skyguide

safety bulletin

Inside this issue

2 **Editorial**
New S, Simon Maurer, presents himself

3-4 **Safety Nets**
ACAS and STCA - cohabitation or competition?

5-6 **The human factors column**
Human error across ages

7-8 **Technics**
Skyguide Technical Competence Model

9 **Safety Policy**
The «good-looking» version is now available

#23 JULY/AUGUST/SEPTEMBER 2008 – www.skyguide.ch/dossiers/safety management
editor: thomas.novotny@skyguide.ch - intranet: skyline/issue/safety/safety bulletin

Dear colleagues

I should probably introduce myself first, and then tell you a bit more about my background: my name is Simon Maurer, 40 years, married, three kids (all girls). I am the new Head of the Skyguide Safety, Security and Quality Department, and will be in charge from January 1st, 2009.

So what did I do before joining Skyguide? After the Matura in Basel, I went on to the Diploma in Experimental Physics at the Basel and Lausanne Universities. Lucky enough to be accepted in the Swissair Pilots School, I decided to step into professional aviation in 1994. As Swissair didn't hire pilots at that time, I only started flying in 1998, on the Airbus fleet. Leading operational projects for Swissair (and then Swiss), I learned more about the Aviation system and the people in it.

In hindsight, I don't regret the decision, but in 2004, I wasn't so sure: I left Swiss to become the Deputy of the Civil Aviation Safety Officer at DETEC, a function yet more on the systemic level. During that time, I completed the MTEC studies (Swiss Federal Institute of Technology's MBA). You bet that when Skyguide was seeking the Head of it's newly created Safety Department, I couldn't resist.

Arrived on September 1st at Skyguide, I have now time to focus on learning. It started with a one-week Safety course chez Sidney

Dekker at Lund University in Sweden.

Sidney was speaking about «Newtonian», linear accident and system models, about complex linear models, and about the current dynamic, nonlinear system models, and people like Heisenberg, or Bohr. Of course that rang a bell – be the parallel just accidental or not, the similarity to the development in Physics is obvious.

At the end of the 19th century, it was believed that the biggest problems in Physics were solved, and that the model was more or less complete. These were the complex linear models, basically still Newtonian, which described the behavior of the macroscopic world. But it was far from over! New and better experimental technology yielded results that could not be explained at all. The macro model desperately needed extension, giving birth to completely new ways of thinking, if not a new culture – Quantum mechanics, the Physics of probabilities, and Relativity, just to name a few.

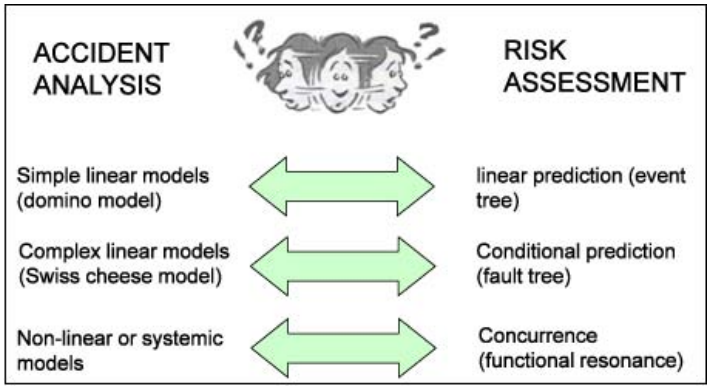
Also in Safety, we have to think ahead in order to maintain today's levels. The linear models (such as the linear Swiss Cheese models with its «barriers») aren't all wrong, but aren't right either – they need extension or, rather, revision. Not only in Aviation, we are facing complex, highly coupled socio-technical systems, systems which cannot be unambiguously decomposed into the (Newtonian) mechanics for the identification of single causes for mishaps (and quick-fixes). That doesn't mean that we can't find improvements of course; but rather that they should be based on a set of consolidated data, and probabilities (risks), not single events.

With the establishment of the new Safety Department, Skyguide has paved the ground to meet today's and the coming Safety challenges. I am happy to lead that Department and to go ahead in Safety, to bring appropriate theories into application together with my expert team.

Looking forward to see you all

Simon Maurer
s

P.S. If you think that e.g. Einsteins Theory of Relativity is «only» a theory, playground for the researchers, you're wrong: Today's GPS would be unusable without taking into account relativistic effects.



Picture: models for accident analysis and risk assessment (Hollnagel, 2006)

ACAS & STCA - cohabitation or competition?

Interoperability it certainly is not! At least not in the near future.

This summer yet another sad anniversary of the Überlingen catastrophe passed and still nothing significant has changed at the systemic level when it comes to the Short Term Conflict Alert (STCA) and Airborne Collision and Avoiding System (ACAS) cohabitation in today's worldwide ATM system!

What needs to be changed, what is the issue here, when can it be changed for better… how much, what, how… many core questions are arising…

For some we have answers, for some the answers are pending the outcomes of major studies and data collection efforts, but still for some others we will have to wait a good few years until emerging technologies and the interaction with existing systems consolidate. A long (too long) process for the resolution of the safety critical issue?

Unfortunately, the «issue» has become identified as THE Issue only recently (few years ago).

So, what is THE Issue?

ACAS and STCA were developed completely independently and aimed at similar, yet very different roles in ATM. At the time of their emerging, a clear need for Safety Nets in the ATM system was already identified, however the drivers, operational requirements and envisaged roles were established with no vision of their future cohabitation (let alone interoperability) once they started performing in the real world. Have these lessons been learned?

ACAS was standardized through ICAO Annex 10 Volume IV – seeing the light of day as the only available product on the market compliant with these ICAO established standards – in the form of TCAS (of which several versions have been put into operation).

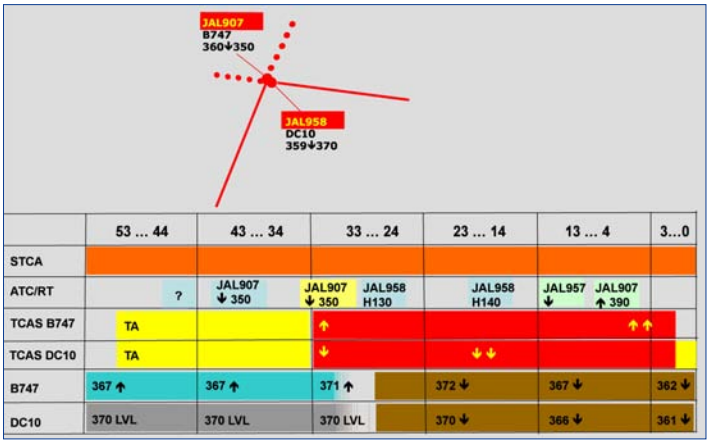
STCA, however, was developed world-wide at several different locations with numerous variations of operational, environmental, safety and other (read - business) requirements resulting in hundreds of different performance settings.

All this uncoordinated (until recently) effort ends up in a real world overwhelmed with an ever growing quantity and complexity of air traffic causing possible nightmare scenarios in situations where one would (rightly) expect that technologies, procedures and humans would be performing according the clearest & safest possible standards.
The problem – as easy as it might sound - is simply the fact that cognitive loop between ATCOs and pilots is not closed resulting in many layers of possible misunderstanding. Namely, ATCOs are not aware whether an aircraft is following a TCAS RA (Resolution Advisory) unless advised by the flight crew, and issue instructions in an attempt to resolve the conflict.

This results in the situation where an ATCO instruction (triggered by STCA) reaches the cockpit during or immediately before a TCAS RA triggered action commands the flight crew standard operating procedure. Simply, ACAS RA directs one line of action and ATC something else, or even exactly the opposite.
In late January 2001, a «yellow card» was issued to the world wide ATM community through the Yaizu accident:

- Two wide-body aircraft carrying 700 people missed each other by 30 meters at FL362
- Dozen of people were injured – several of them with broken spines confined to wheel-chairs for the rest of their lives

What happened:



1. B747 was in climb passing FL367 while DC10 was maintaining FL370
2. STCA sounded 53" before the Closest Point of Approach (CPA)
3. At approximately the same time onboard both aircraft, a TA (Traffic Advisory) sounded
4. 43" before the CPA, ATC issued a «descend» instruction to the climbing B747 in an attempt to resolve the developing conflict (this action looks very much like the scenario of the mid-air collision over Zagreb – Yugoslavia, at the time, in 1976)
5. A few seconds later, TCAS RA ordered pilot of B747 to climb
6. B747 followed the ATC instruction instead, ignoring the TCAS RA, but kept visual contact with the conflicting DC10
7. Strengthening RAs sounded in both aircraft, but by that time the only way out of trouble was by the pilots having each other's aircraft in visual contact

ACAS & STCA - cohabitation or competition?

The forces involved in the last avoiding maneuver (push and turn) are best illustrated by the fact that a drinks trolley flew through the ceiling of the B747 passenger cabin (see photo).

Does this scenario resemble also the Überlingen one? Almost 1: 1 in many aspects!

Even though ICAO has since changed the procedures (both ATC and airborne sides) in order to mitigate for similar situations, the statistics available indicate the improvement is yet to be observed.

Similar events have occurred again! The two sides are still divided conceptually:

- they have access to two different alerting systems
- they might have divergent plans
- they are not informed about each other's plans
- they might work in an overlapping time frames
- they are working under extreme pressure

Pilots are still reporting RAs on the radio very late or incorrectly, so ATCOs simply continue to provide instructions since they are still not aware of the ongoing RA. Despite ICAO is clearly promulgating that the flight crews shall follow the RA even if the ATCO instruction imposes a different line of action – this is still far from always being the case in real life.

All mentioned is now an established fact – but it wasn't always like that. THE Issue was already partly addressed through an attempt to investigate the «down-linking of RA», through two (inconclusive) studies conducted by Eurocontrol (skyguide provided ATCOs) and some other efforts.

However, it seems that the «point of no return» was reached when:

- In October 2006 an STCA Related workshop was held in Eurocontrol-Luxembourg, where skyguide presented the STCA concept – highlighting the STCA/TCAS competition/cohabitation issue
- Even though the focus of the presentation was a general overview THE Issue seemed to catch most of the attention of the participants
- As a follow up, the Deputy Swiss Civil Aviation Safety Officer (coming Chief Safety Officer – «S»- of skyguide) established contact with the skyguide SNTF (Safety Nets Task Force) in the attempt to get more answers and possibly to initiate a Safety Project Directive in this regard.
- Very soon, it became clear that this is not an issue that can be resolved within Swiss boundaries and the initiative involved Eurocontrol
- This cooperation resulted in the excellent (by invitation) workshop held in skyguide in Dübendorf involving the FAA, Eurocontrol, the industry…

Today, only two years later, as a follow up on this «innocent attempt» to present THE Issue the **P**erformance and safety **A**spects of **S**hort-term Conflict Alert – full **S**tudy (PASS) project is ongoing (skyguide participating), the I AM SAFE preliminary project is finalized and a few other major undertakings are either ongoing or about to be launched. All this effort is planned to be structured through SESAR in a way that should bring these two Safety Nets «loose ends» together, finally overcome the competition/cohabitation situation and bring in **interoperability**.

Isa Alkalay / OOTP
Skyguide SNTF Chairman

Human error across ages

It will be the theme of this article to explain a little bit how the ideas about «human error» have evolved over time depending on the historical background, and why they are therefore essentially a product of our history and culture.

It is crucial in order to follow the article to understand that we, humans, can hardly live with uncertainty. We absolutely need to understand the world in which we are living. As a species, we humans, feel very insecure if there is something about which we can not find an explanation. The Newtonian-Cartesian way of thinking is one of the responses to that. In this sense if we observe an effect, we straightforwardly assume that there must be a cause somewhere. Actually, finding a cause or an explanation to an event is much more important to us than to understand what happened[3].

«The quest for certainty blocks the search for meaning»
Erich Fromm, U.S psychologist

To illustrate this theory we might say that it is often our first reaction to blame those who question our representation of the world. Nowadays for example an «erratic» practitioner might hamper the safe system in which we desperately want (need) to live, and will therefore often be prosecuted for the sake of keeping our beliefs about the safe system intact. Going back some centuries ago Galileo questioned the agreed-upon fact (by church) that the Earth was flat und therefore underwent serious troubles. Example here are obviously numerous but citing them would be fastidious and useless.

Dark Ages and witch-hunting

From the «Dark Ages» until Renaissance (14-17th century), and even Enlightenment (17-18th century) Europe was in a witch-hunting period where deviants (mainly from catholic church) were considered hopeless or even dangerous witches or wild beast. As such these deviants were treated with methods whose cruelty is unparalleled in history[1]. It is argued here that the present urge to search for human agents of misfortune and their following prosecution (in the aftermath of a disaster) might be considered as a modern peak of witch-hunting[2]. The difference is that the present miscreants (poor practitioners) are prosecuted more fairly in appearance and that the cruelty is of sole psychological nature, probably. Then the question here is whether this kind of «modern witch-hunting» is really basically very different, if at all, from what supposedly more primitive people have been doing?

Industrial revolution

With the arrival of the steam engine, cotton spinning and iron founding, new technology surfaced and related new opportunities for errors were mainly managed with a predominant focus on technical components. Therefore in the second half of the 18th century some uncertainties about our ability to control human destiny were dampened through the improved comfort of people and the reduction of the risks in certain areas of life. Consequently during this period the search for human errors and its associated blame cycle was attenuated, but only temporarily as we will see thereafter.

Modern Ages

Erik Hollnagel in his book «Barriers and Accident Prevention» has been through a period of accident analysis of about 50 years and has finally extracted the following graphic out of it (admittedly rather theoretical than empirical):

It is fundamental here to understand that the curves display what has been found in the investigation as a cause, meaning not necessarily the «true» cause. As we do not like to live in uncertainty a cause is always attributed and then the contributors need to sum up to 100%.

Going back to 1960, it would be rather unusual to attribute a cause to organizational factors. During the last half of the 20th century the technology became more and more reliable, this explaining why the technology curve decreases until reaching some kind of «minimum» level as a contributor to around 10% of accidents. As technology became more reliable therefore logically another contributor needed to compensate for this good score: the human error became a more and more «sexy» cause for mishaps… Indeed many recent studies suggest that the human contribution to accidents is around 90 %!!

So until late 70s people involved in accident analysis were quite happy with attributing the cause to either technology or humans, with the «lead» of contributing factor shifting slowly from technology to humans. However in the early 80s a third category began to emerge (organisational factors) with the nuclear accident at Three Mile Island U.S. in 1979 as seminal event.

Human error across ages

This accident clearly demonstrated that it was not enough to look into human and technological causes. So while technology continued to improve, the human contribution then started to decrease in favour of the organisational causes. Following this trend literature about organisational accidents and safety culture became quite common since the middle of 90s.
In summary we switched the focus from technology to human performance, then to human-machine mismatches and finally to organisational causes. As Simon Maurer adressed in his editorial there are plenty of different views about accidents (Domino model, Swiss cheese etc..) which development followed the evolution described here, however it seems that safety practitioners essentially found new categories whereas the stereotypical way of thinking about accidents essentially remained the same.

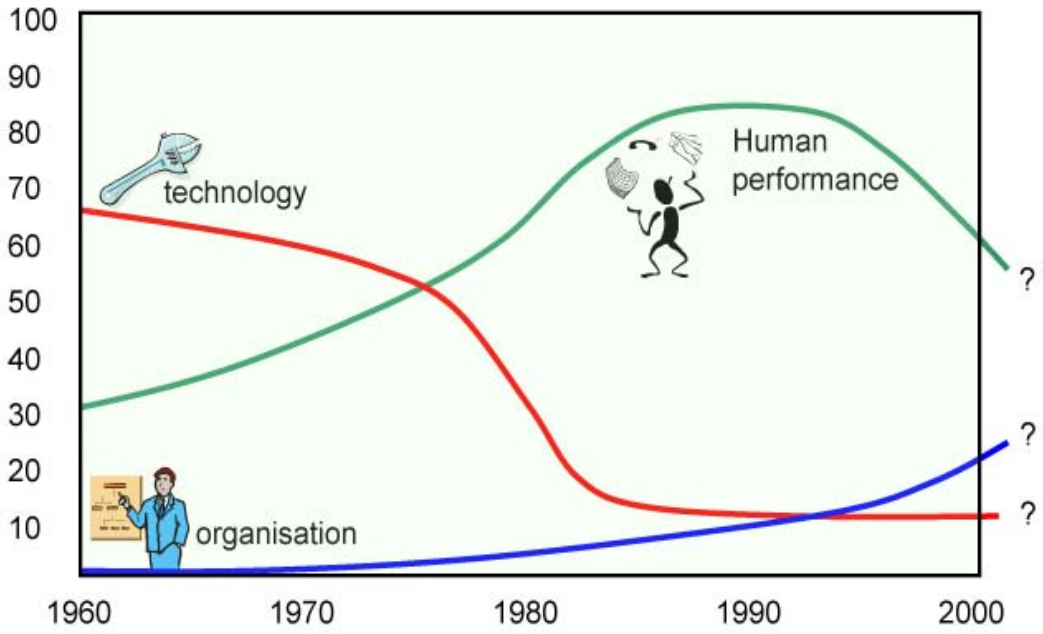


Figure: trends in attributed accident causes (Hollnagel, 2004)3

Going back to the beginning of the article I hope that the point has been made that our way of attributing causes (and human errors) is deeply intertwined with our history and culture. This meaning that as our society is constantly evolving then our understanding is constantly changing, this implying that our assessment about causes is constantly questionable… The organisational factor (arguably the faulty practitioner) is the present witch, who's next?

THOMAS NOVOTNY
Safety Development, SDE

1 *Rotenberg M. (2003), Damnation and Deviance*
2 *Barraz S (2008), Homework for Master thesis at Lund university*
3 *Hollnagel, E. (2004) Barriers and Accident Prevention*

Skyguide Technical Competence Model

For many years, skyguide relied on professional ethics and training to ensure that Engineers and Technicians were competent to fulfill their responsibilities. «Old timers» taught newcomers how to do the job competently. Shortly after the millennium turn, Eurocontrol published ESARR, a set of safety requirements that forced skyguide to migrate from a company dominated by the sense of professional ethics to a regulated industry. Among these requirements, the technical organisation had the leadership and responsibility to establish frameworks capable of demonstrating that:

- the technical tasks are performed by competent people experienced enough to operate safety-related equipment properly,
- the lifecycle of technical equipment is managed in a repeatable and predictive way,
- the risks associated with interventions on technical equipment are identified, mitigated and properly communicated to every stakeholder.

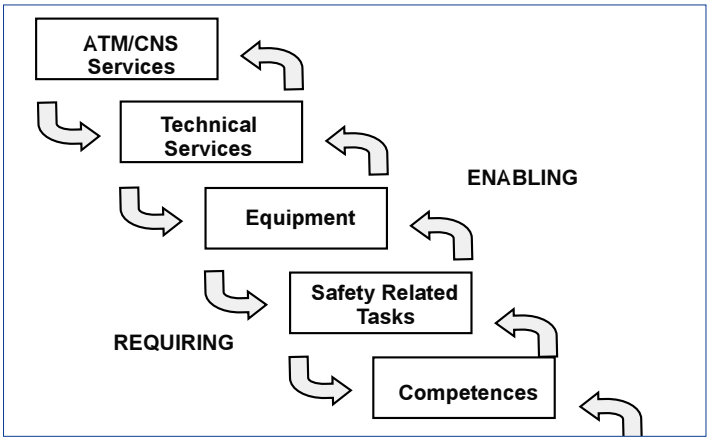


Figure 1: Assurance Rationale

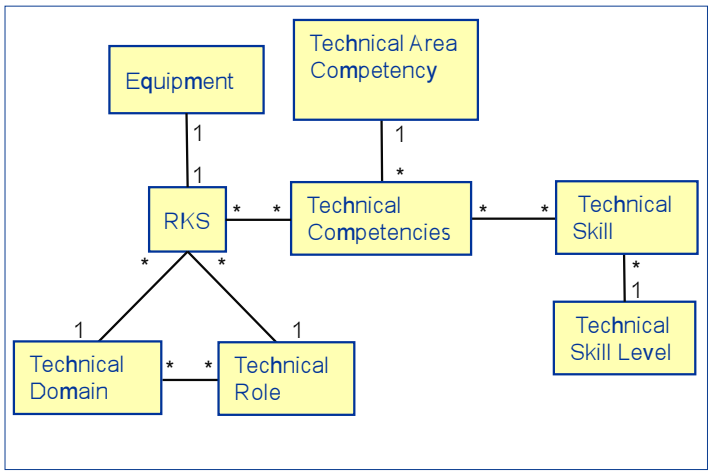


Figure 2: RKS Design

Competence vs. Training

Figure 1 presents the contribution chain of competence and training toward the safe ATM/CNS service provisioning. It clearly distinguishes competence from training, and defines training as means to acquire competence. The challenge was really to separate these two concepts that were previously deeply intertwined.

ATM/CNS services supplied by Air Traffic Controllers are using technical services. These technical services are delivered by equipment e.g. Flight Data Processing, Radio, Instrument Landing System (ILS), which are operated by technical people called Air Traffic Safety Electronics Personnel (ATSEP). Operating this equipment means, for example, performing deployment and maintenance tasks. These tasks are defined as the Safety Related Tasks (SRT) for which the ATSEP shall have proven competences, acquired through training. Training may take several forms depending on the competence nature to be acquired as explained later on.

On the other hand, training enables the acquisition of competences, necessary for executing safety related tasks on a given piece of equipment, which provides functionality contributing to the technical services used to deliver ATM services.

ATSEP Certification

An ATSEP is a technical personnel working on equipment, as being a member of the company or not e.g. maintenance contractor. A compliant-ESARR5 framework for ATSEP is organised around three pillars that are Technical Competences, English fluency, and Medical Fitness. ESARR5 sets requirements on ATSEP medical fitness. However the Swiss law does not allow to formally assess the medical fitness of staff members. Therefore skyguide circumvented this constraint by addressing the doubt related to the medical fitness instead. The ATSEP is certified when it can be formally proven that the ATSEP acquired these competences, is fluent in English and there is no doubt regarding its medical fitness. ATSEP Certification is valid for a two-year time period. The skyguide implementation makes possible to update the ATSEP competence as often as the ATSEP Safety Related Tasks evolve without the need for new certification.

What is the competence?

The competence is the ability to undertake responsibilities and to perform activities to a recognised standard on a regular basis. Competence is a combination of

Skyguide Technical Competence Model

practical and thinking skills, experience and knowledge. Competent people are those with the right skills, experience and knowledge to do their job properly and safely under all working conditions. An example is: «Acting as an Equipment Specialist with an Expert level on Air Conditioning in the Infrastructure domain».

The competence consists of a set of competencies that can be defined as a chunk of knowledge, skill, or professional value. A competency can be further decomposed into set of fined-grained activities. An competency example could be: «Supervise the Radio Transmitter and Receiver Station».

Safety-Related Task

A Safety-Related Task performed on an equipment is a fine-grained activity that can have an impact on the provision of safe CNS/ATM or AIM. Safety-Related Tasks are classified into two categories: Technical Service Provisioning and Technical System Monitoring and Control. Safety-Related equipment is an equipment on which, at least, one Safety-Related Task is performed.

Required Knowledge and Skills (RKS)

(Figure 2) represent the competencies an ATSEP must possess to be allowed to fulfill a certain Technical Role in a given Technical Domain on specific Equipment. This means that each ATSEP certification is associated with a given RKS, which in turn is associated with a given triplet {Technical Domain, Technical Role, Equipment}. When the ATSEP certification is limited to a single RKS, this RKS represents the ATSEP competence. However, usually an ATSEP plays several Technical Roles on different Technical Equipment in the same Technical Domain; therefore an ATSEP is certified on several RKS. Consider a technical employee in the Navigation unit (Technical Domain), acting as Equipment Engineer (Technical Role) for the Instrument Landing System model S4000 (Technical Equipment), his certification scope is {Navigation, Equipment Engineer, and ILS S4000}. As such, one of his competencies is to be able to «use the simulation tools preparing ILS equipment parameter data to be deployed».

Competencies are organised in seven pre-defined Technical Competency Areas, which are valid for all Technical Domains listed in Figure 3. Technical Competencies consist of Technical Skills; each of them associated with a Technical Skill Level (Elementary, Standard or Expert). These levels are used to differentiate between Technical Roles for specific Equipment. For instance, an On-Call ATSEP role performing daily routine maintenance tasks, requires less knowledge on a given equipment, as compared to the Swiss Application Manager responsible for analysing and correcting problems related to Flight Data Processing.

ATSEP Certification Path

For the sake of efficiency, the technical competence framework was designed as flexible and customisable as possible. The training program towards the certification depends on every ATSEP. This training program is set up right after the ATSEP is recruited, and depends on the ATSEP technical domain, assigned technical roles, academic grade and already acquired competencies and experience. Additionally, necessary training courses may be taken in parallel, in order to optimise the time necessary to get the certification.

Conclusion

This new business model as part of the Safety Management System allowed skyguide to meet ESARR5 requirements and is a step toward reducing the contribution of the technical elements to the safety risks. This was done by writing processes, which were integrated in the skyguide business process model as part of the Quality Management System.

This model has been deployed since 2006. The actual implementation challenge is to get a process working as seamlessly as possible across the various involved organisations..

Patricia Bomme & Guillaume Boppe
Methods and Tools, TM

	Procedure	Security	Technical Activity	Tools	Technology	Business	General
Elementary							
Standard	Coordination with FCS Equipment: Logbooks SYMA procedures	Drive on Airport Area Fire fighting First Aid Awareness Radio license for driving on airport runways	Site specific infrastructure	NAVAIDS measurement tool	NAVAIDS Basics	Knowledge of airports and distant sites facilities and procedure Knowledge of operational needs and expectations	
Expert	Awareness of Service Level Agreement for the NAVAIDS system Knowledge of maintenance concept Manufacturer Point of Contact		Equipment knowledge after manufacturer training on NAVAIDS System users interface	Simulation software		Knowledge of standards and recommandations	

Figure 3: RKS (Navigation, Equipment Engineer, ILS S4000)

safety policy

skyguide

PO 0200E V4.0 18.06.2008

As a responsible Air Navigation Service Provider skyguide, and all its subsidiaries, is committed to ensuring the highest, practicable level of safety. As such, we are committed to ensuring that the priority of safety is considered in all of our business decisions and resultant business activities, such that we can minimise our contribution to all safety risks.

The Chief Executive Officer (CEO) is ultimately responsible for the safety of our business and in achieving this it is the intention of the CEO to consider the High Reliability Theory principles where applicable. To fulfil these responsibilities the CEO delegates responsibility for establishing and maintaining an effective Safety Management System (SMS) to the Chief Safety Officer (CSO), and delegates to all staff responsibilities commensurate with their business responsibilities. In doing so, the CEO includes the appropriate decisional power to complete the tasks necessary to fulfil these responsibilities. All staff are made aware of these responsibilities and are provided with the necessary tools and training to fulfil them.

In establishing and maintaining an effective SMS, the CSO establishes and maintains a corporate safety department that provides the necessary processes, tools, expertise and training so that the identification of safety risks and their management is conducted in a formalised, reproducible and traceable manner.

The purpose of our SMS is to ensure that skyguide can improve its level of safety and its confidence in safety practices and that the SMS is considered as an integral part of our business management. As such, it is designed to be practical and efficient in the context of the specific needs of our business, whilst ensuring it complies with all external regulatory constraints including national and international obligations.

Our SMS takes both a proactive and reactive approach to safety management to ensure that we not only identify and manage existing safety risks but prevent the inadvertent introduction of further risks into our business as it evolves.

As we believe that safety consideration should be inherent in all business activities, a positive safety culture is promoted. Pivotal to this safety culture is a safety communication process that ensures safety information is not only available but actively distributed. Staff are encouraged to learn from this information, provide their feed-back and, if necessary, change their behaviour.

We promote a just culture, central to which is a non-punitive investigation process that prevents inhibiting reporting. We require that this philosophy is observed by employees at all levels. Within the limits of our legal obligations we observe strict confidentiality requirements to protect the privacy of individuals.

We believe that our safety management processes must not only be documented, but must be applied and adjusted. To ensure this our SMS is subject to regular internal and external assurance audits and safety surveys. The results of these activities are actively used to identify potential gaps within our SMS and provide important information for its improvement and evolution. To measure the effectiveness and progress of our SMS we regularly establish appropriate safety targets, goals and key activities which are contained within our strategic safety plan.

Daniel Weder, CEO *Jürg Schmid, CSO*