in order to demonstrate the connection between theory and practice in aviation.

Safety paradigms

"If you have a hammer in your hand, every problem will look like a nail". This is assumed to be a Japanese say and it fits well to describe the situation faced by the investigators: in fact, the spectacles that the investigators don, when they analyze an accident, let them see some items, identified as causes, while neglecting others. During the '30's, according to a "way of thinking" influenced by the Neo-positivistic approach orbiting around the "Wien circle", several disciplines adopted a similar approach to investigate their domain. To synthesize the basic assumptions of that period, every theory should ground its thesis on empirical observation, on measurements, using a language that aims to be universal. During the same period, the industrial domain adopted the scientific management, fostered by Frederick Taylor, based on measurement and optimization of the workers' performance. Psychology, as well, saw the dominance of behaviorism, in which the psyche's inner dynamics (called the black box) were disregarded to focus on observable e measurable acts displayed by the behavior. Safety discipline, too, was influenced and the main tool to explain an accident was the "error's chain", developed by Heinrich, to explain how a single event, originated far away, propagates to affect every other system's component as in a "domino effect".

This metaphor hold on until it was replaced by more functional theory, based on different paradigms. In fact, from the '60's on, the linear explanation was subject to harsh criticisms. In philosophy of science, philosopher as Hans Kuhn proposed a different way to explain the scientific revolution as a paradigm shift, based on collective enterprise either in proposing or in accepting new theories. Moreover, the studies of Von Bertalannfy gave a new impulse on the systemic approach that influenced a lot of disciplines, especially in the biological domains. The stress on the collective thinking fostered a series of new approaches, spanning from industrial domain where a new way of management (team work, total quality) emerged. Even the safety science evolved, shifting from an attitude where the single operator bore the blame for the accident (usually the front end operator, the nearer to the final event leading to the mishap), to a more general approach looking at the different stages of the organizations where hidden traps lie, waiting for a trigger to produce the conditions leading to an accident. This is the theory fostered by James Reason, the Swiss Cheese Model, where safety is seen as a result of different stages acting serially to assure freedom from risks. Every organizational level is seen a barrier fit to intercept any dynamics potentially hazardous for the entire system. Since every barrier has a human component inside, it is prone to errors. This structural condition represents a hole (or set of holes) in the barrier, as in a Swiss cheese. From the initial development of the accident dynamics, the error path passes through all these barriers, eventually causing the accident. This is a more general approach, compared to the preceding one ("name and blame approach", focused on people to charge them legally and morally) attributing liabilities at a much higher level, from the political level, to regulators, to the top management, to middle management and then front end operators.

Nevertheless, this paradigm is still systemic but not yet complex.

Complexity is a new paradigm, emerged from late '80's on, following a bare necessity felt by biological sciences (genetics, biology, medicine) where a reductionist approach was insufficient to put under scrutiny thoroughly the domain. One of the main philosophers that convincingly has proposed a new approach based on complexity is Edgar Morin. On his conception, complexity is difficult also to define, but, as a general way of thinking, it has some common characteristics. It refuses the reductionist and engineering approaches, based on an over-simplification of the reality. The level of observation at which we decide to stay, influences our point of view and determines also our tools to investigate the reality and has its own laws, not necessarily applicable at different levels.

Some scientific disciplines are almost "forced" to adopt such an approach, as genetics, but also in the field of management new theories are emerging to improve performances and comprehension of the organizations.

The safety science followed with different theories in competition to explain the dynamics in complex organizations. To comply with the paper' length requested we cite just three approaches: the normal accident theory (proposed by Charles Perrow), the High Reliable Organizations (studied mainly by James Woods) and the Resilience Engineering approach (Erik Hollnagel is one of the most appreciated authors in this field).

Perrow holds that "zero accident" is not achievable, because of the inner nature of complex system. Too many elements in interaction, give way to unpredictable (and sometimes, unmanageable) situations. Since some domains are not completely under control, such as nuclear plants, they should be closed because the damage arising from an accident is by many times higher than benefits we could gain from their use.

Conversely to what is thought to be a pessimistic approach (or just realistic?) the High Reliable Organizations are some empirical examples of how the man made organizations could be substantially risk-free. They are based on professionalism, on a continuous feedback from the operational levels that is capitalize from top and middle managements. Experience is highly considered as the communication between peers to exchange points of view and to share knowledge. Awareness of an accident is so high that everyone is sincerely committed to safety. Woods studied some organizations revealing that the "safe mentality" is pivotal in assuring a low (if none) rate of accidents. On the contrary to the common say: "No new is good news" these organizations rely on the assumption that "No news is bad news" and when no weak signals of pathogen elements present in the whole system are detected, the management strive to (and push the operational levels) to scrutinize in a deeper way.

Last but not least, we mention the resilience engineering approach. It conceives a safe system as the one who can cope with unexpected events. It has to adapt itself in a flexible and still robust way to respond reliably to the challenge given by a complex system.

Man, in this conception, is not the flaw in the system, but is the main resource to assure flexibility, acting as an intelligent part of the system.

The safety conception assumed in this paper is grounded on the resilience engineering point of view.

In fact, aviation is a complex system in which men, equipments and environment interact. Every of these element is complex in itself.

How should we approach the safety system in aviation, then?

A brief history of accidents

(Graphic's explanation: decades on the x-axis, accidents per million take-offs on the y-axis. Source: Flight Safety Foundation)

Most of the corrections to existing systems or procedures, in aviation, were introduced following severe mishaps. So the path of the entire industry has been a kind of "trial and response" dynamics: innovation, mishaps, correction. According to the statistics, the human error has played a pivotal role in the accidents, with a higher rate, compared with other factors as environment (meteorological conditions, Air traffic that induces mid-air collision, and so on), mechanics (i.e.: structural limit exceeded, poor cockpit design) security (high-jacking, bomb onboard, etc.).

Starting from the '40's, investigators wondered why airplanes crash. Taken for granted that the pilots were the fallible factor in the entire system, someone started to analyze "why" pilots did so many errors. At the beginning, till the mid '50's, the main cause of accident was identified as "Loss of control". This category includes situations in which pilots lost the airplane control such as: reaching (and exceeding) the structural limits, conditions in which the airplane stalls, overbanks or experiences an unusual attitude that put in jeopardize the flight progress. The root cause of lost of control spanned from fatigue, to distraction, to excessive workload, to sleepiness, and so on. Briefly, the problem was identified in the main area of "human performances and limitations".

The solution thought to fix this kind of problems was the engineering, to provide more systems, more aids and more technology.

The technological approach focused on two sides: innovation of ground-based aids and implementation of new instruments onboard.

On the first side, two main innovations were provided:

- the air traffic controllers were equipped with radars to monitor the airplanes approaching the airports and;
- the installation of ground based equipments such as ILS (Instrumental Landing System) gave a strong help to pilots in order to land as precisely as possible.

On the other side, namely the introduction of new technologies onboard of the airplanes, the introduction of auto-pilot, auto-throttle, flight director, helped to:

- lower the workload, when too much attention was needed to carry on the task, or;
- relief the pilot from monitor boring activities, reducing duties related to monotonous operations.

The effects of these innovations were successful, since the rate of accident sharply dropped. Nevertheless, during the '70's the accident rate started to rise again, but with a different dynamics. In fact, the main cause of accident shifted from "Loss of Control" to CFIT (Controlled Flight Into Terrain). In this kind of dynamics, a perfectly efficient airplane hit an obstacle in the nearby of the airport when full in control of the crew. Furthermore, we have to consider that most of the accidents happen during the approach phase. The investigations revealed that a poor decision making, a loss in the situational awareness, a conflict (open or concealed) was in progress between the pilots. In short, there was a problem in the human interaction onboard.

This time the solution didn't pass through technology, but applying a new approach, based on psychological assumptions on what is thought to be a good team work. We should mention that, on that period, other new technologies were introduced in the aviation system, but it is generally assumed that the psychological approach was pivotal in improving the system's safety. Courses of CRM (Crew Resource Management) were implemented in most of the main airlines to enhance the interaction between the pilots (and, later, also between the entire crew, cabin attendants included).

The accident curve dropped again, but during the '90's it raised again, even if in a smaller magnitude compared with the past decades. The problem is that the overall dimension of the air transport, nowadays, has inflated in the last decades and even a small amount of accidents (lower than in any other transportation domain such as roads, railway, sea, etc.) could be unbearable for some reasons. Firstly, the human, legal and economic cost of an accident is huge and could destroy an airline's stability, leading it out of the economic contest. Secondly, an air accident has a worldwide resonance and could distort the real perception of air safety in the public opinion.

Whatever the consequences of air mishaps, it is essential to understand why they keep on happening. During the '90's, the main cause of accident shifted once again, as a pendulum, swinging back to "Loss of control", but in a different shape, compared to the one experienced during the '50's. In fact, today the pilots have so many technological aids that is hard to conceive how they can lose the control of the airplane. Actually, the implementation of so many systems is the consequence of the engineering approach to safety in which the pilots are seen as the weak ring in the industrial chain. So, automatisms are intended to substitute many functions played usually by pilots.

There is a widespread opinion among authors studying human factor in aviation that in this case we may talk about "over-redundancy": too many instruments induce a low workload that could provoke complacency, inadequate training make the pilots unable to override the automatisms in case of their failure or misbehavior.

Case studies

Here are briefly presented two case studies illustrating the relationship between pilots and technology: one related to the misuse of instruments by pilots induced by a poor designed system and the unpredictability of a system behavior when in the real operational context.

The first case involved an Airbus A-321 operated by Air Inter who crashed in Strasbourg after the captain misunderstood the descent profile usability because of the similarity between the flight path angle function and the vertical speed function. In fact, both were displayed via a two digits figure in the same feed back window. For instance, 3.3 could represent either a vertical speed of 3300 feet per minute or 3.3 degrees of vertical path. The captain selected 3.3 being sure to descent with a vertical path selected, while he was descending with 3300 feet per minute, a much steeper path than the desired one. The approach was conducted among high terrain around the airport and such an error gave the crew no way out to recover timely. After that disaster, the display onboard was changed and now there is no way to misunderstand similar functions during the approach phase. Furthermore, after the accident the French authority requested, as mandatory, the installation of the GPWS (Ground Proximity Warning System), which warns the crew in case of excessive approach rate to the ground. It is designed to avoid unintentional collision with obstacle, when not in landing configuration. Today this apparatus has been improved, becoming EGPWS, which is linked to the satellite indication. This allows the system to realize if the low altitude is consistent with the airport location and with obstacles scattered in its vicinity. All the relevant information are displayed to the pilots, who immediately could be aware of the presence of mountainous terrain close to the aircraft position.

The second case involved an A-300 approaching Miami. Due to bad weather around the airport the crew expected to enter an area of turbulence. The crew was instructed to hold over a radio-facility. During the descent, with engine at idle thrust, the auto-throttle (managing the engine thrust, via an automatic movement of the throttle governing the necessary thrust) disengaged with no evident signal displayed to the crew. In the proximity of the holding pattern, the airplane leveled-off, reducing its speed well below the minimum required to sustain the flight. During the initial turn in the holding pattern, the airplane stalled, down-spiraling and losing about three thousand feet. This is a very serious condition for a wide-body aircraft. While spiraling downward, the crew lost all the attitude indications for few seconds, that looked (according to the captain, interviewed after the incident) an eternity. In fact, the only useful instruments in such a situation are the attitude and the speed indicator. The attitude indicator was, by design, conceived to go blank in case of oscillations exceeding some amplitude and frequency. This assumption, made at the design phase, comes from the idea that such oscillations are very unlikely in the airline flight. Reality, alas, is much more unpredictable than the engineer's fantasy.

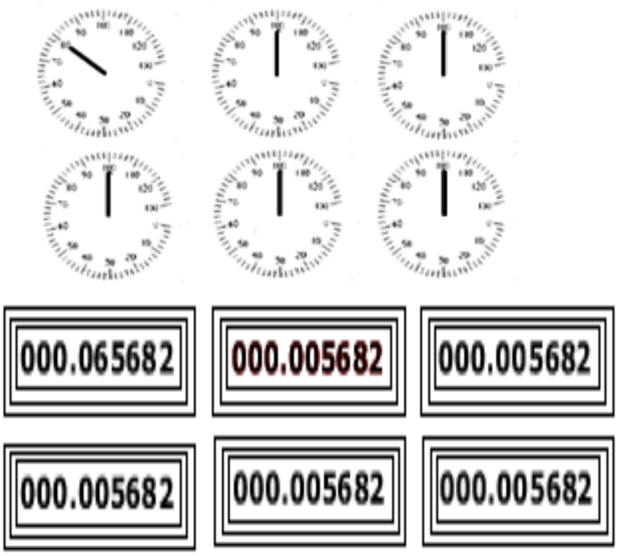
Human factor and technology

There are different conceptions of Ergonomics, as emerges from the evolution of the discipline along the years. Initially, ergonomics was conceived as corrective ergonomics: expert tried to understand how to make system better, after the misuse of something badly designed.

Here it is an example: the design of an airplane with variable wings. In the engineer's mind, it was quite simple to conceive an airplane with variable wings, setting them from straight wings to swept wings. Actually, the straight wings are used at low speed, whilst the swept wings are useful at high speed. To one person observing an airplane is intuitive to understand how to imagine the command lever to change the wings configuration: putting the lever forward, you get straight wings, if you put the lever backward, you get swept wings. It looked quite simple, but some accidents happened cause by pilots' misuse of the command lever. In fact, for a pilot's point of view, every action linked to the idea of speed leads him to move forward: increasing the thrust? Throttle forward. Increasing the speed in case of sudden loss? Pitch down, putting the yoke forward. So when the new system was implemented, a lot of pilots misused it, following their mental pattern related to the speed.

Nowadays, human factor experts are involved at early stage in the design process, to keep the system user friendly. Actually, what is required is the expertise of someone who can translate an engineering necessity in an operational suitable system. Let's think about the number display onboard.

According to the Gestalt principles, human mind is more concerned about general configuration rather than in analytical vision. This is more than true inside a cockpit, because the number of the displays, the short time available to detect every single variation, the process of interpretation of multiple data. In a pilot's mind, symmetry is more important than a precise indication. Here it is an example:



Given the same figures, it is obviously easier to spot a difference on the left side display, called "field vision", versus the "analytical vision" on the right side.

The same applies to the speed indicator, such a speed tape, set on the left of the modern attitude indicator (PFD: Primary Flight Indicator). They have the great advantage, compared to the older version (analogue indicator) of speed indicator: it can represents also the speed related to the entire operational envelope, such as flaps and slats operating limitations, over speed, approach to stall warning et cetera. The problem, as a philosophy of flight is that things appear to go better when the workload is low (inducing perhaps complacency) while they go worst when there is a main failure. In fact, all those useful indications are removed from the speed tape, leaving the pilot to strive with a higher mental workload.

Conclusion

In this short introduction to the problems arising from the implementation of new technology in a modern cockpit, this paper tried to point out the difference between the user friendly concept, as imagined by the airplane designer, and the pilot friendly concept, that follows a mental pattern given by experience and knowledge of the sharp end operators. To obtain a higher level of safety, everyone should strive to make it resilient. The history of airplanes' accidents shows quite clearly that new solutions bring new problems. In this phase we may say that an excessive use of technology could make the entire system less resilient. In fact, the pilots are used to have knowledge of the airplane they fly, based on a kind of "over-learning". This ample knowledge gives the pilot some flexibility, allowing the user to utilize the machine in a non standard way, whenever necessary. At the time in which new generation of airplanes (Fly-by-wire, dark panel, Flight Management System) were conceived, the pilot has been set at the edge of the innovation process. That induced some kind of accidents due to poor interaction and basically to a misunderstanding of the system inner logic.

Paradoxically, to many instruments, thought to be a substitute for humans, could bring two main problem, from a pilot's point of view. Firstly, they induce a low workload when things are running normally and this low workload could induce complacency on the system's reliability. Over-reliance is at the core of some accidents, when pilots could not regain the full control of the aircraft after the automatisms failed.

On the other side, when pilots are in emergency they need more help. Conversely, much of the aids normally available to pilots are removed during an emergency situation. We may, in short, say that the paradox of automation onboard could be said as: "When good, better; when bad, worse".

In my experience, I see that to enhance safety via an engineering approach, it is necessary to take into consideration the pilot's point of view, to implement new systems at the same time useful and usable. But, before introducing new technologies, we should first set the frame to make clear which is our safety paradigm and which is the intended outcome.

The expertise given by the final user is, in this context, highly valuable, since it represents the necessary connection between aims and tools.

References

Cooper, G.E., White, M.D., & Lauber, J.K. (Eds.) (1980) "Resource management on the flightdeck," Proceedings of a NASA/Industry Workshop (NASA CP-2120)

Dekker, S., Johan Rignér, (2000) "Sharing the Burden of Flight Deck Automation Training", The International Journal Of Aviation Psychology, 10(4), 317–326 Lawrence Erlbaum Associates, Inc.

Dekker, S. (2001) "Reconstructing human contributions to accidents" Technical Report - 01, Lund University School of Aviation

Dismukes, Berman, Loukopoulos (2008), The limits of expertise, Ashgate, Aldershot, Hampshire

Goeters k.M. (2004), Aviation Psychology: Practice and Research, Ashgate Publishing Ltd. Aldeshot Hampshire.

Hollnagel E., Woods D., Leveson N. (2006) (a cura di), Resilience Engineering – Concepts and Precepts, Ashgate, Aldershot Hampshire

Hollnagel Erik, (2008) "Critical Information Infrastructures : should models represent structures or functions ?", in Computer Safety, Reliability and Security, Springer, Heidelberg

Hollnagel Erik, (2009), The ETTO Principle – Efficiency-Thoroughness Trade-Off, Ashgate, Surrey, England

ICAO, (1998), Human Factors Training Manual, Doc 9683-AN/950.

IATA (1994), Aircraft Automation Report, Safety Advisory Sub-Committee and Maintenance Advisory Sub-committee

Norman Donald (2005), La caffettiera del masochista, Giunti Editore, Firenze

Ralli Marcello (1993), Fattore umano e operazioni di volo, Libreria dell'Orologio, Roma

Reason James, (1990) Human error, Cambridge University Press, Cambridge

Tichauer E. R., (1978), The Biomechanical Basis of Ergonomics: Anatomy Applied to the Design of Work Stations, New York: John Wiley & Sons,