

Safety Bulletin



e-mail: s.b@skyguide.ch

Intranet: SWAN/management/safety/safety bulletin

Inside this Issue: From the Regulator, page 2 / Lessons learned, page 4 / Technique, page 6 / Risk Management, page 9

Editorial

Dear readers, as you are reading this forth *Safety Bulletin* we can celebrate the first anniversary of this bulletin. This is just one of quite a few safety activities which made good progress during the last year. Some of them should be mentioned here.

What the *Safety Bulletin* is for the whole company are the *Safety Letters* for the operational units. A lot of these *Safety Letters* were produced during the last year by the responsible *Safety Officers*. This is an important step forward in regard of lesson dissemination and safety improvement.

In the domain of our *Risk Assessment and Mitigation* activities big progress was made and several complex safety cases have been completed (see page 9 onwards).

Good progress was also made in the implementation of our *Safety Management System* and in the domain of our *Occurrence Reporting*. These two Eurocontrol Requirements have been audited by the FOCA for the first time and the results were very satisfactory (see page 2 and 3). But an occurrence reporting is not good just because the process is implemented and well running. A good reporting culture depends on a "Just culture" environment. Read the first article and you will see that we can expect positive changes very soon.

An other success was the implementation of our *Safety Improvement Reporting (SIR)*. In the first year we have received nearly 100 reports. And some of these reports have already led to improvements. A big "Thank you" to all of you who have made the effort to write a *Safety Improvement Report*. Twice the problem "Loss of detection in the South of the Mt Blanc" has been reported. The two articles on pages 6 and 7 describe this problem and the

efforts that have already been made to solve this problem, but it also shows that there still remain problems to solve.

Furthermore in Geneva, Zurich and Berne *Local Runway Safety Teams* were mandated to improve the runway safety in a close co-operation between Skyguide, the Aerodrome and the Airlines. The activities of *the Local Runway Safety Teams* should become visible during the next year.

One of the major risk in our airspace are the unauthorised penetrations of controlled airspace. The number of reported penetrations has increased significantly during the last three years. Finally FOCA could be convinced to take care of this problem. A first workshop to discuss the problem "*Luftraumverletzungen*" has been held, where the major representatives of the concerned parties participated. Only due to the fact that penetrations are reported via OIRs we had the statistical evidence to demonstrate the severity of this problem.

Therefore use the OIR-form to report any deviation from required ATM-rules.

Let's come back to *our Safety Bulletin*. The *Safety Bulletin* team tries - in addition to their daily job - to produce a good bulletin every three months. But you are the readers and you have to be satisfied of the bulletin.

Please give us your open and honest feedback about the *Safety Bulletin*. What you are missing or what should be improved or just tell us if the *Safety Bulletin* meets your expectations.

Martin Probst, DMS

Safety Bulletin Team: Editor Martin Probst

Operations Safety Group Denis Droz (Head), Alois Schneider, Christoph Gilgen, Bertrand Du Bois, Heinrich Baumgartner, Lukas Vasatko, Olivier Bussard, Reto Hunger, Rloand Baumgartner **Audit Management** Jürg Bichsel, Peter Scheuber

Risk Management Stephane Barraz **Safety Management** Martin Probst, Thomas Novotny

From the Regulator

About the Implementation of the NLR-Recommendations and the SAFIR Action Plan

The **SAFIR** (*Safety FIRst*) **Action Plan** is based on the mandate by Federal Councillor Moritz Leuenberger, President of DETEC. It strives to improve all aspects of aviation safety management systems in our country with the aim of returning Switzerland in the shortest possible time to the worldwide “champions’ league” regarding aviation safety. This project is strictly forward oriented. It does not consider nor investigate any individual earlier shortcomings by whomever. The aim is to boost the quality of processes and procedures, i.e. the overall safety related performance of all aviation actors in, and out of, Switzerland. For this we need to know if and, if so, where exactly these (partly new) quality requirements have not been met. All organisations, authorities as well as companies, and all its individual members are, therefore, invited to participate within this SAFIR project and to contribute to a supplementary survey with their knowledge

of possibly hidden deficiencies or shortcomings which may be of crucial importance. In this context we follow strictly a “no blame approach” for any unintentional mistakes, i.e. that no one should be afraid of legal consequences of such reporting. There will be none.

We need your professional information and we thank you for your contribution in the interest of this most important and very demanding project’s objective.

In this context you may be interested in another information: We are in the process of drafting an amendment of the Federal Law on Civil Aviation (Loi sur l’aviation/Luftfahrtgesetz) granting what is called “*non-punitive reporting*”. Our aim is to present this draft to the political authorities by the end of March 2004.

Dr. Markus Mohler, DETEC Safety Delegate (Civil Aviation),
Andrea Muggli, DETEC Civil Aviation Safety Officer

New approach in safety oversight

Introduction

The beginning dates back to the year 1997. After the decision by the ministers of the European Civil Aviation Conference (ECAC), Eurocontrol started with the development of the new Pan-European safety standards for air traffic service providers and for states. Those are known as the ESARR Eurocontrol Safety Regulatory Requirements. Some segments are implemented or are in the implementing phase at the air traffic service providers. This concerns the requirements for a safety management system, for the assessment and reporting of occurrences, for the risk assessment and mitigation and for air traffic management personnel. Some segments like software or procedures are still under development at Eurocontrol. Implementation is now progressed in a way, that safety oversight has to start in FOCA.

Change for FOCA

Eurocontrol Safety Regulatory Requirements are mandatory for all Eurocontrol-member states. Switzerland as an Eurocontrol member state since 1992 is obliged to adapt the new safety standards. Mandatory Eurocontrol Requirements are part of the Swiss law.

The implementation of ESARRs enforces FOCA to establish a new safety oversight concept. The inauguration of a new safety oversight concept is a milestone and represents a harvest of the huge preceding work for the definition of the new safety regulation requirements.

Safety Oversight Concept of FOCA

The concept is as recommended by Eurocontrol and is based on international standards for auditing. FOCA-audits are not a redundancy to the already well-known TriNET-audits, which exist since 1998 and which has to be regarded as internal audits as required by ESARR 3. Safety oversight is divided into two main parts

- initial safety oversight and
- ongoing safety oversight.

Safety oversight starts with an intensive initial Audit. An approval will be issued after this audit and after completion of all corrective actions. Ongoing safety oversight is the continuous yearly recurrent auditing and consists of a reassessment audit every third year and of less laborious surveillance audits in the years in between. Follow-up audits might be arranged if corrective actions have to be checked.

Safety oversight has to cover the whole organisation of skyguide with it’s 2 main sites and it’s 12 branches.

Safety oversight might be enriched with announced or unannounced inspections or with specific safety oversight activities if necessary or due to additional specific needs.

FOCA is working on a project for a new IT-tool for a better support of all audit and inspection activities.

Benefits

Safety Oversight helps to ensure, that all actors within aviation fulfill the demands of the traveling public in concern of a safe air travel. Increasing liberalisation and commercialisation are treats to maintain a required high level of safety. Increasing mobility leads to the prerequisite of continuous improvements. A safety management system and specific safety requirements give us the possibility to

achieve, ensure and promote safety systematically. Audits will elicit weaknesses and their reports are navigators on the way to an excellent safety.

Current safety oversight activities

Initial audit for the safety management system, which is currently build-up, is divided into three parts done or to be done September 2003, January and June 2004. The result of the first audit was generally spoken very good but it demonstrates clearly, where strong efforts needs to be made.

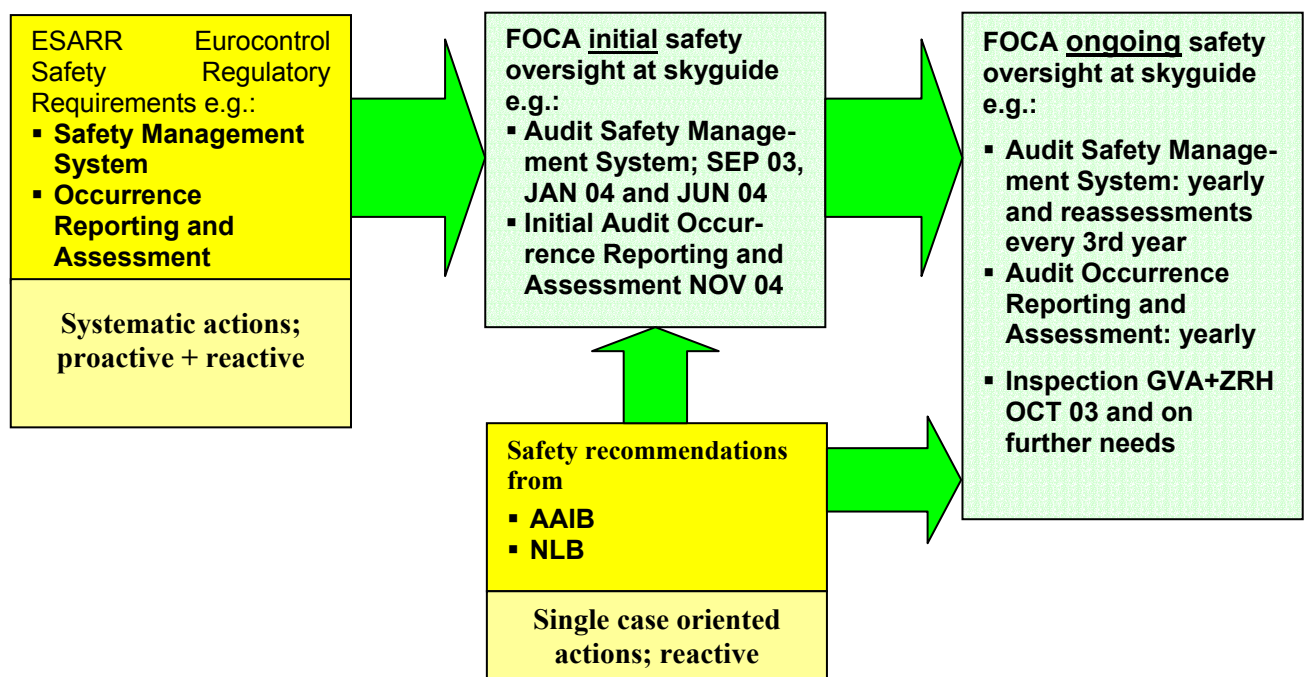
The second audit during November concerned the already implemented assessment and reporting of occurrences. The result of this audit was also very good. But efforts have to be made in the harmonization of the occurrence reporting

between civil and military airports and in the severity classification of the technical occurrences.

The main impediment for the full implementation of a powerful occurrence reporting is the Swiss Legislation, which does not allow a "non-punitive reporting". But as mentioned in the article above this obstacle should soon be removed.

Another audit is planned during February in the field of personnel licensing. This segment is currently under development.

We conducted two inspections during this autumn. One unannounced inspection in Zurich and one announced inspection in Geneva. Topics were headsets, MSAW, no single person operation, STCA, training for rwy 34, information flow from flight crew to ATC, within ATC and to meteo-office especially in case of hail or thunderstorm and some minor items.



Findings with deadlines for corrective actions and intended follow-up are reported in a document and distributed to the responsible in skyguide, to the audit or inspection team and to the client of the activity which is the directorate of FOCA.

Outlook

We are looking forward to a new approach in safety oversight in a culture, which with a holistic view strives to continuous improvement.

*Walter Ott, Auditor Air Traffic Management
FOCA; IP Infrastructure – Planning*

Lessons learned

Human factors in Level Bust

A considerable number of Level Busts are the result of communication errors between pilots and controllers; heading and altitude confusion, call-sign confusion, incorrect read-back or hear-back. The current European figure in the mishear and hear-back/read-back error category is 12%). A study conducted by the FAA has highlighted that the complexity of a message can impact the accuracy of communication errors in ATC. It shows that the number of errors doubles for messages with more than four instructions. Some knowledge about human memory can help to explain those findings.

In verbal communication, which is the most used mode between pilots and controllers, any information goes first to the so called 'verbal acoustic loop' before it is processed by the brain.

This is known as sensory memory. This loop has its limitation in storage capacity. It can contain 7, plus or minus 2, pieces of information depending on the context and environment. In the aeronautical context one digit of a number or one alphanumeric character can be seen as a piece of information that is exchanged between pilots and controllers. However, it is also well known that workload and stress reduce this storage capacity. Nevertheless, the brain does aggregate bits of information. Frequently used information can be memorised and used as one 'block'. A radio frequency used often by a controller will be one element in his working memory whereas for a pilot it may require four or five memory 'blocks'. Conversely, the pilot's memory will aggregate the aircraft call-sign down to one element after many repetitions, whereas the same call sign will remain at four or five elements for the controller since he is rarely using the same call sign for the "reduce to one memory block" process to happen.

Consequently, the same message may well saturate the working memory of the pilot while the controller will still have some unused working memory capacity and vice-versa.

Numbers (in opposition to words) will particularly ask for working memory. The example in the column beside gives an example of the different "memory blocks" of a controller and a pilot.

<i>ABC 2117 climb to FL 290 and turn left heading 325</i>						
Controller						
ABC	2	1	1	7	290	325
Pilot						
ABC 2117	2	9	0	3	2	5

The green "memory blocks" can be memorized easily whereas the red "memory blocks" are more difficult to memorize.

Pilots and controllers compensate for the limitations of the working memory in many ways. For example, pilots try to anticipate upcoming clearances and they pre-select the expected next frequency. Controllers in the same way may assume a heading or altitude change since the aircraft always transits the airspace in the same way each day. Unfortunately, this makes them vulnerable to another pitfall of human nature: when we expect to hear or see something - we tend to hear or see what we expect. For the same reason, catching read-back errors through hear-back becomes a difficult exercise when controllers are under heavy workload.

At the end, it might be worth noticing that the quality of pilot's read-backs very much depends on their degree of alertness. Pilots during cruise phase, or during low traffic at night can be expected to be less "efficient" than during a busy approach phase.

This article is a summary of the Eurocontrol Safety Letter "En route to reducing Level Bust". Available on our SWAN under "operations / safety infos / external".

Thomas Novotny, DMS

Unnoticed wrong read-back

Description of the occurrence

During a calm period at the ACC sector, ACFT A (B762) is transiting at FL250. Seven minutes after ACFT A, ACFT B coming opposite at FL270 establishes contact with the same sector. During its initial contact, it is cleared to descend to FL260. The pilot's wrong read-back of FL240 remains undetected by the ATCO. Two minutes later the STCA goes off. The ATCO's very quick decision to clear ACFT B, passing FL 257, to descend further to FL 240 with an increased rate is good and efficient. Traffic info is given to both aircraft, which cross each other with a minimum distance of 4.8 NM and 800 ft.. No TCAS alert was triggered. It is to be noted that the pilot already made a wrong read-back on the preceding ACC sector.

What happened?

The human "safety barrier" of detecting the wrong read-back failed. The STCA showed its efficiency. An alarm was triggered when the aircraft were 14.4 NM and 700 ft apart. This helped the ATCO to prevent a more severe separation minima infringement. The ATCO was wearing his headset but complained about some noise created by another ATCO.

Consideration

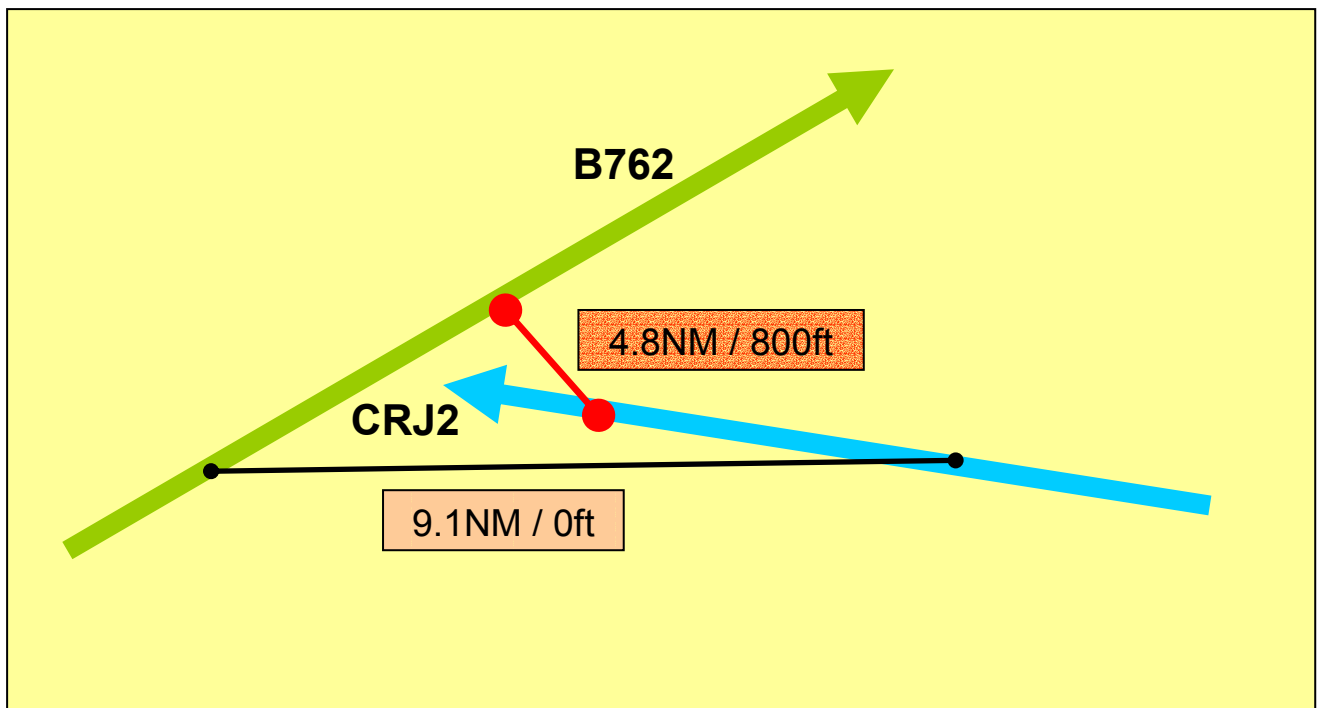
It seems that amongst pilots a tendency exists to rely more and more on the controller's task to detect wrong hear-backs:

"I should not pay too much attention to what is said on radio because anyway if I do not understand the controller correctly, he is there to correct me..." might be the attitude of some pilots.

Recommendation

- If the amount of inputs received by ATCO (R/T, coordination, adjacent centers, etc...) reaches a peak beyond the human multi-tasking skills. **Priority shall always be given to the frequency, and therefore to pilot's read-backs.**

(Referring the "limitations of the working memory" see the article on page 4: Human factors in Level Bust)



Technique

Losses of detection

South of AOSTA – BAVMI / OMETO axis

In 2000 and 2001, an alarming number of losses of detection had been observed for aircrafts in an area over Italy, along the axis defined by BAVMI and OMETO way points, and in the South of AOSTA way point. All the useful radars in this area were losing simultaneously the aircrafts for 30 to 210 seconds.

The analysis of this phenomenon pointed out that some local radio links, working in the same frequency range as the radars, were responsible for electromagnetic perturbations at the level of aircrafts transponders. Unfortunately, even if the airspace is under Skyguide responsibility, these frequencies are under the exclusive responsibility of Italian authorities. The frequencies of these radio links were then reported to Italy to be changed in September 2001 and the problem almost completely disappeared around the BAVMI – OMETO axis, while spontaneously vanishing in the South of AOSTA.

However, a few cases of aircrafts disappearing were still observed from time to time, especially south of AOSTA. It was suspected that there were still some radio links emitting in the radar bandwidth in these areas. All efforts towards the Italian institutions for them to fix entirely this problem stayed unanswered up until now.

Since February 2003, several reports from ATCO suggest a resumption of aircrafts losses in these two regions. In particular, 10 reports in the AOSTA zone have been filed by the controllers.

Therefore, it was decided to reinstate the automatic detection of multiradar losses with the SASS-C tool as already done in 2001. The goal is to provide precise data

on the number and severity of cases, in order to support new actions towards Italian institutions.

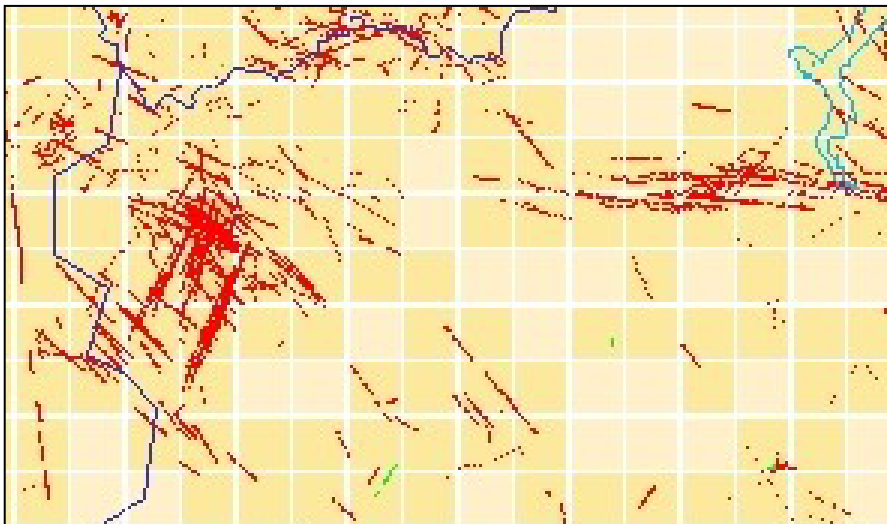
Two different levels were considered during the analysis : On the technical level, the focus was set on radar data output without the extrapolations from the radars, giving a view of the "real" multiradar losses of detection. On the operational level, the data output from the actual Multi Radar Tracker, the MV9800, was taken into account, with extrapolations both from the radars and from the MRT, in order to evaluate the operational impact of these losses of detection, i.e. what the controllers see on their screens.

The two zones are clearly visible on the map, with the highest number of losses for the South of AOSTA. Actually, the amplitude of the phenomenon for AOSTA is unprecedented : there have never been as many losses as now, since the first complains from the controllers in 2000.

Concerning BAVMI – OMETO, the density of losses remains lower than what it used to be around April and May 2001, but it is definitely very much higher than in December 2001, three months after the frequencies of the radio links had been changed.

A subset of the radar data used to generate this map, 18 days of data, was further analysed at the technical level. Only losses of 30 seconds and more were considered. During this period, there were 25 cases of losses over the two regions. This makes an average of, approximately, 1 multiradar loss by day. The duration of these losses are comprised between 30 and 82 seconds, with an average of 43 seconds.

However, most of these losses are not seen by the ATCO, because of the extrapolations made by the radars and by the actual MRT. Indeed, only losses of detection longer than



The map represents the multiradar losses of 30 seconds and more, on the technical level (radar data without extrapolations), above FL100, for the period from July 2003 to September 2003 included (3 months). Each dot represents an absence of detection by a radar for one scan. Red dots stand for FL100 and above, whereas green dots are for unknown altitudes (Mode C absent).

approximately 36 seconds lead to track losses at the output of the MRT. In consequence, only 13 cases out of the 25 resulted in a track loss at the output of the actual MRT. The operational impact of these losses on the new MRT ARTAS / MV PRIMUS will be assessed.

Deeper analysis of multiradar loss cases are being done, in order to provide more precise data on the operational impact (track loss duration), as well as on the concerned aircrafts (call sign or registration number).

Such aircraft disappearance in the area of responsibility of Skyguide is unacceptable and has to be addressed. Each

identified case of loss will be analysed and reported in a future document.

Renewed request to the Swiss authorities (FOCA) was addressed by Skyguide's Safety Management to initiate corrective actions by Italy on these radiolink interferences. Dedicated temporary operational restrictions and detailed information are also planned and studied on the Skyguide side under the supervision of the Safety Steering Group.

Nicolas Brice, TDA

Operational consequences for a loss of radar contact South of the Alps

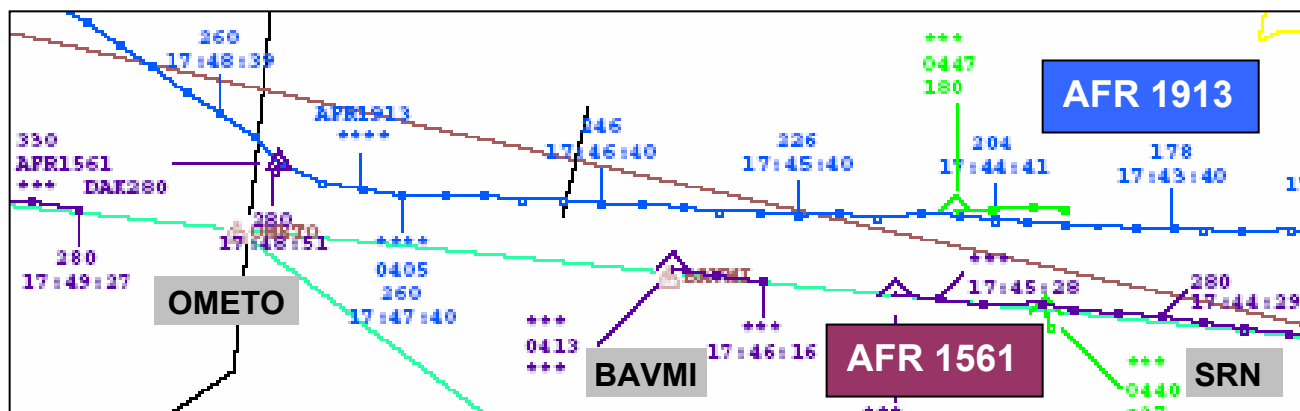
On November 10th 2003, around 17.45 UTC, a loss of radar detection occurred for Geneva Control between two Air France flights South of the Alps (between Saronno VOR and AOSTA). This incident is a good illustration of the problems that Nicolas Brice of our technical department describes in his article about radar detection problems in Northern Italy.

General considerations

From an operational point of view it has to be stressed that even when working in European high density continental airspace radar environment, such as Zurich and Geneva, and even when disposing of state of the art equipment, it is not a good operational practice to rely only, or almost exclusively, on radar observation to provide ATC service. As we air traffic controllers know, starting from ab-initio

school and basic training, detection of a conflict, and resolution of traffic situations has to be done taking into account all sources of information, not just radar.

The possibility of a failure or degradation of our system is always real and a possibility. ATCOs must take into consideration that outages, such as a full or partial radar failure, a radio outage, frequency blocking or a lack of flight plan data (e.g. OLDI failure) can happen without warning and almost instantly. As for the Geneva controllers working the evening of November 10, 2003, it came without warning that an aircraft active in their sector disappeared from their screens. So they were left with just one other indication alerting them of a dangerous conflict: the flight progress strips (the loss of track for flight AFR 1561 lasted for more than 2 minutes, leaving no visible trace on the radar screen of the sector. This loss of contact went beyond the radar "coast function", indicated by a red colored label).



Radar-plot: Time (UTC): 10.11.2003 17:50:46

One may be tempted to say that controllers are required and trained to use all means and technical equipment at their disposal to provide safe and expeditious radar service. Nevertheless, this tells only part of the problem. Working in a high density radar environment with multiple radar heads means that there is a real possibility that some

“shortcuts” are taken, especially when traffic is high, or when confidence in the system is so high that systematic work and full compliance to the procedures (SOPs) is relaxed. This is the reason why we have taken this example, that ended well, to highlight once again, that standard operating procedures and basic controller tactics

remain valid and must be used without exceptions and/or deviations.

Circle of confirmation

Similar to what is done in cockpits, especially in smaller aircraft without sophisticated autopilots, FMS or EFIS systems, the basic piloting skills, such as applying a standard scan of all vital instruments, is what brings safety, especially when flying in IMC and without outside reference. Same goes for ATC, even when full radar service is provided and apparently no technical problems are to be reported or to be expected. This scan, or "circle of confirmation" as it is called commonly, is a systematic scanning between the situation presented on the radar screen, using the flight progress strips as confirmation and back-up. In a climb or descent situation the relevant flight progress strip has to be taken out of the stack, handled by the controller delivering the clearance, moved physically up or down the other strips of the sector, and, during the passage it should be checked that no conflict exists on the radar and that all flights are visible and well separated. This is basic controlling skills and part of our routine, not just nuisance and hindering of efficiency. This is particularly true for zones and areas of known radar problems, where this routine of a good radar controller is essential and part of standard working procedures.

Conclusion

As seen on November 10, 2003, the systematic and full use of all data prevented a very dangerous loss of separation in the region South of the Alps where there is a known history of poor and insufficient radar coverage and tracking. It cannot be stressed enough that standard working procedures, such a learnt in basic ATC training, remain valid and will continue to remain valid for some time. This even when more and more sophisticated ATC equipment and better tools to perform our job will appear and be implemented.

I don't want to conclude this small reminder without mentioning that I am very worried, I would even say utmost concerned by these repetitious incidents of bad or insufficient radar coverage and radar tracking South of the Alps towards Italy. Urgent action is required as this is a real safety concern for SKYGUIDE, not just Geneva. As we all know, human errors occur, and despite all our efforts and actions to prevent them, when they happen in a moment when the ATC system is already weakened (e.g. no STCA available due to lack of detection), the consequences can be grave.

*Christoph Gilgen
Safety Officer ACC/UAC Geneva,
Member of OSG*

Risk Management

The ZAP-DVO2 Safety Assessment

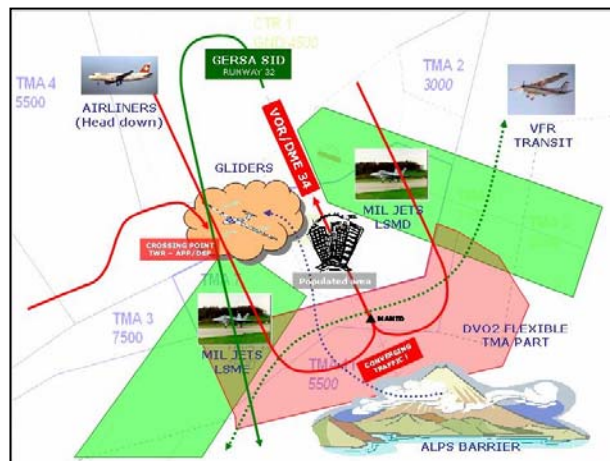
At the beginning of 2003, our CEO Alain Rossier endorsed together with the national regulator the skyguide Risk Management Policy. This document defined the steps for a reasonable transition towards an ESARR4 compliant Risk Management System. The heart of the process is based on our ability to formally identify and mitigate the Risks resulting from the introduction of new Systems or modification of existing ones. This is usually done by the means of well organized Safety Assessment Programs delivering Safety Case Documents providing the formal demonstration that the assessed System can be considered reasonably Safe. Based on a "learning by doing" approach that lies within the frame of its Risk Management Policy, skyguide formally addressed this year the Risks associated with several ATM-related Systems. This article is fully dedicated to the presentation of a concrete Safety Assessment Program. Due to its high level of actuality, ZAP-DVO2 has been chosen for that purpose.

To accommodate the approaches in Zürich in order to take into account the overflight restrictions requested last year by the German government, our transport minister, Mr. Moritz Leuenberger, negotiated and proposed a political agreement based on the progressive implementation of "Wochenendregelungen".

After rejection of this proposal by the Zürich political bodies, this agreement has been replaced by more stringent unilateral measures named "Durchführungsverordnung" or simply DVO. The changes required to be compliant are actually being introduced by skyguide in three steps within the frame of the **ZAP/NBR project**¹.

The first step (DVO1) has been introduced April 17th 2003, the second step (DVO2) October 30th 2003 and the third step (DVO3) is in preparation for next year. For the purpose of DVO2, the introduction of VOR/DME based approaches conducted from the south of the airport towards runway 34 has been necessary and required important modifications of the airspace structure. Arrival and departure routes together with the skyguide operational concept have also been adapted and technical modifications on the existing equipment realized accordingly.

To go a little bit more into detail, let's consider the main consequences of the changes that have been implemented by DVO2 on the 30th of October 2003:



- Non-precision approaches are conducted from the south of the airport between two important military operations areas.
- Aircraft are vectored in a convergent way towards runway 34 final approach path located between a dense populated area and the alps barrier.
- The airport is used from the south in a converging and crossing runways situation, resulting in complex and new wake turbulence situations.
- The usage of new IFR departure procedures results in the presence of additional crossing points and altitude constraints.
- Operations taking place in the southern part of the airport are conducted in a flexible airspace structure that may be crowded by General Aviation traffic

According to ESARR4 requirements, skyguide was expected in such a situation to conduct a formal Risk assessment process before going into operations. For that purpose, a Safety Assessment Program has been launched at the beginning of the year and conducted based on the following overall Safety objective:

" To make sure that the changes introduced by the implementation of DVO2 airspace structure and procedures don't result in remaining unacceptable Risks which have not been properly mitigated "

Dedicated working sessions gathering many aviation experts from various domains (e.g. general aviation, military operations, ATC operations and flight operations) allowed the identification of 34 Risks amongst which 13 have been judged unacceptable, 11 tolerable and 10 acceptable.

¹ ZAP/NBR states for "Zürich Adaptation Program / Neu Betrieb Reglement". It is a common program between skyguide and Unique which has been launched in order to rethink the overall operational concept of the Zürich airport.

By merging these Risks into a set of generic **Key-Risk Factors**², it has been possible to establish a global Risk picture and to formally demonstrate why and how **Safety Barriers** shall be put in place by the means of the implementation of well defined **Safety Recommendations**. To complete the process, the predictive impact of these Safety Recommendations on the achievement of the Safety Barriers has been formally described in order to demonstrate their effectiveness.

To summarize the situation, let's have a look at these Key Risk Factors and consider them as the most relevant contributors to the development of potential unsafe situations:

1. Illegal controlled airspace sectors penetrations by General Aviation pilots having a significant lack of understanding in global ATC operations conducted in the area.
2. Increased System complexity resulting in a large reduction of Safety margins due to numerous compromises made by *skyguide* under directives issued by FOCA in order to allow maximum airspace usage to all kind of traffic willing to fly in the area.
3. Introduction of a new non-precision IFR approach conducted towards converging runways and located in a complex and mountainous airspace structure potentially crowded by heterogeneous non-professional traffic.
4. Increased joint civil and military operations affecting traffic that shall be coordinated by three different jurisdiction geographically de-located.
5. Introduction of significant changes impacting the whole aviation community and requiring proper information management in order to avoid the development of unsafe situations.

It would be too long and out of the scope of this article to present the complete Risk mitigation plan that has been established to counteract these factors.

But let's nevertheless consider an example by having a look at the Risk mitigation strategy affecting **General Aviation operations**³. The implementation of Safety Barriers has been based on the following principles :

- Close immediately airspace to General Aviation during southern approach operations.
- Train General Aviation pilots during winter time under institutional supervision.
- Reopen airspace to those pilots having received and successfully completed the training.
- Reinforce FOCA position towards airspace illegal penetrations and prosecute violators.

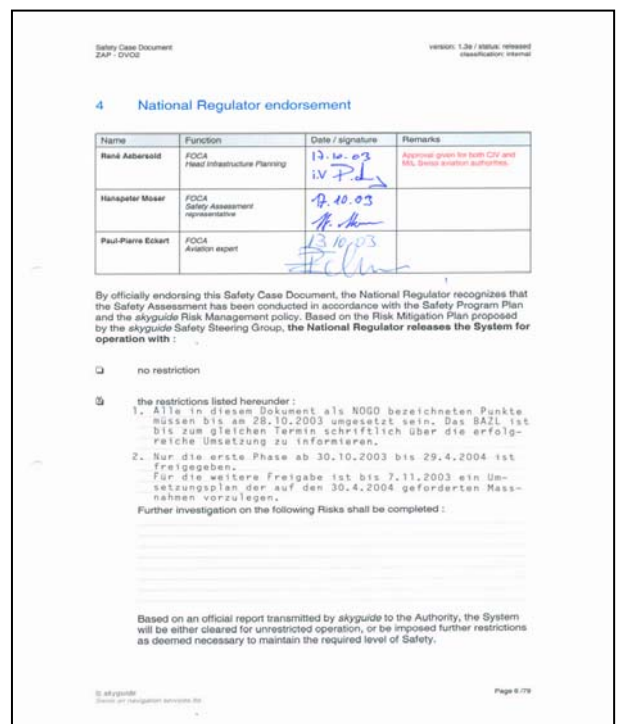
² Obviously applicable to DVO2 operations only.

³ Addressing the Key Risk Factor 1, e.g. illegal airspace penetrations by General Aviation pilots.

The table extract presented on the next page shows the way it has been formatted in the Safety Case Document and submitted to the management bodies for validation.

It is basically a global summary depicting how the identified Key Risk Factor is counteracted by a specific initial Safety Barrier and how this barrier evolves in time with the implementation of additional Safety Recommendations.

After having addressed all Key Risk Factors the same way, the final Safety Case Document has been released by *skyguide* on the 8th of October 2003 and the proposed Risk Mitigation plan conditionally validated by the National Regulator as depicted hereafter.



Based on the experience gained within the frame of DVO2, the Safety aspects of DVO3 will be addressed next year with the same approach.

To conclude, I'd like to take here the opportunity to sincerely thank all the people involved in this Program and especially the members of my team⁴ for their high level of professionalism, excellent work, constant availability and active contribution.

I remain at your disposal for any question or comment you may have on the subject.

Stéphane Barraç, DMR

⁴ The ZAP-DVO2 Safety Assessment Program team has been composed of the following aviation experts : Reto Hunger, Emil Heeb, Beat Werffeli, Christian Weiss, Jürg Kobert, Armin Hunziker, Paul-Pierre Eckert and Hanspeter Moser.

KEY-RISK FACTOR	SAFETY BARRIER	SAFETY RECOMMENDATIONS	PREDICTIVE IMPACT
<p>KRF01</p> <p>“ Illegal controlled airspace sectors penetrations by General Aviation pilots having a significant lack of understanding in global ATC operations conducted in the area ”</p>	<p>BY OCT30-2003 / NOGO</p> <p>Airspace is closed to General Aviation during DVO times.</p>	<p>SR01</p> <p>Introduce a new "Restricted" area comprising TMA710/1 (GND to FL105) and close it to CIV/MFR operations during DVO time active</p> <p>SR02</p> <p>Establish permanent FIC and request mandatory radio contact during daylight hours and DVO time active</p>	<p>Significantly reduces the Risk of unwanted and/or illegal airspace penetration resulting in potential conflictual situations.</p>
	<p>BY APR30-2004 / SUPPORTING</p> <p>The usage of airspace during DVO time is limited to qualified pilots only.</p>	<p>SR03</p> <p>Review DVO2 airspace structure and AT C procedures taking into account the considerations made during the Risk mitigation sessions and the SIRX030903. Improve pilot documentation accordingly by publishing dedicated DVO chart(s).</p>	<p>Increase of Safety Margins available to react in case of unwanted or illegal airspace penetration.</p>
	<p>SR04</p> <p>Define and organize under FOCA institutional control a General Aviation pilots DVO training recognizable by official endorsement.</p>	<p>SR05</p> <p>Conduct General Aviation pilots training and re-open progressively the "Restricted" airspace to those having fulfilled the training requirements.</p>	<p>Develops ATC operations awareness and significantly reduces the Risk of unwanted and/or illegal airspace penetration.</p>
	<p>BY DEC31-2004 / SUGGESTED</p> <p>The usage of airspace is regularly controlled by appropriate policy measures.</p>	<p>SR06</p> <p>Introduce MLL controlled airspace surveillance by the means of "spot-checks" conducted by jet fighters within the whole LSZH area.</p>	<p>Significantly reduces the Risk of illegal airspace penetration.</p>

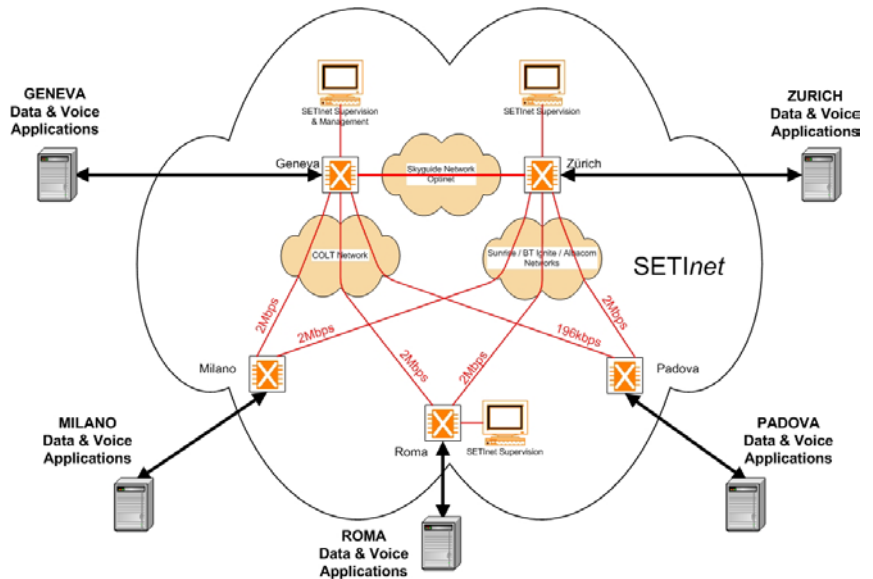
SETInet

Form the causes to the consequences

The project SETInet

SETInet project consists of the migration of the leased lines between Switzerland and Italy towards a proprietary multiplexed network which will be used as a common carrier for ATC applications. Mainly voice and OLDI data transportation are used for coordination and transfer functions between control centres.

As nodal system for Swiss and Italian operations SETInet is designed with the objective to offer high reliability and quality of service. Complete redundancy for hardware and diversification of Telecom operators links are implemented to meet the objective.



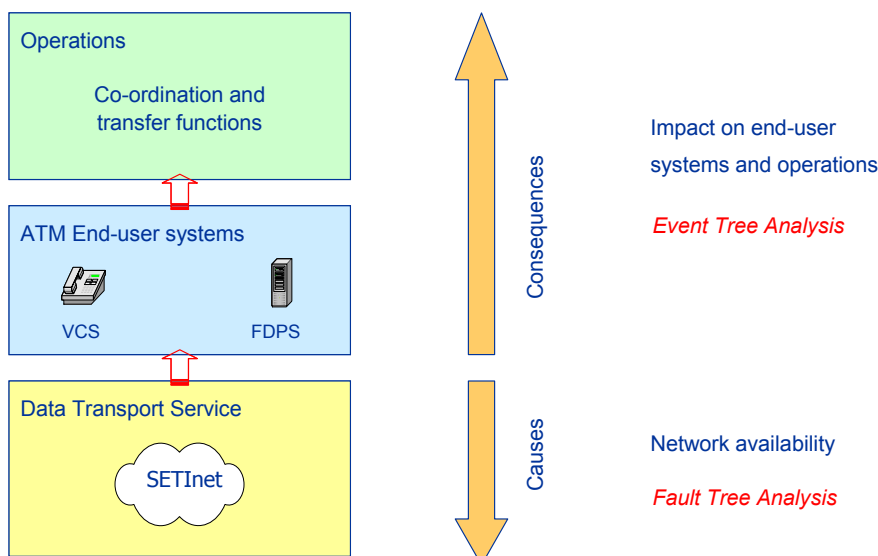
The Safety Assessment

A demonstration that SETInet will provide a service as safe as today could be considered as the most direct and efficient approach. Nevertheless statistical figures related to the existing systems are limited and would require a deep investigation to compile failure rate figures.

Furthermore SETInet will concentrate on the same medium ATC applications between Switzerland and Italy carried so far by individual leased lines. This issue is considered as a

major safety critical aspect and has to be appropriately addressed.

Taking into account all these elements it was decided not to limit the safety assessment to a network analysis but to consider in a wider scope the impact of unavailability of SETInet service on end-user systems and operations. Two complementary analytical techniques were used to carry out the overall Safety Assessment Program :



Event Tree Analysis

Fault Tree Analysis

The *Fault Tree Analysis* is a deductive logic model technique. It begins with a stated top level undesired event and uses logic diagrams to identify single events and combination of events that could cause the top event.

Loss of provision of data transportation between Switzerland and Italy were taken as feared events. Contributors (hardware components, telecom operators links) have been identified with their probability of failure. The result of this quantitative assessment is a set of predictive availability figures for the SETInet service between the different locations.

The *Event Tree Analysis* is an inductive technique used to identify, describe and assess the consequences that can result in case of the occurrence of a potentially hazardous event.

This logic representation examines all possible responses to an initiating event in the sequence they are activated.

The initiating events considered were the loss of provision of data transportation between Switzerland and Italy quantified previously. This method allowed the identification of outcomes corresponding to the different steps of degraded modes.

The situations were described and the risks associated were assessed in term of severity and likelihood. A clear picture of the consequences on the operational functions could be obtained in particular for the situations where SETInet failure impact simultaneously FDP and VCS functionalities.

Main outcomes

The achievement of the Safety Assessment Program led to a set of safety recommendations. Some of them have been qualified as mandatory to consider the system safe for operational use. They are presented hereafter in two distinct groups.

Generic recommendations addressing the global framework of the Safety Assessment Program are essential to validate the overall approach:

- Presentation of the results of the study and awareness actions to convince Italian partners to adopt a similar approach on their side.
- Verification of the context of application of OLDI standard and Letters of Agreement.

Specific recommendations related to SETInet environment are means to maintain or improve the service level delivered to end-user systems :

- Periodical review of the telecom operators concerning the network topology and the diversification of leased circuits.
- Appropriate repartition of spare material on the different locations.
- Provision of a statistical tool to monitor the service.

Additional recommendations addressing directly the end-users systems (Voice Communication, Flight Data Processing) have been proposed and can be considered as safety requirements for future evolutions of those systems.

Jean-Marc Bory, TSS

What is actually going on ?

To give you on a regular basis a short overview of the main activities that are running in the Risk Management domain, the following table will from now on be presented with the

Risk Management rubric. For any question you may have or for deeper details on the subject, please contact directly the person in charge of the related Safety Assessment.

Safety Assessment Programs status			
System	Responsible	Status	Target date
ASR-10 GVA	S.Barraz	Running	09.12.2003
PRIMUS	JM. Bory	Running	2004
ZAP-DVO3	S.Barraz	Initialized	2004
ATMAS	F.Balda	Initialized	2005
UAC/UTWG	--	Standby	--
UAC/Radio concept	--	Standby	--
FDP-ZRH	--	Standby	--
SEPAGE/CLARINES	--	Standby	--
SAMAX	--	Standby	--
ZAP-DVO2	S.Barraz	Achieved	29.10.2003
SETInet	JM.Bory	Achieved	30.09.2003
TWR-ZRH	S.Barraz	Achieved	10.06.2003
IFREG	JM.Bory	Achieved	11.02.2003

Running

Mandate is officially attributed by the skyguide Safety Steering Group, Safety Program Plan is validated, Safety Assessment Program team is constituted and working sessions are running.

Initialized

Mandate is officially attributed by the skyguide Safety Steering Group and Safety Program Plan is under preparation.

Standby

Pre-evaluation of the feasibility, added value and required resources necessary to the completion of a Safety Assessment Program is done. Decision from the skyguide Safety Steering Group is required.

Achieved

Safety Case Document is delivered and officially endorsed by the skyguide Safety Steering Group and when required also by the National Regulator (FOCA)