

# 18.0 THE MEASUREMENT OF SAFETY

*James Reason*

*Department of Psychology, University of Manchester*

## INTRODUCTION

What is a safe organization? The usual answer is one that has relatively few bad events or negative outcomes—accident, incidents, quality lapses and the like. But there are many problems with this type of assessment.

- In aviation, the most obvious difficulty is the scarcity of bad events. Major accidents have fluctuated around the same low level (around  $1.5 \times 10^6$  departures) for the past twenty years or so. There are, of course, a much larger number of less serious events but—in maintenance especially—these are massively under-reported.
- Bad events have a large chance component. Only if system managers had complete control over all possible accident-producing factors could the number of bad events sustained by the organization provide a valid index of its absolute safety. But this is not the case. Natural hazards can be anticipated and defended against, unsafe acts can be moderated to some degree, but neither can be eliminated altogether. There is no way—short of ceasing operations altogether—of preventing the chance conjunction of unsafe acts, local triggers and latent conditions so that they penetrate—albeit very rarely—the system's many barriers, controls and safeguards (1,2). In short, there is no such thing as absolute safety. There is no 'target zero'.
- The large random component in accident causation means that 'safe' organizations can still have bad accidents and 'unsafe' ones can still escape accidents for long periods. Chance works both ways. It can afflict the deserving and protect the unworthy.
- Where there are large numbers of bad events, as in construction or road transport, for example, outcome measures based on accident rates do provide a reasonable measure of an organization's relative safety. But when the numbers are small and asymptotic, as in aviation, such measures are both unreliable and, on occasions, dangerously misleading. Organizations having the same comparably low levels of bad events could actually differ very widely in their degree of intrinsic safety.

If we cannot use *negative outcome* measures reliably, what then is the alternative? The argument to be presented here is that the most meaningful way of assessing safety is through *process* measures that reflect the system's current 'safety health' through the regular sampling of its vital signs. In order to provide a principled basis for this claim, we need to consider more closely what is meant by the term 'safety' other than some unattainable freedom from hazard or danger. As indicated earlier, neither gravity nor terrain will go away; nor will human fallibility or systemic weaknesses.

## THE POSITIVE FACE OF SAFETY

Safety has two faces. The negative face is very obvious and is revealed by bad events, near misses and the like. This face lends itself very easily to being quantified and so holds great appeal to managers. But there is also another face that is both benign and more hidden. This aspect of safety can be defined as the system's *intrinsic resistance* to its operational hazards. In other words, some organizations will be more robust, more resistant, or more resilient than others in coping with the dangers associated with their core business. This will be true for aircraft maintenance organizations as for any other part of the wider aviation system.

Let us give some substance to this rather vague notion of 'intrinsic resistance.' Consider a ball bearing resting upon blocks of various shapes: convex, rectangular and concave. Imagine that the ball bearing and the block are being continuously perturbed by forces equivalent to operational hazards. A bad outcome occurs when the ball bearing is displaced from the block. Clearly, it will take a good deal more agitation to disturb the ball on the concave block than either of the other two.

Now consider an even more concrete example. Engineers are accustomed to carrying out tests to destruction. For a particular aircraft type, a 'test to destruction' is roughly analogous to the number of factors required to bring about a fatal accident. A recent study (3) examined 90 fatal accident investigation reports carried out by the UK Air Accident Investigation Branch between the 1970s and the 1990s with a view to establishing how many of 16 possible contributory factors were implicated in accidents sustained by three different aircraft types: large jets, light aircraft and helicopters. The contributory factors included such things as airframe problems, system problems, fuel problems, wind, precipitation, pilot handling problems and the like. The results were very clear. On average, it took 1.95 problems to crash a helicopter, 3.38 for a light aircraft and 4.46 problems for a large commercial jet. Not surprisingly, helicopters—that merely beat the wind—are considerably more vulnerable (or less resistant) than large jets.

## THE SAFETY SPACE

Another way of representing the ideas of resistance and vulnerability is as the extremes of a notional cigar-shaped space—termed the safety space. Each organization occupies—at any one time—a position within this space. The space is cigar-shaped because most organizations will cluster in the midpoint regions with the numbers diminishing as one moves to either end

Organizations are free to move up and down the space. In this, they are subject to two kinds of forces: those existing externally within the space itself and those emanating from the organization. The external forces act inwards from either extreme of the space. If the organization drifts too close to the vulnerable end, it is likely to suffer an accident. This, in turn, will bring about both internal and external pressures to become more resistant. Improvements in the safety management system will drive the organization towards the resistant end. But these are not often sustained, so that the organization drifts once again back towards the vulnerable end. Left largely to their own devices, organizations will tend to drift to and fro within the space.

Two things are required to both drive the organization towards the resistant end and then to keep it there. First, it requires effective navigational aids—that is, something other than the frequency of bad events. Secondly, it needs an ‘engine’ to overcome the external tides and currents and to maintain a fixed heading.

## REACTIVE AND PROACTIVE MEASURES

Where major accidents are few and far between, the reactive measures will be derived mainly from near miss and incident reporting systems, or ‘free lessons.’ Such safety information systems have been considered at length elsewhere (2, 4) and will not be discussed in detail here. We can, however, summarise their likely benefits.

1. If the right lessons are learned from these retrospective data, they can act like vaccines to mobilise the organization’s defences against some more serious occurrence in the future. And, like vaccines, they can do this without lasting harm to the system.
2. These data can also inform us as to which safeguards and barriers remained effective, thus thwarting a more damaging event.
3. Near misses and incidents provide important qualitative insights into how small defensive failures could combine to create major accidents.
4. Such data can also yield the larger numbers required for more far-reaching quantitative analyses. Analyses of several comparable incidents (e.g., missing O-rings, missing fastenings, etc.) can reveal patterns of cause and effect that are rarely evident in single-case investigations.
5. Most importantly, an understanding of these data serves to slow down the inevitable process of forgetting to be afraid of the operational dangers.

Proactive measures identify in advance those factors likely to contribute to some future accident. Used appropriately, they help to make visible to those who operate and manage the system the latent conditions and ‘resident pathogens’ (1) that are an inevitable part of any hazardous technology. Their great advantage is that they do not have to wait upon an accident or an incident; they can be applied now and at any time. Proactive measures involve making regular checks upon the organization’s defences and upon its various essential processes—planning, forecasting scheduling, budgeting, maintaining, training, creating procedures, and the like. There is no single comprehensive measure of the organization’s overall ‘safety health.’ Just as in medicine, establishing organizational fitness—or intrinsic resistance—means sampling a subset of a larger collection of leading indicators, each reflecting the various systemic vital signs. A more detailed consideration of these diagnostic indicators has been given elsewhere (2, 5).

Effective safety management requires the use of both reactive and proactive measures. In combination, they provide essential information about the state of the defences and about the workplace and systemic factors known to contribute to adverse events. The main elements of their integrated usage are summarised in [Table 18-1](#).

<b>Table 18.1. Summarising the interactions between reactive and proactive measures</b>		
	Type of navigational aid	
	Reactive Measures	Proactive measures
Local and organisational conditions	<i>Analysis of many incidents can reveal recurrent patterns of cause and effect.</i>	<i>Identify those conditions most needing correction, leading to steady gains in resistance or "fitness."</i>
Defences barriers & safeguards	<i>Each event shows a partial or complete trajectory through the defences.</i>	<i>Regular checks reveal where holes exist now and where they are most likely to appear next.</i>

## **SOME PROACTIVE MEASURES APPLICABLE TO AVIATION MAINTENANCE**

A number of proactive safety measures have been created specifically for aviation maintenance. Two are listed below. Each has been discussed at length elsewhere.

1. Managing Engineering Safety Health or MESH (2)
2. Proactive Error Reduction System or PERS (6)

## **CONCLUSIONS**

1. Negative outcome data are both too sparse and too unreliable to provide an adequate measure of a maintenance system's safety health.
2. Safety is a function of an organization's intrinsic resistance to its operational hazards.
3. This can only be achieved by the combined use of both reactive and proactive measures. MEDA (Maintenance Error Decision Aid) provides a good example of a reactive measuring tool capable of identifying accident-producing factors before they combine to cause a bad event (7). [MESH](#) and [PERS](#) operate proactively to identify those systemic 'vital signs' that need fixing in order to enhance a system's resistance to hazards.

## REFERENCES

1. Reason, J. (1990). *Human Error*. New York: Cambridge University Press.
2. Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.
3. Stephens, D. (1996). The 'rule of three' in aircraft accident causation. Manchester: University of Manchester, Department of Psychology Report.
4. Van der Schaaf, T.W., Lucas, D.A., & Hale, A.R. (1991). *Near Miss Reporting as a Safety Tool*. Oxford: Butterworth-Heinemann.
5. Hudson, P., Reason, J., Wagenaar, W., Bentley, P., Primrose, M., & Visser, J. (1994). Tripod-Delta: Proactive approach to enhanced safety. *Journal of Petroleum Technology*, 40: 58-62.
6. Drury, C.G., Wenner, C.L., & Murthy, M. (1997). A proactive error reduction system. In: *Proceedings of the 11<sup>th</sup> Meeting on Human factors Issues in Aviation Maintenance and Inspection*, March 12-13, San Diego. Washington DC: Federal Aviation Administration.
7. Boeing (1994). *Maintenance Error Decision Aid*. Seattle, WA: Boeing Commercial Airplane Group.