

# A Complementary Approach to Support Risk Management and Decision-Making

Jean Paries & Corinne Bieder

jparies@dedale.net

Dédale S.A. FRANCE

## ABSTRACT

This paper describes a new approach intended to facilitate the extraction of “safety lessons” from reported events and to support safety-related Decision Making. The corner stone of this approach is to make the system Safety Model explicit through identifying macro events -called Generic Initiators (GIs) - that would naturally develop into an accident in the absence of successful recovery action. For each GI, a Safety Architecture (SA) is developed, i.e. the logical combination of all the protections, or Safety Principles (SPs), supposed to *prevent* this GI, or *recover* from it before it develops into an accident, or to *mitigate* the consequences of an accident. The behavior (i.e. success or failure) of each SP during reported events is then recorded. The build-up in experience allows to draw a health-map for each SP. This points out the critical weaknesses of the actual safety system, helps suggesting modifications, and facilitates an evaluation of the efficiency of optional solutions.

## KEYWORDS

Safety analysis, incidents analysis, Safety Model, Safety Principles, operational feedback.

## INTRODUCTION

Analyzing incidents to improve safety is a common strategy in virtually all activities, including Aviation Maintenance. Incidents are seen as accident embryos. A better understanding of what caused incidents is expected to generate ideas to amend the design or the operation of the system, in order to make it safer. Furthermore, safety management strives to be as proactive as possible, and tries to learn lessons from minor failures, errors or deviations, situated as far as possible from the accident itself (Koornneef (2000)). Considering incidents to prevent accidents, then errors to prevent incidents, seems a wise and easy thing to do. Unfortunately, it might well be wise, but it is certainly not easy to achieve.

## THE CHALLENGES OF LEARNING FROM INCIDENTS

Safety management decisions need answers to questions like: “what is the potential damage associated with such an incident? What are the odds for such damage? What are the protections currently existing? How efficient are they? How to improve them? At what cost? What are the priorities? ” But in many domains, including Aviation Maintenance, the answers to such questions are not easily provided to decision makers by the current incident analysis systems. The reason is manifold:

- accessing the incidental data is difficult and the conditions for statistical validity are difficult to meet. What can be kept invisible is not reported, and there is a lack of baseline data.
- incident analyses are based on a process of “causal” attribution. However, the notion of cause is multifaceted. An incident is something that is not supposed to happen. Therefore what needs to be explained is *why something that was not expected to happen, actually happened*. Hence identifying the causes of an incident necessarily refers to a model of what is supposed to make that system safe.
- even when causes are identified from a safety model perspective, it is mainly done implicitly. There is generally no *explicit* description of the safety defenses. The attribution of “causes” then reflects individual analyst thinking about safety (Hollnagel (1998)). Additionally, the causation model is taken as a truth, whereas it should be a falsifiable assumption.
- a significant part of the ‘causality’ of an event is context related. And this context will not repeat itself. A lesson can only be learned from an event if some generalization is achieved. As Rasmussen (2000) puts it, “completeness removes regularity” The challenge to extract a safety lesson is then to find cross-contextual elements that condense the system safety behavior shared across all the occurrences.

In order to address these difficulties, a complementary approach has been developed,

within the EC funded ADAMS Project, leading to the design of a software-based Aviation Maintenance Safety Management Assistant (AMSMA).

### A NEW AND COMPLEMENTARY APPROACH

The core idea of the new approach is to confront incidents directly to the reasons why they were not meant to happen, in other words to the corresponding Safety Principles (SPs), in order to assess and map the strengths and weaknesses of these SPs. The Safety Principles (SPs) are all the assumptions made about the safety of the system. However, there is a need for a screening function to identify the relevant subset of SPs associated with a specific incident. For that purpose, the notion of “Generic Initiator“ (GI) is introduced. A GI is defined as *any event (or non event) from which an accident would develop, should no specific recovery action be positively taken*. A GI is an *initiator*, which means that at one point, the system switches from a safe, under control, state to an unstable, uncontrolled, intrinsically unsafe state. It is *generic*, which means that it is independent from particular circumstances.

For each of the GIs, the Safety Architecture (the logical combination of SPs that are assumed to protect the system) is then developed as represented in figure 2:



**Figure 2:** Safety Architecture (i.e. combinations of Safety Principles) associated with a Generic Initiator

- SPs intended for preventing the Generic Initiator from happening are called *Prevention* SPs.

- SPs intended for preventing the Generic Initiator from developing into an accident are called *Recovery* SPs.
- SPs intended for preventing the Accident from developing into its worse consequences are called *Accident Consequences Mitigation* SPs

The methodology to identify GIs and to develop Safety Architectures will not be addressed in depth in this paper. Generic Initiators can either be identified opportunistically from reported incidents, or be derived from a systematic top-down approach, from the loss of the Safety Functions of the maintenance system. The identification of SPs is based on a functional approach, and starts with the “high level” SPs. Then each SP is decomposed into a logical combination of lower level SPs, and so on. The method goes from the most abstract (strategy) to the most concrete (expected behaviour of the components, the operators, and their interactions).

### Analysing reported events

The first thing an analyst must do is to match the reported events to an available Generic Initiator. If no Generic Initiator can be found in the existing list, then a new Generic Initiator has to be defined, and the associated Safety Architecture has to be developed. Once the reported event has been related to a Generic Initiator, the Safety Principles potentially involved in the event are those included in the associated Safety Architecture.

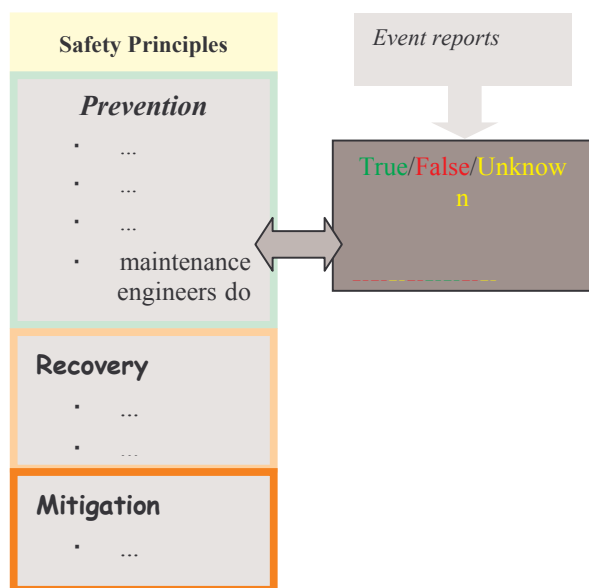
Assessing these Safety Principles then consists in pointing out and recording which of them *failed*, were actually *successful*, were triggered, but of which behaviour is not available in the report, and also, which of them were clearly *not triggered*. This behaviour qualification (*success, failure, unknown outcome, or not triggered*) of the SPs involved in one event is stored into the AMSMA data base through a colour coding of the link established between the event and the SPs.

### Assessing the health of safety protections

While the process of assessing SPs behaviour is repeated, event report after event report, the AMSMA system starts to accumulate the coloured links. The series of links associated to one SP will then form what could be called the “Health Map” of that Safety Principle, as illustrated by Fig.3.

The next step is to interpret the "health map" of each Safety Principle to assess its *robustness*, in other words, the level of trust that can be vested in it, on the grounds of the knowledge gained through

an interpretation of the available feedback from experience.



**Figure 3:** Safety Principle Health Map

This will be achieved through a four-level scale rating of the SPs reliability. A colour coding of the ratings will be implemented in the Safety Architectures displays : SPs will appear under their corresponding rating colour to better visualise the consequences of a rating.

For most SPs, and certainly for all those SPs related to Human behaviour, this will only be a qualitative assessment. These ratings are the outcome of an expert judgement, possibly a collective and consensus-based one. The health map is only expected to *support* that judgement process, through a *colour coded visualisation of the available experience*.

The safety lesson further depends on the role played by the SP, mainly on two main aspects: i) how *critical* the SP is: what happens to the safety of the system if that SP fails? What is the amount of risk involved? ii) how *common* it is: how far is the overall Aviation Maintenance safety contaminated if that SP fails?

### Supporting Safety related Decision Making

The objective of AMSMA is not to develop a complete decision-making rationale, but to provide decision-makers with safety information to help

them better take safety issues into account. AMSMA can assist safety-related decision-making from several perspectives, that will most probably be invented by the analysts themselves during their operational use of the system. However, it can be anticipated that AMSMA will assist two kind of safety-related decisions:

- decisions concerning the perception of the system safety status: e.g. modification of the robustness rating of a SP; modification of a Safety Architecture;
- decisions related to the management of the system safety: e.g. monitoring of the safety implications of a change in a Safety Architecture; propagation of implications to other Safety Architectures; decisions related to the modification of the system to improve its safety level (safety recommendations)

### CONCLUSION

The approach suggested in AMSMA differs from traditional incident analysis approaches in that it tends to describe why the system is supposed to be safe, instead of trying to understand why it fails. It seeks to learn safety lessons through a permanent comparison of expected and actual behaviour of the safety system. Through the notion of Generic Initiator, the approach goes beyond the specific circumstances of an incident, and memorise the reasons with they could breach the system's protections. Thus, the Decision-Making process proposed in the AMSMA approach benefits from the complete aggregated experience, rather than from a collection of single event experiences.

### REFERENCES

- Hollnagel, E. (1998) *Cognitive Reliability and Error Analysis method*, Elsevier , Oxford, England
- Koornneef, F.(2000) *Organised Learning from Small-scale Incidents*; Delft University Press, Delft, The Netherlands.
- Rasmussen, J. , Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society* , Karlstad, Sweden: Swedish Rescue Services Agency