

safety bulletin

Inside this issue

2 Editorial
Managing complexity- for the sake of safety

3 Lessons learned
Aircraft performance at high altitude

4-5 The human factors column
Safety and Quality : friends or foes?

6 Safe or Unsafe
The Multimillion Dollar Question?



Managing complexity – for the sake of safety



I think you're all aware of the fact that ATM today is a very complex socio-technical system – a system, whose performance is built on the combination of the strengths of the human and the strengths of a highly automated technical system.

The interactions within this system are non-linear, and mostly non-deterministic, which means that the functioning of our system cannot be decompiled into simple, linear processes. This in turn has the consequence that after a mishap, it is not possible to identify a single «root cause» (or even some root causes) in hindsight. If at all, only a set of «contributing factors» can be identified, and these sets are probably never complete, nor unique.

After a visible mishap, we are often «supposed to do something» (ask the press, for example). However, basing «improvement measures» on single events can be dangerous: It is changing a system, which went right a million times, on the basis of a hindsight-constructed, incomplete and uncertain interpretation of one single mishap. How big is the danger that you do not improve, but worsen the stability of the system?

Our system has become too complex at some places, which makes managing the risks in it – and this is what safety mostly is about – more difficult. When the risks become increasingly unmanageable – e.g. because additional factors such as weather, restricted runway use etc. come in – the capacity has to be reduced in order to maintain the safety. In other words: too much complexity leads to a less stable system with more transitions, thus inherently creating additional risks.

More automation doesn't generally do the trick, as more automation



Figure: complexity, 24 hours of traffic at skyguide

usually also means more complexity, and thus more risks. Neither does train the ATCO a little more (today often a mitigation measure), as human performance also has its clear limitations.

Consequence: a system which is both performing in terms of capacity and safety, which is stable also vis-à-vis of temporary disruptions or suboptimal conditions, is one in which the complexity is under control, in which the complexity is as low as possible, but not lower. We have various instruments to achieve this goal.

One is that we must understand how exactly the system works, where the shortcomings and strengths are. For this, reporting is important; the detailed analysis of mishaps and other reportable events helps identify where the system performs badly, and possibly also where a complexity issue exists. In fact, it would help even more if we had a «what-went-right»-type of reporting, because this would help us identify the strengths. I can only stress here how important your reporting is; the more complete reports we have, the more we learn how and where to improve the system! (Note: the legal cases don't do

us a favor here, but neither does non-reporting).

Another path to reducing complexity is what CANSO recently called «safe-by-design». This means the earlier safety is considered in the design process of anything being changed, and the more systematically the safety analysis is conducted, the better we can design systems, which are inherently safe and robust. Where safety has been taken into account (too) late in the design (namely when the design is already poured in concrete), either fixes must be applied (in the form of mitigation measures, typically more training), leading to a less robust system, or the project must be redesigned at significant cost and delay.

As you can imagine, to work for a less complex, more robust, ultimately more performing one in both safety and capacity terms needs constant effort, sometimes fights, and sometimes difficult decisions have to be taken which may hurt in the short term, but are beneficial in the long term.

A Merry Christmas and A Happy New Year!

SIMON MAURER
5

Aircraft performance at high altitude

Situation

An Airbus A321 outbound Metz was climbing to FL 350 out of FL 285 just approaching TRA on course to KPT and the east, while an Airbus A320 was crossing its flight path from south to north maintaining FL 320 over ZUE.

Events

- A321 approaching TRA climbing to FL 320 with M3 Sector requested cruising FL 350, so far unknown to the ATCO.
- ATCO asked A321 crew: «are you able to climb to FL 350 with a minimum rate of climb of 1500ft per minute until out of FL 340?»
- A321 confirmed to be able to follow the clearance.
- ATCO cleared A321 crew: «climb to FL 350 with a minimum rate of climb of 1500ft per minute until out of FL 340», which was confirmed correctly by the crew.
- A321 was climbing with 1600ft/min, two minutes later with 800ft/min and shortly before the crossing with only 400ft/min.
- ATCO gave avoiding heading for both aircraft to the right.
- A321 passing FL 325 for FL 350 crossed the A320 maintaining FL 320.

Analysis

The A321 called in at the M3 sector approaching TRA on course to KPT climbing through FL 285 for FL 320 with an average rate of climb of around 1200ft/min. During the initial call the crew requested a new cruising FL 350. The estimated calculated time the A321 had to fly to the crossing point of the A320 com-

ing from the south at FL 320 was about four minutes. The ATCO asked the A321 crew, whether they would be able to climb to FL 350 with a rate of climb of 1500ft per minute or more until out of FL 340 to get the aircraft 1000ft above the A320. The A321 crew confirmed that and was then cleared to FL 350 with a rate of climb of 1500ft per minute or more until out of FL 340, which was read back correctly by the crew. As the A321 achieved a rate of climb of 1600ft/min, and two minutes later only 800ft/min and finally 400ft/min, shortly before the STCA alarm started, the ATCO urged the A321 to expedite climb due to crossing traffic, which the crew confirmed to do. When passing 3,5 NM slightly behind the crossing A320, the A321 was climbing out of FL 325 for FL 350, 500ft above the A320 resulting in a separation minimum infringement. The ATCO had given a heading of 20° to the right for the A321 and 10° to the right for the A320 to achieve a larger horizontal separation.

Lessons learned

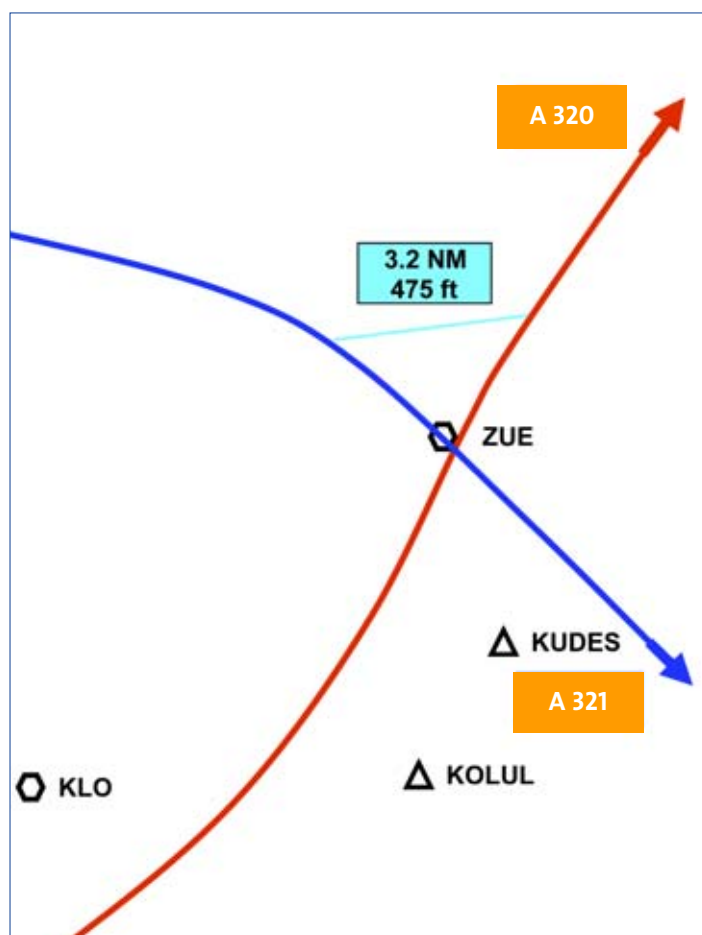
In a highly complex and densely loaded environment, where horizontal separation criteria for crossing traffic are difficult to achieve and a vertical separation of 1000ft is chosen instead, a clearance using a certain rate of climb can be essential to achieve the minimum separation. A given minimum rate of climb is often accepted by the crew at the moment the clearance is issued, but during a climb phase of several minutes then cannot be maintained. Especially in the upper airspace, the performance of the aircraft and its

ability to maintain a given rate of climb can rapidly change. This separation concept is very fragile and therefore alternatives, such as safety buffers should be planned and constantly monitored as predictions are unreliable.

Additionally, misunderstandings can be part of the problem. The ATCO needs and expects an average rate of climb to get the aircraft 1000ft below or above a crossing or opposite

traffic, while the crew interprets the clearance rather as a rate of climb they have to achieve during their climb phase, starting with a low rate of climb and accelerating then to the cleared rate, or in the actual incident, the rate of climb collapsed approaching FL 325 due to the technical limitations of the A321 resulting in a low average rate of climb in the end.

NICHOLAS SCHERRER
SRO



Safety and Quality: friends or foes ?

The debate opposing Safety and Quality can certainly be traced back to the times when these terms started to coexist within organizational setups. One may argue that a good Safety Management System can only be constructed on the basis of a solid and credible Quality Management System. Another perspective would claim that Safety is much more than managing the Quality of a system's components. This article explores such opposing lines of thought and emphasizes the problems that may arise from an inadequate positioning of these two important but profoundly different domains.

The importance of Quality

Quality is undeniably an important component of a good Safety Management System. Indeed, having for instance a structured process in place to identify and manage Risks is something that shouldn't be underestimated. Similarly, Safety deliverables (as well as others, of course) shall be thoroughly structured and written in an understandable and usable manner. Moreover, the evidences brandished to support the argument that an ATM System change can be conducted in an acceptably Safe manner often refer to the process by means of which these evidences were produced. In this respect, the Quality framework put in place for the purpose of preparing and conducting the KLO-DUB migration was an important piece of the final Safety argumentation. So far so good. Safety needs Quality to achieve its purposes. Or more precisely, some of its purposes.

The heart of the debate

So why do we need to debate the coexistence of these two domains? Simply because the way of thinking induced by Quality-based approaches may impeach further progress on Safety within complex socio-technical systems. Impressive claim, isn't it? But let's start with the beginning. Our way to think and to act is profoundly influenced by the way we «perceive» the world around us. There is no «real» world lying out there; that some people see correctly and others do not. In fact, each of us looks at the world through different lenses and see, as a result, different things. As a consequence, nobody is right and nobody is wrong. But some «visions» are better than others to achieve specific endeavors. These lenses are reflecting the existence of what specialists name different paradigms. More formally, a paradigm is a term used to mean a model, a theory, a perception, an assumption or a

frame of reference. Paradigms are powerful because they create the lenses through which we see the world: we don't see the world as it is but as we are conditioned to see it.

Young lady or old witch ?



Figure 1 - The two conditioning pictures

A simple and convincing way to experience the power of paradigms was introduced several years ago at the Harvard Business school in order to demonstrate that two people can see the same thing, disagree and yet both be right. It consists in equitably distributing two different drawings to a group of people and to ask each of its individuals to carefully observe during 15 seconds the exemplar he received without showing it to its neighbors (Figure 1).

Then, another drawing is showed to the whole group and people are asked to describe what they see (Figure 2). Interestingly, more than 90% of the individuals involved in the experience usually see first what

they were conditioned to see – namely a young lady or an old witch. After some time, both camps start to see what the other sees and everybody finally realizes that different people can look at the same thing and see it totally differently depending on powerful conditioning factors like for instance education, culture or personal beliefs. Who is right and who is wrong? Obviously nobody !



Figure 2 - What do you see?

► Safety and Quality: friends or foes?

Back to Safety and Quality

So what is so profoundly different between the Quality and the Safety lenses that may impeach us to make further progress on Safety? First, we have to consider the nature of the «system» we are attempting to keep under control. While a «system» can be broadly defined as the intentional organization or arrangement of parts (usually human, equipment and procedures) that make possible the achievement of specified and required goals, the idea of a socio-technical system is that the conditions for successful organizational performance are created by the

interaction between social and technical factors. Under the increasing influence of business pressures and with the development of complex and coupled technologies, our ATM System has increasingly become of socio-technical nature.

Research work conducted in this domain has shown that the paradigms applied up to now to manage Risks have reached their limits. Indeed, the models we use to understand how and why mishap occurs – our current accident paradigms – are based on the fundamental hypothesis that small events combine and develop in a linear fashion into «chains of events». This belief

is clearly reflected by Probabilistic Risk Assessment (PRA) methods introduced in the early 50's and still widely applied nowadays (Figure 3). Their popularity not only come from the simplification they introduce but also from their adequacy with the «process-based» approaches introduced and promoted by industrial Quality Management techniques. And this is exactly where the problem lies: linear-based accident models are difficult to abandon because they better fit the way Quality «process-based» approaches have conditioned our mind during the past decades. Thus, adopting Safety models which better fit the complexity of modern socio-technical systems requires a profound «paradigm shift» that may be rendered difficult by Quality-based thinking !

grant to the evidences produced by the organization. But Safety urgently needs to escape «Quality thinking» in order to facilitate the adoption of new paradigms that are necessary to better understand and manage the complexity of modern socio-technical systems. Thus, the debate opposing Safety and Quality is far away to be over and shall remain an important preoccupation for all those in charge of keeping Safety at the highest possible level.

STÉPHANE BARRAZ
Safety Program Manager

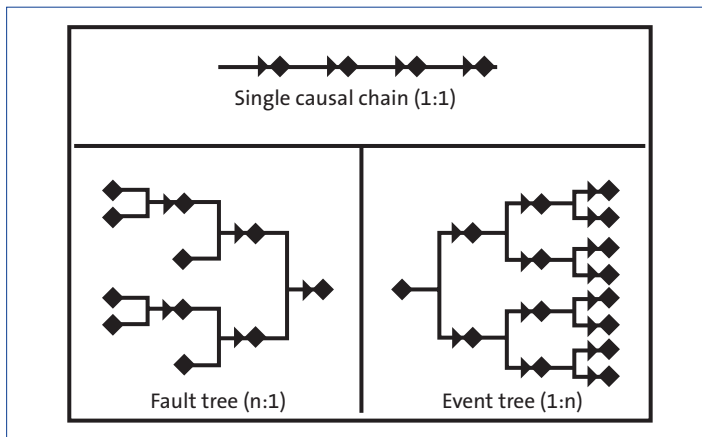


Figure 3 - PRA «Bow-Tie» analysis

So, friends or foes ?

It appears therefore that Quality and Safety are at the same time friends and foes; what makes their respective positioning quite difficult to manage adequately. Safety needs «Quality doing» because it provides a structured approach of problems and enhances the trust one may

Sources used in this article:

- The ETTO principle: why things that go right sometimes go wrong
Erik Hollnagel – Ashgate publishing, 2009 – ISBN 978-0-7546-7677-5
- The 7 habits of highly effective people: powerful lessons in personal change
Stephen R. Covey – Free Press, 2004 – ISBN 978-0-7432-6951-9

Safe or Unsafe – the Multimillion Dollar Question?

All aviation professionals try to be the winner in safety. However, in most cases, we only find out our safety score after the event!

Aviation has the highest safety record per km travelled. But, how is it that safety is still a «fuzzy» concept? Why is it that nobody can tell what is safe and predict a safe outcome with the same certainty that we know the sun will rise or set?

Many readers will not agree with me, especially all the aviation professionals, and in particular Air traffic controllers. Safety is not really predictable and we struggle to define safety precisely. There are indeed commonly developed and accepted definitions, e.g. ICAO talks about «the condition in which the risk of harm or damage is limited to an acceptable level».

Safety is of course a very serious issue, especially when we are talking about Air traffic control. The longer we try to define it, create it and defend it as the basis for our profession, the more it is like buying a lottery ticket. At least, for me, every time I buy a lottery ticket I see myself as a future multimillionaire. It is only following the lottery draw that I know whether buying a ticket was worthwhile. The establishment of what is safe or the construction of safety follows a similar pattern. All the professionals will try to be a 100% winner, something only the future can tell!

The safety outcome is not predictable, and only is measurable once



Does achieving safety give us the same thrill as when we buy a lottery ticket? photo: dreamstime.com

the event has passed. Weick has defined safety is a «dynamic non-event». However, from an intellectual point of view, how can a «non-event» be «dynamic»? According to Weick it is dynamic because processes remain under control due to the continuous adjustments, adaptations and compensations made by the human elements of the system. It is a «non-event» because «normal» outcomes claim little or no attention. The paradox is rooted in the fact that events claim attention, while non-events, by definition, do not.

So, if safety is a «non event», why do we see it as the «holy grail» or the multimillion lottery ticket? Or does achieving safety give us the same thrill as when we buy a lottery ticket? Are we perhaps imagining what we would do with the gain?

Moving away from the craft of air traffic control to the science of air

traffic management with its increased automation will we be buying lottery tickets to keep the dynamic non-event's sufficiently in line with mathematical models? Will this justify investments in future technology to keep us all safe? For quite some time, this has been the question for me. Can we actually develop models, approaches, information and/or communication campaigns preparing our profession and our industry for the next step of automation? Do we understand the approach to increase the intricacies of a set of systems which will reach levels of complexity which are currently unknown in our working environment?

Recent publications by researchers like Dekker, Hollnagel, Reason and others are assisting in understanding what is a stake and providing us with a scientific approach to what we are doing and what will be done. We are currently in the transition period

towards a safety management process. It is very helpful as it explains our activity and it's related risk in a focused way. But the question still remains on how to manage your winning lottery ticket ahead of the potential gain?

In the quest to improve the dynamic non events, we are not alone. Bert Ruitenbergh, our Human Factor specialist, wrote an article entitled «safety was 16 today». Safety measurement is a science and it is reactive and serves (in the new business world) to determine the performance bonuses of our ANSP CEO's. ICAO recommends a safety management approach. CANSO asks for a changed business model where liberalised and economical performance will assist improvements to safety. Eurocontrol proposes a new methodology to bring us a step further in predicting and shaping the safety outcome with a Aerospace Performance Factor. So let us, as IFATCA, remain on the forefront to be among the potential winners in safety, by continuing to educate, influence and participate in shaping the safety discussion.

Oh, and by the way, did I forget to mention: 100% of lottery winners did buy a ticket!

MARC BAUMGARTNER
President and CEO IFATCA

published in IFATCA magazine «The Controllers», 4/2009 special safety edition