

# safety bulletin

## Inside this issue

**2 Editorial**  
*By Dani Weder, CEO*

**3-4 Lessons learned**  
*Should we further enhance DST?*

**5-6 Overdeliveries**  
*Or why do people not always follow procedures*

**7-8 Safety engineering**  
*Changing configuration data; is it safety relevant?*



# New paradigms for the ANS industry.



*For several years now, ANS has been in a continuous improvement process. Intensive efforts to achieve the complex balance between safety, capacity and cost are leading to ever better performance. Safety management has gained in conceptual insight and widespread application throughout the industry. However, in spite of these good news, I do not believe that the challenges of the future will be met with the present structure. We need new infrastructures, new airspace design and new business models to take up the challenges of the 21<sup>st</sup> century. And this should be viewed as a welcomed news!*

The last successful global capacity increasing measure was the implementation of RVSM between 1997 and 2005. What else is in the pipeline to handle the ever increasing amount of air traffic? New control systems, data link to reduce ATCO workload, improved sectorisation and better inter-centre coordination for more direct routes etc. Additionally, there are several strongly communicated initiatives to improve the environmental footprint of our industry. We, in Europe, are of course well aware of the Single European Sky and SESAR, the most important initiatives to boost performance in our region. How much they will bring and at what cost cannot be said today. Today, the investments and efforts needed to generate even marginal improvements in air traffic control are considerable and maybe occasionally disproportionate to the benefits.

The degree of systemic complexity becomes such that safety, our paramount target and raison d'être, might be hindered in the long run. Paradoxically, many ANSPs invest heavily to optimise the existing system without ever questioning the basic business model of ANS provision. Our industry needs a new way of thinking and different business models to secure the target levels of performance – and naturally of safety - defined for the future.

Thinking «out of the box» following eight points constitute the foundation for the future development of our industry. While national sovereignty is not questioned, we need to:

1. Undertake new airspace design which shall reflect traffic flows and support dynamic airspace management;
2. Build a system and business model «from scratch» with lowest possible basic complexity. Eliminating inherited assumptions will lead the industry to further improvements. By doing this both safety and capacity can simultaneously be increased;
3. Achieve the highest possible standardisation of processes and systems; buy systems from the shelf whenever possible;
4. Consolidate ANS centres where necessary to achieve an optimal scale effect.
5. Promote cross-border service provision wherever such practices are expected to improve overall performance;

6. See ATS as the core activity with ANSPs purchasing all ancillary services (such as technics, training, AIM etc.);
7. Establish new organisational constructions such as national holdings in order to manage companies and participations;
8. Establish system redundancy between centres, and possibly between ANSPs, and not only within individual centres.

All points will contribute to enhanced safety by reducing complexity and improving transparency. A new regime of economic regulation will be required to meet these strategic objectives. There should be some sort of incentive for innovation in the ANS industry where those willing and able to progress with all due attention to safety are rewarded. ANS is a people business where safety, capacity and cost management are key. Efficiency gains will be obtained by new business models. Pure cutting of salaries is not the practical way in this respect. It is neither acceptable from a social point of view nor the wise economic base line. Much higher benefits can be expected from managerial practices which associate the staff to the good performance of the system.

I know that there is a long way to go. We better get going right now.

DANIEL WEDER  
CEO

# Should we further enhance DST\*?

Since the end of last year, I am conducting the internal investigations for the ACC Geneva. I am an ATCO in Geneva since 1995, and presently work at the INI sectors. With the precious help of the RIT-team (Ivan Rochat, Xavier Henriod and David Fraternali), four internal investigation reports could already be released, and work is in progress for another three.

Now you might be asking yourself «what the heck is an internal investigation and what is its goal?»

As a matter of principle, every submitted OIR is analyzed by the SR team and the operations, and if any of us suspect some potential for learning something out of the occurrence or an opportunity for improvement of the ATC system, then we go on with an internal investigation.

An internal investigation report contains normally 4 items: 1. The Facts, 2. The Analysis, 3. The Conclusion, and 4. The Recommendations.

So let's start with:

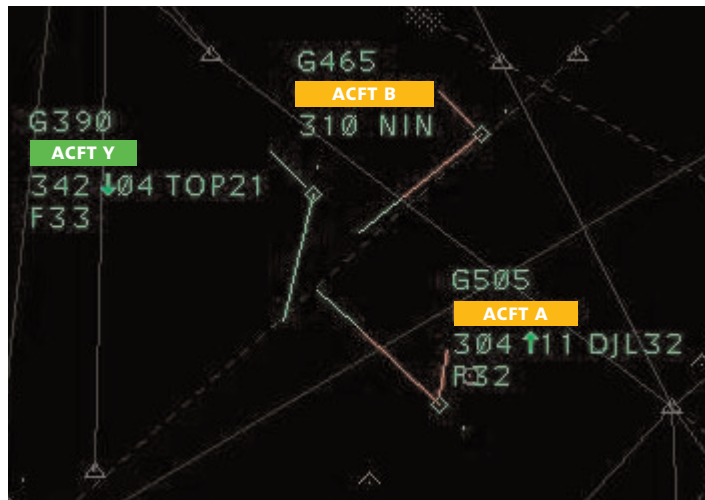
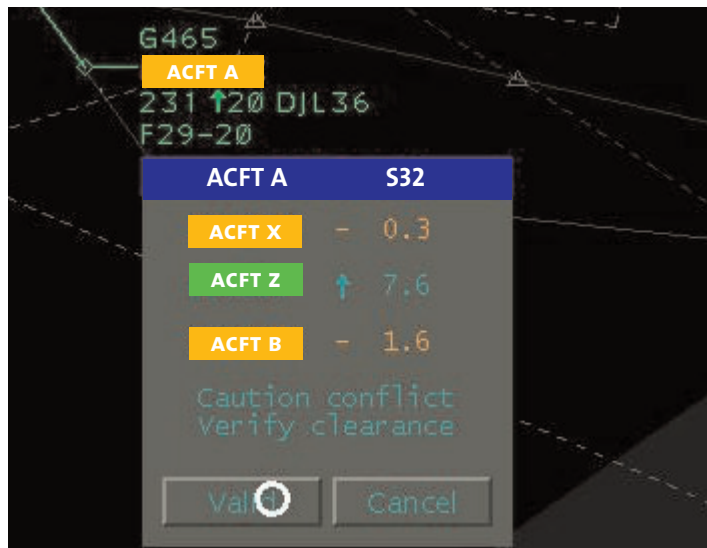
## 1. The Facts

In the afternoon of April 19th, sectors KL2 and KL3 are combined, with a workload described by the ATCO as «medium, a lot to do but not too much».

Acft A is calling on the KL23 frequency, climbing to FL260. The

KL23 ATCO clears Acft A to FL290 after a coordination with KL1. Shortly after, Acft B calls in at FL310 and is cleared BENOT-NINTU.

One minute later, Acft A is cleared to FL320. This clearance triggers a DST alert with 3 aircraft, as shown in the picture below:



The ATCO validates the DST alert, and 7 minutes later, E-STCA triggers an alarm between Acft A and Acft B. Separation at that time: 13NM, 600ft.

Immediately, Acft A is instructed to re descend to FL300 and to turn left on HDG270.

Acft B is instructed to turn on HDG180.

Those avoiding actions result in a minimum separation of 5.1NM, 925ft.

## 2. Analysis

The main question that has to be asked for the analysis is: WHY. Why did the controller act in a certain way and why did it make sense to him at that particular moment?

So if we look at the picture of the DST alert, the first question might be «why did the controller validate the CFL320 despite the DST alarm

showing a conflict with Acft B and 2 other aircraft?»

To get an answer to that kind of questions, it is necessary to conduct an interview with the controller. During that interview, the ATCO stated that he could not remember if there was a DST alert or not, but using our general experience in handling DST alerts allowed us to reconstruct a hypothetical explanation:

The conflict shown in the first line was expected, since already coordinated with KL1 and solved by the rate of climb (2000ft/min) instructed to Acft A in the previous clearance.

The second conflict was of no issue to the controller, since the Acft Z was not known to him and its position in the region of ASLEG, around FL240, considered to be out of the «potential conflict range».

\*DST = Dynamic scanning tool

► *Should we further enhance DST?*

Finally, and only in 3<sup>rd</sup> line, the potential conflict between **Acft A** - **Acft B**.

Representing this potential conflict in 3<sup>rd</sup> line seemed to be insufficient to alert the controller, probably because the first two lines of the DST were of «no use» to him.

Furthermore, we know that the analysis of a triple line DST is a time consuming task, and that an open DST window literally hampers the continuation of the controller's work, since there are no other inputs possible. Therefore, the temptation to «click the window away» is always present.

Some other interesting elements that were raised by the RE and RP during the interviews:

Both stated that it was «quite a while ago» since they worked last on KL23 combined sector. Unfortunately it is not possible to retrace controlling hours on combined sectors in the ATCO time measurement.

The RP also said that he could not hear the clearance for **Acft A**, being occupied by coordinating this complex situation with KL1. He considered the «close the loop» procedure insufficient to stay in the loop in this situation, and missed a kind of «log list» of DST alerts.

Another question we could possibly ask: why was the **Acft A** on KL23 frequency, virtually conflicting with 3 aircraft on KL1 frequency?

Besides the fact that **Acft A** was probably sent by Milano on the wrong frequency, we have to keep in mind that frequency separation is literally baked into our ATC system. Procedures such as the «no need» function, the «release zone» between K and L sectors, and so on, are institutionalised in a way that they become factually irreversible considering nowadays' traffic load. Frequency separation is part of the organisational trade off between sector capacity against safety.

### 3. Conclusion

The situation was complex in a relatively unusual sectorisation. The unsuitable display of the DST window and the absence of a redundancy check between the RE and RP hampered an efficient conflict detection.

### 4. Recommendations

1. Explore possible solutions to improve the redundancy, traceability and the general layout of the DST alarms. This could include the following:

- Display the DST alarms on all positions of the sector (like HST)
- Create a log list of acknowledged DST alarms, where the conflict is listed until it is solved (like HST)
- Trigger a new DST-calculation when closing the loop
- Allow the controller to perform other inputs despite an open DST window

- Avoid multiple lines of potential conflicts in one DST window.

2. Evaluate if the currency rule has to take into account vertically combined sectors.
3. Consider the frequency separation problem for future procedures / projects / etc...

Please remember that this is a short version of the Internal Investigation Report published last month. If you want to read the whole report and/or all the other reports, you will find them on skyline:

<http://skyline/Livelink/livelink.exe?func=11&objId=1524446&objAction=browse&sort=name>

ALAIN GABERELL  
Investigator and ATCO GVA ACC

# Overdeliveries

## Or why do people not always follow procedures



**Eurocontrol in May 2009 launched a Request for Support Message with the title: «Sector overdeliveries due to non adherence».**

In accordance with this perspective, already in August 2008 a service order was effectuated in skyguide's ACC Geneva, which prohibits the alteration of RFL (requested flight level) from the filed flight plan and limits the change of XFL (exit flight level) with the purpose to avoid overdeliveries in regulated sectors and increase published sector-capacities according to CAPAN studies.

### Problem identified and solved one could assume.

Apparently this was not the case. In our reporting and investigation division we received several SIR's (Safety Improvement Reports) as a consequence of this service order. However the reports had contradictory content. On one side, ATCOs stated that «regular non-adherence

occurs which is endangering safety» and consequentially proposed further tightening of procedures or even removal of certain alteration possibilities in HMI. On the other hand, colleagues of the same unit stated, that «the limited manoeuvring freedom and additional workload for deviations may hamper the safe handling of traffic.»

On a daily basis ATCOs are working in a highly complex and densely loaded environment that has been continuously optimized and regulated during especially the last 10-20 years. While these measures where successful in the past, they are reaching their limits and the symptoms of this are starting to emerge on several levels. Nevertheless there seems to be a strong persistent belief, that further tightening and enforcement of some kind of «rule adherence» will solve the problem for us. It seems we continue to use a mechanistic reductionist approach, where we try to fix the broken component or symptom

locally in an environment, which has developed into a highly interdependent socio-technical system. Oversimplification of the problem bears the inherent risk that the applied countermeasures will turn out to be ineffective or at worst counterproductive.

When analysing the problems with regards to sector overdeliveries we need to look deeper into how safety is created or hampered in daily work and what the roles of procedures and practitioners are in this framework. Furthermore we should examine the goal conflicts and performance constraints, this highly optimized environment has created at the sharp end.

On a conceptual level the problems with rule following have been extensively addressed by Sidney Dekker in «10 Questions About Human Error» (2005) from which I extracted the two following paragraphs:

*People do not always follow the procedures. We can easily observe this when watching people at work, and managers, supervisors and regulators often consider it to be a large practical problem. Performance variations, especially those at odds with written guidance, easily get overestimated for their role in mishaps (in this case overdeliveries). What looks like violations from the outside and in hindsight are often actions that make sense given the pressures and trade-off's that exist on the inside of real work. Finding procedure violations as causes or contributors to mishaps, in other words, says more about us, and the biases we introduce when looking*

*back on a sequence of events, than it does about people who were doing actual work at the time.*

*Yet if procedure violations are judged to be such a large ingredient of mishaps, then it can be tempting, in the wake of failure, to introduce even more procedures, or to change existing ones, or to enforce stricter compliance. Introducing more procedures does not necessarily avoid the next incident, nor do exhortations to follow rules more carefully necessarily increase compliance or enhance safety. In the end, a mismatch between procedures and practice is not unique to Accident/incident sequences. Not following procedures does not necessarily lead to trouble, and safe outcomes may be preceded by just as many procedural deviations as accidents are.*

*When rules are violated, are these bad people ignoring the rules? Or are these bad rules ill matched to the demands of real work?*

*There is always a distance between a written rule and an actual task. This distance needs to be bridged. The gap must be closed, and the only thing that can close it is human interpretation and application.*

*If we want to make progress on safety with procedures we need to:*

- *Monitor the gap between procedure and practice and try to understand why it exists (and resist trying to close it simply by telling people to comply).*
- *Help people develop skills to judge when and how to adapt (and resist only telling people they should follow procedures).*

► *Overdeliveries Or why do people not always follow procedures*

**The application of this concept leads me to the following considerations:**

In order to cope with all the competing demands in the operational environment of ATC, controllers need a certain «decisional space» in which they can balance the need for safety, efficiency, customer service and recently also sustainability. This can best be achieved by measures that support sensemaking and decision making but is increasingly being hampered by introduction of additional often rigid and over-specified rules that rarely fit the real-life dynamics.

The FMP regulations form only an approximate grid in which the actual traffic load may still fluctuate substantially within short periods of time. These fluctuations are influenced by variables that are not sufficiently addressable by FMP regulations such as unanticipated weather conditions or the complexity of emerging traffic situations. The deviations from a planned Flight Level occur for several reasons with different origins and to some extent outbalance each other in the end. Some examples are:

- Pilot filing lower RFL than effectively requested to avoid FMP regulated sectors and then requesting higher on ATC frequency during flight. (This is the factor which the service order is primarily addressing).
- Pilot requesting lower FL on

ATC frequency than filed in FPL. (This happens regularly with RJ85 + RJ100. The reasons may be similar to those mentioned above but with the opposite effect. Furthermore ATC has practically no means to force aircraft above their actually requested flight level).

- Exit problem in a particular sector triggers a need to clear aircraft to XFL which deviates from filed RFL. (This may include climb and descent).
- Met conditions en route turn out to deviate from forecast, triggering need for a level change. (I am not addressing turbulence here but more subtle deviations like i.e. unexpected changes in temperature that could affect aircraft performance).
- Adaptation of procedures based on experience and an attempt to provide optimal service. (Since in the future environmental concerns will also have to be incorporated in our goals, unnecessary prolonged flight at low altitude with consequential increased fuel-consumption may very well become an issue).

In the end it is a «give and take» where ATC and airline needs are traded off against each other in a mutual collaborative atmosphere. Pilots know that ATCOs will incorporate their specific needs in their traffic management where possible and in return are willing to help out by compromising own goals, when the traffic management situation demands this.

What would be the consequence if a rigid adherence to filed RFL on ATC side would be countered by the same rigid insistence on remaining at a RFL, when traffic management is in need of pilot flexibility?

The Eurocontrol analysis also mentions use of direct tracks as a source of «distortion» of traffic predictions. Surely we cannot expect controllers to check every direct track for its effect on FMP compliance. Furthermore direct tracks are a tactically applied means to solve potential conflicts and a major contributor to reduction of flight trajectories and hence CO2 emissions (sustainability goal) and finally part of the professional upbringing and pride of most ATCOs.

New approaches have to be elaborated when attempting to bridge the gap between strategic FMP regulations, published sector capacities and tactical needs of flexibility in the operational environment without overloading any sectors in the process. In other words we need to look for ways to make our systems more resilient. This could mean to design in slack.

Maybe a more promising (safer) approach of defining sector capacities would include the possibility to absorb some degree of overdelivery, in realisation that this might not be avoidable. Furthermore a more interactive dynamic update of actual traffic patterns with the possibility to respond tactically to a developing situation before the aircraft actually enter the concerned sec-

tors, could facilitate increased flexibility in handling traffic and might even have positive effect on the overall capacity. Precursors for such tools already exist in some of today's stripless environments.

To give an example of the creativity used in an increasingly congested automotive environment consider the latest development of the Navigation system producer Tom Tom. In certain countries they now have a data exchange agreement with a major mobile phone provider. Since every mobile phone's approximate position can be verified through interpolation of a few antennas, so can the speed. These average speeds can be correlated with a roadmap and give an up to date dynamic picture of the actual traffic speeds driven on the road. The newest generation of Navigation Systems can receive this information and re-plan routes instantly if traffic slows down on the previously planned route.

Of course this idea can not be transplanted one to one. Still I believe it points in a fascinating and promising direction. Off course it is also more complicated and resource demanding. After all it is much easier and hence tempting to tell ATCOs to follow the rules and hold them accountable where this was not the case, but do we really believe this will make our system safer?

MARCIAN TESSIN  
SR

# Changing Configuration Data: Is It Safety Relevant?

## Introduction

The safety engineering group (SAE) main mission is to support skyguide commitment to conduct safety assessments of system changes as stated in skyguide safety policy. SAE is especially dedicated to safety assess changes impacting operational equipment items. To do so, SAE applies the safety assessment framework (SAF) and the different tools it encompasses.

As part of its activities, SAE is confronted with the assessment of configuration data (CD) changes. Most of the time, change managers are rather reluctant to perform a formal safety assessment for that kind of changes which are considered as «simple» changes. The question is really whether it is appropriate to spend time and resources to perform safety assessments on CD, in other words, whether CD changes are safety relevant or not.

The answer to these questions is neither simple, nor can it be systematic. Based on field experience, we will try to illustrate this in this paper.

## Deciding to Perform a CD Safety Assessment

There is a tendency within the company to consider that configuration data changes do not need to be formally safety assessed. The justifications brought are, for example that «it is a minor change» for the ATCO, «the application itself does not change», it is a «small/easy change»,



Figure 1: «Blue screen of death» in the cockpit of an aircraft.

«the code is not modified», etc. Nevertheless, this is done without considering the potential (negative) operational impact of such a «small» modification, which is the main trigger for performing a safety assessment.

Formally, the way to determine whether a change (including a CD change) needs to be safety assessed is dictated by a work instruction (WI)<sup>1</sup> that gives guidance on how to determine if a change must undergo a safety assessment or not. This work

instruction contains «exemption criteria» along with a set of 8 «justifications» that allow to decide if the change is not subject to a safety assessment. If the change is *fully* covered by one of the exemption criteria, no safety assessment is needed. However, no exemption criteria explicitly address configuration data. Therefore the decision to perform a safety assessment now comes down to identifying the operational impact of the change. In the cases submitted to us, a thorough analysis rarely leads

the CM and the SSE to conclude that a safety assessment of the change is not needed. Let's now look at some «real life» examples.

## «Real-Life» Examples

Since a few months, the SAE team is involved in the assessment of changes where part of them, not to say the major part of them, consists in modifying configuration data. Two of these changes are being considered below.

<sup>1</sup> M1W10085E «Need for a Safety Assessment» v3.0e, SAF v3.

► **Changing Configuration Data: Is It Safety Relevant?**

In the safety assessment made for the suppression of the Mode A/C interrogation by the MLAT (Multi-LATeration system), the change consists in modifying one parameter file on both central processor units of the MLAT system. Apart from a short MLAT unavailability during the intervention, the change is not expected to impact operations. However, the safety analysis has shown that a corruption of the CD in the modified parameter file could engender a hazardous incorrect situation awareness (due for instance to misplaced or missing plots) for the ATCO and/or APRON potentially leading them to issue erroneous instruction.

This definitely allows to conclude that this CD change is safety relevant and that it was worth allocating it appropriate resources. On the other hand, now that this safety analysis exists, it is useless to reassess similar changes to these MLAT configuration data. Therefore, for future modifications made to the MLAT parameter file, we will use the results of this safety assessment and avoid assessing the change again, because it will be the same kind of change. We will perhaps have new causal factors for the already identified hazards, which will lead to defining new safety requirements. This will significantly shorten the safety assessment process and reduce the needed amount of resources.

The safety assessment being made for NSG (New Sectorisation Geneva) project encompasses both the new sectorisation with 6 vertical layers in Geneva and the change of LoR (Line of Responsibility) between Geneva and Italy. This project has an impact on most of the operational equipment (SKYVISU, SYCO-NT, MV-NT, EMDIS, VISTA etc.) and mostly on their configuration data. For example, none of the 12 modifications made in SKYVISU for the new 6-layers vertical sectorisation will necessitate a modification of the source code.

The safety analysis has shown that these configuration data changes are not harmless. As an illustration, an error apparently as trivial as associating the wrong sector name (either putting the name of another sector or one that corresponds to no sector) to an IP address in the configuration file of EMDIS could result in an ATCO having missing aircrafts on his display, in an emergency situation, leading to potential severe outcomes. Similarly, an error on the value of a frequency in the configuration file of either VISTA-G RAD or VHF de secours could result in an ATCO using the frequency of another sector – or an undefined frequency – and being therefore unable to contact the aircrafts he is supposed to manage, again, with potential severe consequences.

The distribution<sup>2</sup> of the hazards related to the modified configuration files as a function of their severity<sup>3</sup> class is shown in Table 1 below.

Severity	SC1	SC2	SC3	SC4	SC5
Number of hazards	2	4	2	9	1

Table 1: Number of hazards related to CD changes and associated Severities in NSG safety assessment.

This table shows that changes made to configuration data can potentially be involved in various hazardous situations and have a dramatic impact on operations.

**Conclusion**

Even if CD changes seem at first insignificant, the examples provided above show that they can have a strong safety impact on the operations. Therefore, we consider that it is worth involving resources to analyze such changes. However, the intent is not to waste resources and our approach is to reuse existing safety assessments when they are available and appropriate.

More generally, compared to the existing technical domain, made of numerous complex, inter-related, recent (and less recent) equipment, safety assessments are quite recent in

the company. With time and the safety assessments being made, we acquire a better knowledge of the technical equipments and of the type of modifications that are made to them. That knowledge will help us in the future to take «shortcuts» by re-using existing assessments, if applicable. And though the method we use today is not well suited to take these «shortcuts», we will contribute to make it evolve so that it will be adapted to allow us to simplify the handling of some of the changes.

CORINNE GINGINS, PIERRE OBERSON, SAE

<sup>2</sup> So far, we have identified only the hazards linked to the modifications made for the new 6-layers vertical sectorisation.

<sup>3</sup> SC1 is the highest severity.