

safety bulletin

Inside this issue

2 Editorial

Juerg Schmid's last words as «S»

2 Safety Nets

MSAW or APM into GVA?

3-5 Kloten – Dübendorf transfer

Four lessons from the safety assessment

6-7 The human factors column

Safety: science of philosophy?

8 If you happen to witness that

Then report it!



Four lessons from a successful Safety Assessment

On the 24th of October 2008, our National Regulator formally approved the KLO-DUB migration phase by officially endorsing the program over-all Safety Case Document. What lies at the root of this success and how can it be used for the benefit of future Safety Assessments? This article summarises the main lessons learned from the two years during which the KLODUB Safety Assessment program was conducted.

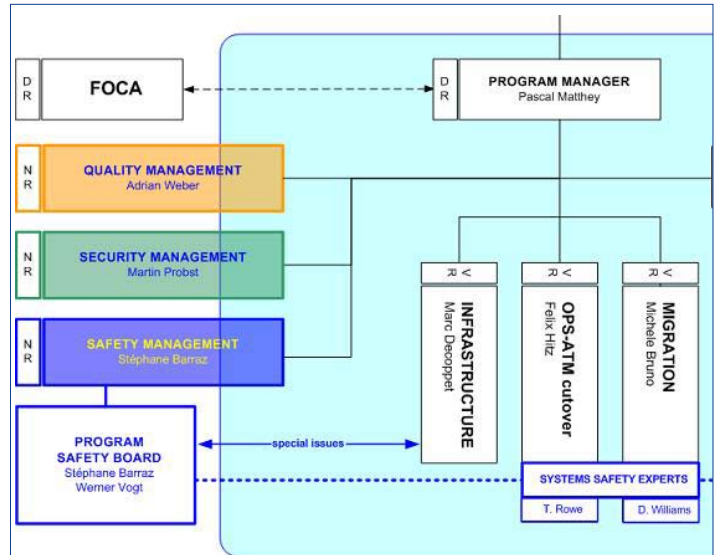
Start with the organisation...

From the beginning, it was the intention of the program management to thoroughly apply skyguide's Safety Assessment framework in order to demonstrate that the transfer of ATM-Services from Klotten to Dübendorf can be achieved in an acceptably Safe manner. For the purpose of doing so, a suitable program organisation was necessary.

In addition, a formal Program Safety Board (PSB) was established in order to follow-up and validate the work conducted at program level with support of dedicated Systems Safety Experts. During the conduct of the program, the Safety Board went through two different setups: plan-

ning and deployment. During the planning phase, the main task of the Program Safety Board was to ensure the delivery of a comprehensive and coherent Safety Program Plan. On that basis, the deployment phase was then fully dedicated to the initiation and follow-up of Safety Assessment activities.

The fact that Safety concerns were no more the property of experts created a high level of trust outside of the program organisation and in particular at the level of Regulatory Authorities (FOCA). This relationship factor played a prominent role in the success of the final acceptance process.



Safety management functions were positioned in such a manner that the program Safety manager was officially member of the program core-team but had only «Nagging Rights» (NR) in the decisional process. By doing so, the «Safety voice» could be heard and considered each time a decision was made by virtue of «Decision and Voting rights» (DR/VR). Thus, interest conflicts were avoided and Safety remained independent while being actively involved and informed.

Lesson #01

One of the most relevant key success factor was **Safety appropriation**. From the beginning, the program manager was deeply engaged in Safety activities and demonstrated a high level of commitment. The whole management team was then progressively integrated where appropriate and the skyguide decisional instances prepared to endorse the results of the Safety Assessment.

► Four lessons from a successful Safety Assessment

Agree about the strategy...

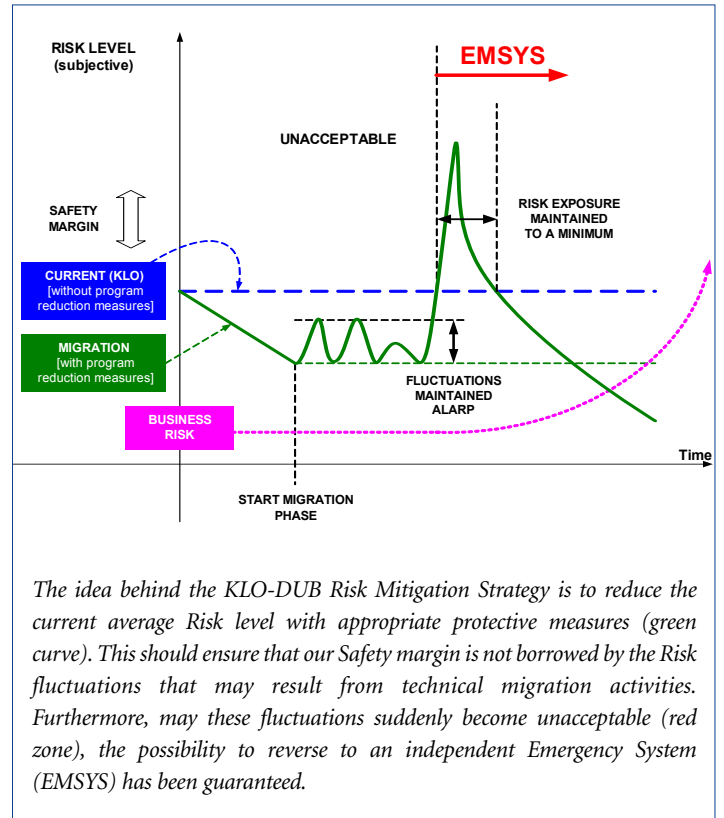
The aim of a Safety Assessment is not only to identify Risks but also to manage them in accordance with a well-defined and agreed Risk Mitigation Strategy. Elaborating such a strategy strongly depends on the change under consideration and on the environment within which this change will take place. There is no standard way to proceed and no possibility to escape intense discussions on the subject. The experience made in KLO-DUB calls for an early initiation of such considerations – both at the level of program management and at the level of Regulatory bodies.

Discussions about a suitable Risk Mitigation Strategy inevitably open the debate on methodological limitations. Despite the fact that skyguide has developed a very good set of rules, tools and processes for assessing ATM-System changes (Safety Assessment Framework), it is unavoidable to encounter application difficulties in complex programs like KLO-DUB. May such a situation develop, the important point is to find an early agreement with internal and external oversight instances in charge of verifying regulatory compliance. Indeed,

knowing where the limits of our models are and dealing appropriately with those limits is essential for a successful Safety Assessment.

Another important point is the integration of Quality and Safety activities. Despite the fact that those two domains are of very different nature, it is nevertheless important to support the development of Safety arguments with quality concerns. In the case of KLO-DUB, a remarkable Quality framework was established for the purpose of validating and testing the equipments affected by the migration. This set of rules and procedures – rigorously followed and supervised by the program Quality Manager – undeniably strengthened the Safety Case and contributed to its seriousness.

It is important to note that in the particular case of KLO-DUB, the National Supervisory Authority (FOCA) not only accepted a Safety Program Plan prior to commencing the Safety Assessment but also a whole set of Quality regulatory documents on the basis of which the whole program was based.



Lesson #02

Serious and thorough discussions about the foreseen **Risk Mitigation Strategy** should be initiated as soon as possible. Furthermore, such discussions shall provide an opportunity to discuss **methodological limitations** and to agree about the way **Quality measures** will support the final Safety Argumentation.

► Four lessons from a successful Safety Assessment

Care about documentation...

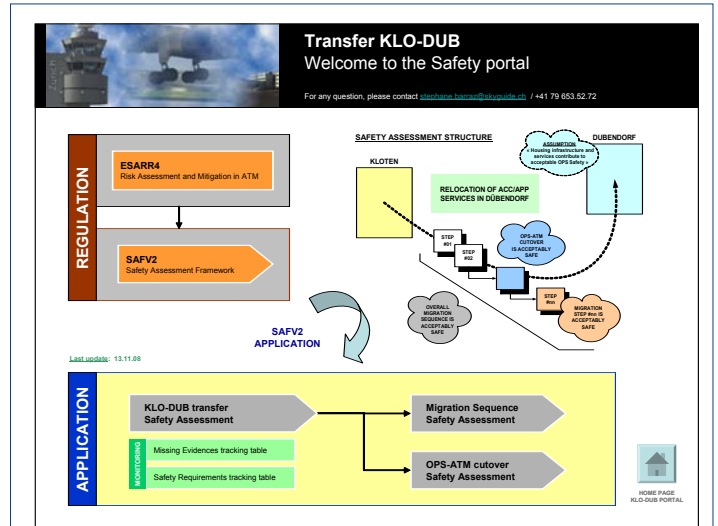
A Safety Assessment like KLO-DUB produces a huge amount of documentation. Without having the exact count available, it is not exaggerated to talk about **several thousands of pages**. Thus, documentation organisation and accessibility becomes rapidly a problem and should be discussed as soon as possible. With this respect, two important points have to be differentiated. First, the documentation should be organised in such a manner that it remains easy to access when needed. With this respect, a so-called «Safety portal» was developed and made accessible from the KLO-DUB documentation access point.

The other problem is that decision makers (internal and external) in charge of endorsing the result of several years of work shall **not be overflowed by complex and detailed documents**. With this respect, the KLO-DUB solution was to agree at the early stage of the Safety Assessment that the sole paper that will be officially endorsed will be an «overall Safety Case Document».

Importantly, this document is not only a summary of the numerous Safety activities conducted within the program but provides also what we called «the glue between the parts». It has been written in such a manner that a good balance was found between completeness and understandability – a real challenge!

The last tip with respect to documentation (and probably the most important one) is: **plan and start early**. Writing good Safety documents is time consuming. This should be done in an iterative manner and involve the whole program/project organisation. Appropriation of results and understanding of complex Safety problems takes also time. Finally, a successful endorsement process at the level of internal and external managerial instances requires not only meetings but also bilateral briefings.

In sum: organise, plan and start writing as soon as possible!



The principle of the KLO-DUB Safety Portal is very simple. A powerpoint show provides a graphical access to several topics. By «clicking» on the symbols, subsequent pages are opened and provide hyperlinks to specific documents. This way to «navigate» through the Safety Assessment process was proven very convenient and efficient. Furthermore, updating the portal when new documents are released is very easy to do.

Lesson #03

The documentation produced by a Safety Assessment should be organised as soon as possible so that its **accessibility** becomes easy and efficient. Furthermore, for large programs, it is recommended to agree about a **top-level document** as being the sole official paper subject to final endorsement.

► Four lessons from a successful Safety Assessment

Pursue after Safety Case endorsement...

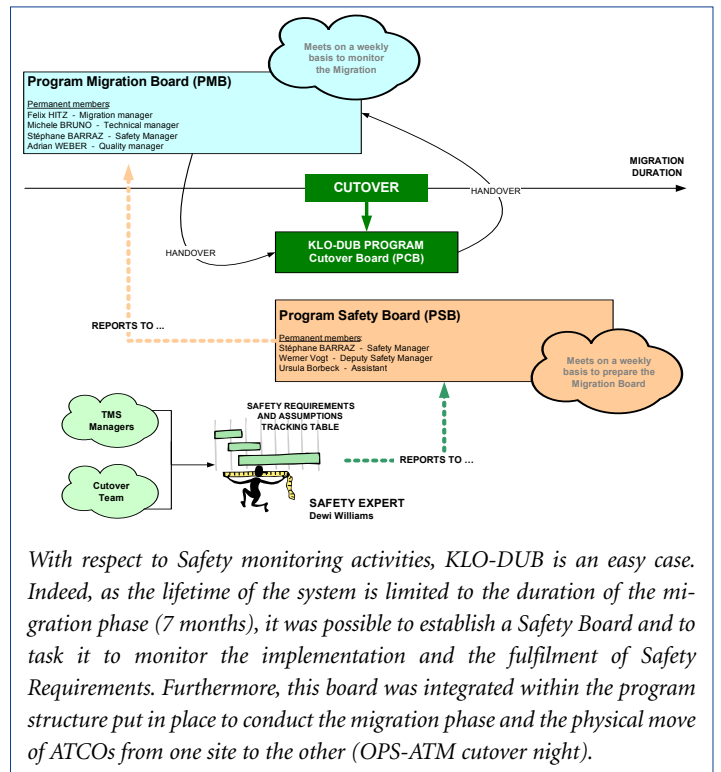
Unfortunately, once a Safety Case Document is endorsed, many people think that the Safety work is done. This is definitely not the case. As mentioned earlier, a Risk Mitigation Strategy is elaborated and agreed in order to maintain Risks within acceptable limits. The result is usually a set of Safety Requirements that have to be translated into an action plan. Some of these Requirements will have to be fulfilled before implementation of the assessed change and others later on. Furthermore, some of them may remain valid for the entire lifetime of the system under consideration. Thus, it is of utmost importance to **define and agree about Safety monitoring activities** at the early possible stage of the Safety Assessment process.

The particularity of KLO-DUB with respect to lifecycle duration is unfortunately not replicable to the many changes assessed within our company. Obviously, a monitoring structure equivalent to the one described above is not possible with a long

duration perspective and cannot be repeated for the numerous changes skyguide implements yearly. A rigorous and thorough answer to this problem is not available for the time being but this difficulty is well-known by our Safety department and solutions are currently being developed in a consistent manner with European requirements and guidelines.

At the time of writing this article, the KLO-DUB migration phase is about to be initiated. The board meetings structure has been put in place and is currently being tuned in order to attain optimal performance. The biggest challenge will be to maintain a strong «Safety voice» alive and to escape the influence of business and success pressure. This could be done for instance by integrating some «resilience» within the organisation – another interesting Safety subject that will certainly be addressed in a future Safety Bulletin!

STÉPHANE BARRAZ
KLO-DUB program Safety Manager



With respect to Safety monitoring activities, KLO-DUB is an easy case. Indeed, as the lifetime of the system is limited to the duration of the migration phase (7 months), it was possible to establish a Safety Board and to task it to monitor the implementation and the fulfilment of Safety Requirements. Furthermore, this board was integrated within the program structure put in place to conduct the migration phase and the physical move of ATCOs from one site to the other (OPS-ATM cutover night).

Lesson #04

Define and plan – whenever possible – Safety monitoring activities for the phase subsequent to the implementation of the assessed change. In other words: keep the Safety Assessment **alive!**

Safety: science or philosophy?

Can we have a serious discussion about Safety without caring about philosophy? Or is Safety an exact science that can be approached at best by traditional scientific methods? This article presents two perspectives that may lead to the development of fundamentally different Safety cultures.

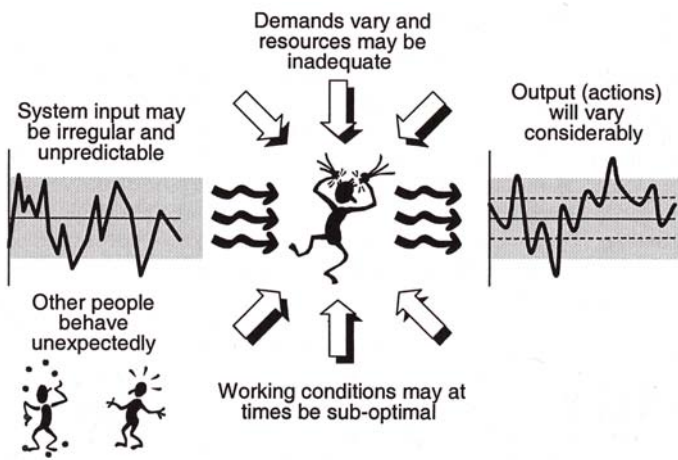
The way most people talk about Safety is by making usage of the language of methods, tools and regulatory compliance. Indeed, most of you probably heard about Safety Assessment Frameworks, Fault Tree Analyses, ESARRs or even Safety Indicators. So why do we need to care about philosophy if Safety can be

apparently so easily addressed by exact sciences? Simply because the tendency we have to believe that Safety can be measured and approached by traditional scientific methods rests indirectly on a strong philosophical position named «realism». Such a worldview – which governs scientific research since many

decades – is based on the belief that we are surrounded by facts, lying anywhere out there, and ready to be approached, measured and understood by adequate methods. And that when our observations differ from our expectations, improving metho-

► Safety: science or philosophy?

The adaptation of human performance ²



«In practice, it is often found that (1) the inputs to the work process are irregular and unpredictable; (2) the demands and resources are inadequate; and (3) the working conditions fall outside normal limits. People are therefore constantly asked to do something without being given means and time to do it. This results in trade-offs that generate outputs which from time to time fail to comply with expectations or norms.»

dology is the only way to re-establish confidence in what we see.

Let's take a simple example well known in our business: the occurrence of airproxes. At first sight, it seems undeniable that aircrafts coming too close together are «facts» that can be observed, counted and categorized in order to feed statistics representative of our current Safety level. Furthermore, it seems evident that reducing the number of such occurrences can be primarily done by identifying their causes – usually human errors – and by implementing reprimanding and training measures.

So far, everything seems to be fine: humans are fallible, they commit errors which are at the root of our Safety problems. Methods to observe, count and categorize these errors can be developed and countermeasures can be implemented to reduce them – mainly through selection, procedures, automation, training or discipline.

Back to philosophy...

Another view of our world is the one defended by «relativists» who assert that we are not surrounded by facts, waiting to be measured and

understood with adequate scientific methods. In contrary, what we see (or what we believe we see) is socially constructed.

With this perspective, airproxes only exist because a community of people defined and agreed about the rules of separation that shall be maintained to ensure acceptable Safety. Outside of this commitment, airproxes have no factual existence. Furthermore, what causes such incidents is not an objective fact but rather a social judgment: it is only when the unwanted consequence occurs that we begin to look for «human errors» and use them as suitable causes. In other words, it is only when the effect has been recognized that the cause becomes important – before that, it has no factual existence.

This bias has been concretely reported in a study whose purpose was to test an error-count method in the domain of Air Traffic Control'. Interestingly, actions that at first sight appeared as deviant could be easily normalized by adopting a different perspective of human work. Put differently, what was initially observed and categorized as an error suddenly became a deliberate strategy deployed to remain in control of a complex and dynamic situation. This study not only confirmed the negotiable nature of observations but also emphasized that human actions cannot be described in binary terms (i.e. as being either correct or incorrect): people always try to do what they think is right at the time they elect to do it – a principle human

factors specialists name «local rationality».

Unfortunately, even the best-intended actions sometimes result in outcomes that differ from expectations. When we observe this happening, we usually name it «human error» and blame the involved people. But does this reaction to failure explain anything? Does it allow to understand what really happened? Does it provide the means to implement corrective measures that will impeach future re-occurrence? Certainly not. To make real progress on Safety, we should rather attempt to understand why and how people constantly try to achieve an acceptable balance between thoroughness (i.e. carrying out actions as well as possible) and efficiency (i.e. doing it without spending too much effort). And this seems only possible by renouncing to consider errors as observable facts – thus by adopting a «relativist» philosophical position.

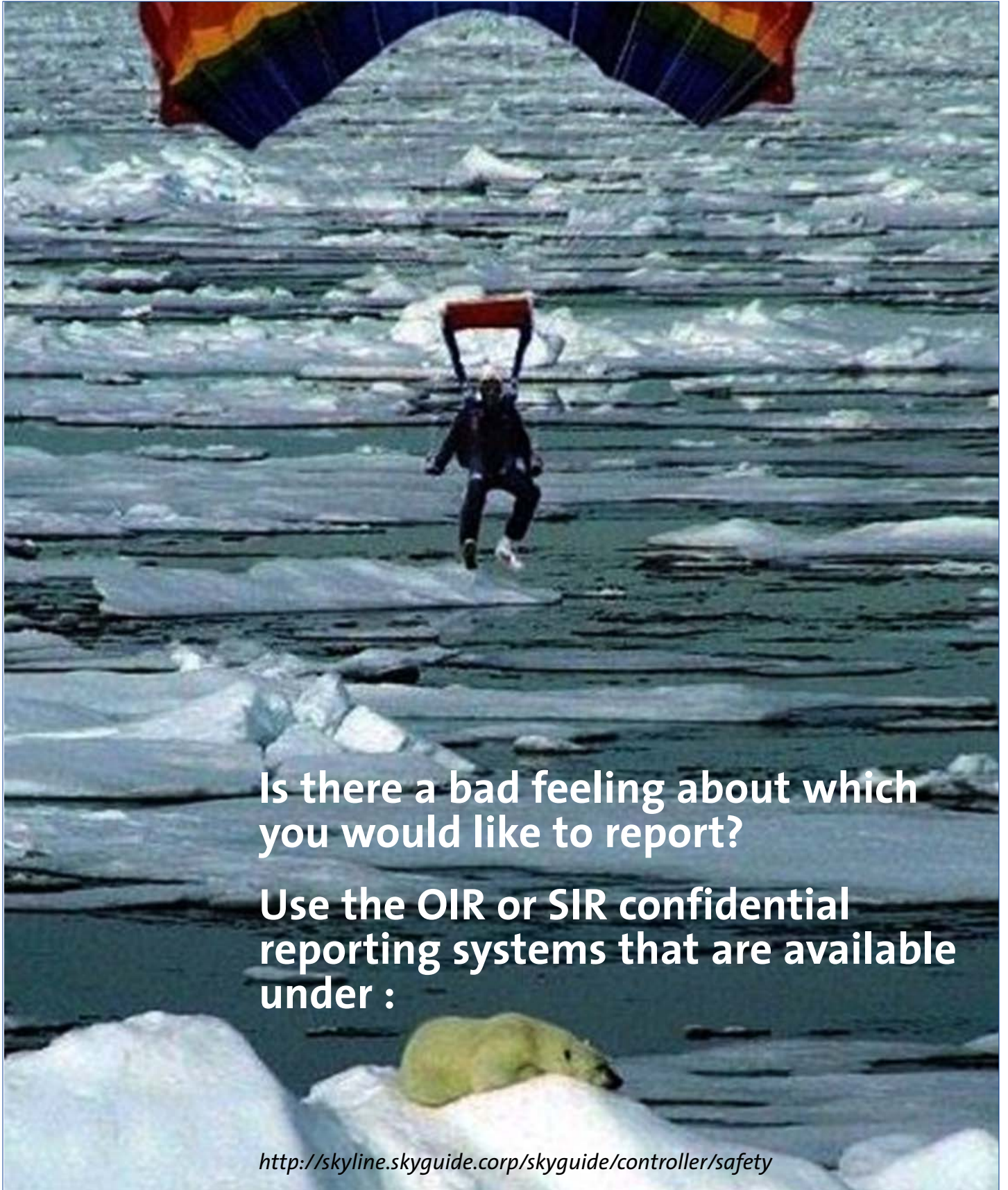
So who is right and who is wrong?

Certainly nobody. But adopting one or the other perspective may lead us to address the difficult subject of human error in diametrically opposed ways. Depending on our choices, we may either pursue a «blaming» culture or we may start developing a Safety culture based on the willingness to better understand the role humans play in the occurrence of accidents. Choice is ours...

STÉPHANE BARRAZ
Safety Program Manager

1-Hollnagel, E., Amalberti, R. (2001). *The emperor's new clothes or whatever happened to «human error»*. 4th International Workshop on Human Error, Safety and System Development – Linköping, Sweden.

2-Hollnagel, E. (2004). *Safety Barriers and accident prevention: how to improve Safety by understanding the nature of accidents rather than finding their causes*. Ashgate publishing, London.



Is there a bad feeling about which you would like to report?

Use the OIR or SIR confidential reporting systems that are available under :

<http://skyline.skyguide.corp/skyguide/controller/safety>