Safety and the cost killers

By Jean Paries

Jean graduated from the French National School of Civil Aviation as engineer, and then joined the DGAC for several positions dealing with air safety regulations. He was a member of the ICAO Human Factors & Flight Safety Study Group since its creation in 1988. In 1990, he joined the Bureau Enquêtes Accident as Deputy Head, and Head of Investigations, where he led the technical investigation into the Mont Saint-Odile Accident, 1992. Currently Jean is CEO - of Dédale SA. He holds a Commercial Pilot Licence with Instrument, Multi-engines, Turboprop, and Instructor ratings and a Helicopter Private Pilot Licence.

A global race

Because he had lifted the Nissan car-maker company from near bankruptcy and given it industry-leading profit margins in just four years, Carlos Ghosn got the sort of adulation in Japan that is normally reserved for rock stars. But when he took over as the CEO at Renault, French journalists had already dubbed him “the Cost Killer”, a rather backhanded welcome compliment. Further evidence of cultural differences... But welcome or not, “cost killing” and productivity are now characteristic of the fierce, global race between companies, regions and nations. Every industry has come under powerful pressure to shorten project realisation time, cut production costs, and also improve quality. Whatever the product or service, anything which is designed, produced, or operated – including ATM – must be done “faster, better, and cheaper”.

But can it be safer as well, or even maintain the same level of safety in the face of these changes? It is in fact quite sensible to raise concerns about the impact of economic pressures and “cost killing” efforts on the (operational and occupational) safety of operations. Obviously, safety has a cost. Safety requirements include carefully thought-out fail-safe design with adequate backups and redundancies, high quality equipment maintenance, adequate staffing and training, due consideration of stress, fatigue and other Human limitations in the design of the work environment and processes. None of these conditions come without a cost. Hence killing costs may affect safety as well. On the other hand, there might be some wisdom in the idea that a smart and coherent evolution of a system can win on all fronts. After all, aviation history itself is a nice example of getting faster, better, cheaper - and safer, at the same time. So, which vision is right? What is the relationship between economic pressure and safety?

Faster, better, cheaper… failure?

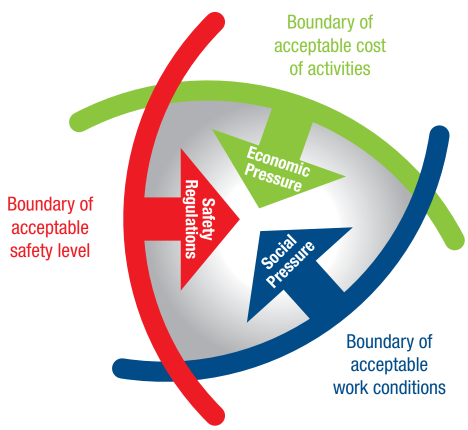
To launch this discussion, it might be interesting to draw on the sources. The “faster, better, cheaper” motto was coined at NASA in the early 90s, when stricter budgets from US Congress forced the space agency to demand better performance from small missions with tighter schedules[5]. It ignited a long-lasting debate over the value of the new credo. Many voices claimed that faster and cheaper were obviously not better[6]. The debate intensified when it appeared that the rate of design errors and associated space mission failures was growing. But its supporters argued that the idea still held: when a mission is inherently risky, it’s better to have a cheap disappointment than an expensive catastrophe. When the Mars Observer was lost in 1993, NASA had already invested a billion dollars - and all its scientific hopes - into the project. In contrast, the combined price tag for the Mars Climate Orbiter and Polar Lander failure[7] “only” amounted to $235 million. So, as a NASA manager once put it, “If you do a multitude of missions, it’s better than if you put all of your resources in one basket.”

While it’s a bit difficult to imagine a straightforward transfer of such debate to ATM – unlike in space ventures, an accident is not an option in ATM – it is a nice illustration that simple ideas are rarely correct where safety is concerned. Because it emerges from complex interactions across its components, the safety of large systems often has surprising, counter-intuitive properties. More is not necessarily better. Local, isolated efforts to optimise safety generally fail to generate an overall best. Using superficial logic, the introduction of an additional safety net like TCAS onboard aircraft is categorically good for safety… unless, as sadly shown by the Überlingen accident and several other events, its potential interactions with the existing safety process are considered. For similar reasons, the consequences of economic pressures on safety are not straight-forward.

Back to Content

Several constraints

In fact, safety is one of the three main constraints that shape production activities. The other two are the economic pressure to increase efficiency, and the social pressure from staff striving to win more favourable work conditions. As shown by the picture, borrowed from Jens Rasmussen's work, these three constraints are only partially antagonistic. They delimit a "green area" which is the envelope of acceptable operations. Outside the boundaries of this area, the business cannot survive.



Within the boundaries, the operation represents a compromise between efficiency, safety and comfort. The best way to relax this antagonism and shift these boundaries is a fundamental technological change. When jet airliners were introduced, they simultaneously offered more efficiency, more comfortable work conditions for the crew, and safer flights. Similar improvements occurred within ATM with the introduction of new technologies like radar, transponder, or computer-based flight displays.

The Long March Towards Quality

But technological revolutions do not happen every day. The overall progress of a system like ATM also results from the confluence of many streams of evolution and improvement: better organisation, better technology, better work processes, better procedures, better training, and so on. Better is the key word. And Quality Management is the key process: clarify the goals, set the proper requirements, do what is specified, monitor what happens, learn from experience, and adapt requirements accordingly.

Is this approach valid for all components of performance? Safety is no exception. Most safety experts would agree that an efficient safety strategy includes the following components: design reliable technology, automate what can be automated, anticipate all work situations (including emergency situations), specify every detail of "the right" behaviour through appropriate procedures, select the "right" operator profiles, train them to follow procedures, monitor adherence to procedures, blame the deviants (intentional violations), detect and explain "honest errors", learn from them and fix the system accordingly.

Efficiency versus flexibility: Should the desert lizard show the way?

In other words, economic pressures and safety requirements tend to take the same form: rationalisation, formalisation, proceduralisation, automation. Essentially, they both try to reduce the messiness and uncertainty in the system by reducing variety, diversity, deviation, instability. But the side effect is that this also reduces autonomy, creativity, and reactivity. They try to increase order, conformity, stability, predictability, discipline, anticipation, repetition, etc. Achieving this renders the systems more efficient, cheaper, and more reliable… within the confines of their standard environment. They also make it more and more brittle outside the boundaries of the normal envelope. They tend to over-adapt the systems and processes to their standard business and operating environment. This trade-off between efficiency (adaptation level) and flexibility (adaptation bandwidth) is universal. Formula 1 car tires have an incredible grip… within a temperature range of plus or minus 5°C. Competition gliders can fly more than 50 km in calm air from an altitude of 1000m… provided no mosquitoes are squashed on their wings. Desert lizards are so well adapted that they can survive for years without water, but would disappear if the climate changed by a few degrees. Trained controllers can handle up to thirty aircraft in a busy sector… provided all aircraft behave exactly as expected.

Thus rational and formal optimisations of production systems make them better (more efficient, more reliable), possibly cheaper, and generally safer within their adaptation envelope. Unfortunately, they also make them less "**resilient**" outside their adaptation envelope. Resilience is the capability of a system or organisation to maintain its integrity and main functions after a disruption - i.e. an external or internal disturbance that fall outside the scope of adaptive behaviour of that system. Resilience is about how a system can actively ensure that things do not get out of hand. It is not enough that a system like ATM be reliable (so that the failure probability is acceptably low); it must also be resilient and have the ability to recover from disruptions and unexpected degradations. It needs not only well adapted processes and procedures, but also robust yet flexible processes, in the face of disruptions or ongoing production pressures. And the main source of robustness and flexibility is intelligence, at both the individual and collective level, in particular for front-line operators. The system must maintain and safeguard this intelligence at any cost.

[5] *Employees were cut from about 25,000 to 18,500 over 7 years.*

[6] *See for example Dekker SWA (2005) Ten Questions about Human Error. Lawrence. Erlbaum, Mahwah, p144.*

[7] *In September 1999, a failure to convert between metric and English units condemned the Mars Climate Orbiter to an unexpected end, while a software flaw contributed to its sister ship (Mars Polar Lander) crash landing in December (the software erroneously detected a landing when the landing gear deployed, and prematurely shut down the engines).*

Back to Content