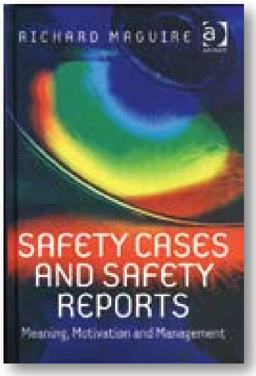
# A Case of Safety

**Creating a safety case early can avoid a lot of grief later — but it needs to be argued clearly.**



**BOOK**

## Safety Cases and Safety Reports: Meaning, Motivation and Management

Maguire, Richard. Aldershot, England, and Burlington, Vermont, U.S.: Ashgate, 2006. 190 pp. Figures, tables, references, index.

The author says in effect that you have two chances to prove your system, project or process is reasonably safe. The first is to develop what is called a safety case before it goes into operation. The second is in a law court after being sued. Creating a safety case is preferable, but it must be built with as much evidence and logic as a legal case.

"The key elements of this text are based around identifying the meaning and measurement of safety and risk; the motivation behind the need to construct a safety case; the management of the task of generating and presenting one; and how to maintain it once it has been produced," Maguire says.

In many respects, a safety case is similar to a legal case. "[A safety case] report summarizes all the key component parts of the safety case, it makes the safety argument explicit and describes the supporting evidence," Maguire says. In addition to showing that the system meets all laws, regulations and standards, "it should confirm that key staff are in place with defined responsibilities; that any further safety requirements and targets that have been set and met are appropriate; that hazard analysis has been carried out correctly; that the level of residual risk is tolerable; and that the safety performance of the entity, process or system has been independently assessed."

A safety case can be only as sound as the language that embodies it, a requirement that Maguire says holds traps for the unwary. At the most basic level, while it is generally accepted that absolute safety is impossible and there must be some satisfactory reasonable degree of safety, what one person means by that may not match what another means. Although he does not use extended twin-engine operations as an example, he might have: The chance of both engines of an approved twin-engine jet failing in oceanic flight is so low that worrying about it hardly seems worth the bother. But it is not zero, and those whose job it is to worry about such things have not always agreed about how many hours flight time should be permitted from the nearest airport suitable for diversion.

Another pitfall in talking about safety in the English language is called *ellipsis*, which Maguire says "allows you to leave out words you think are obvious, and it is perfectly acceptable grammar." He offers as an example a paragraph from an actual safety requirement document, from the section about tracking software failures:

"Visible Bug Tracking. Here we provide evidence of bug tracking for the software. 'XXXXX' is the database that is used to track all issues regarding this system. It has full visibility and is extremely detailed."

This sounds straightforward, but Maguire says it conceals ambiguities. "What is actually mean by 'all issues'?" he asks. "Should this really be 'all *software* issues,' 'all *bug* issues' or 'all *safety* issues'? What does 'full visibility' mean? Full visibility of what? 'Full visibility *of the software*'?

'Full visibility *of bug information*'? Does the 'it' really mean that 'it' *presents* full visibility to the viewer? Or is there something more here, perhaps some extra functionality that we need to know more about? From the text as it is, we just don't know, we have to make assumptions."

The author discusses many standard concepts in safety cases: for example, ALARP —risk "as low as reasonably possible," SFAIRP —"so far as is reasonably practicable" and GALE — "globally at least equivalent," which means that if one particular hazard increases, risks from others must decrease at least as much so that the risk within the whole system is acceptable. Such concepts are valid and necessary, but they can be more complicated than they appear, he says.

Critiquing one "perfectly adequate" risk assessment description for a safety case, he notes that its focus is too narrow. "The risk assessment team explicitly says that they used their 'professional judgment' in the analysis — excellent, very often this is actually missed out," he says. "The process also states that they considered the 'cost of implementing' the potential control measures that they had identified. Again very good.

"Potential concerns are that while human factors get a special mention (good), mechanical, software and managerial factors do not. This implies some special attention to human factors. Also, it is not clarified what the 'cost' actually contains — it should contain factors relating to time, resource and trouble, not just a financial consideration."

The overall conclusion to be drawn from *Safety Cases and Safety Reports* seems to be that the more risk factors that are considered and explicitly discussed before they actually arise, the better.

## REPORTS

A Human Factors Review of the Operational Error Literature

### Human Factors Review of the Operational Error Literature

Schroeder, David; Bailey, Larry; Pounds, Julia; Manning, Carol. U.S. Federal Aviation Administration (FAA) Office of Aerospace Medicine. DOT/FAA/AM-06/21. Final report. August 2006. 66 pp. Figures, references, appendixes. Available via the Internet at <www.faa.gov/library/reports> or from the National Technical Information Service.*

The report reviews documents about research and initiatives to reduce operational errors (OEs) in air traffic control (ATC) — 154 documents published from 1960 to 2005 and 222 OE reduction initiatives from 1986 to 2005.

The literature analysis identified some consistent findings:

- "The amount of [air] traffic measured on a national basis is the single most important determinant of the frequency of OEs."
- "A relatively high percentage of OEs occurred during the first 20 minutes on [the air traffic controller's] position."
- "Pilot-controller miscommunications were historically identified as a primary causal factor associated with OEs, and hearback/readback errors were studied most often. Although analysis of recorded communications revealed that few hearback/readback errors resulted in an OE, a sizeable proportion of OEs were attributed to hearback/readback errors."

The review of initiatives related to organizational and management issues found that some "described concerns about resources available to supervisors to accomplish their jobs and recommended additional supervisory training," while others "focused on mental processes, especially those efforts addressing skills training."

Most initiatives that involved the conditions under which controllers worked were about training, teamwork and communications.

The report says, "Both the research reports and OE reduction initiatives emphasized the same six contextual conditions (although not necessarily in the same order): training and experience; teamwork; pilot-ATC communications; human-machine interaction and equipment; airspace/surface; and traffic."

Appendixes reference research documents by type of study and by categories of contributing factors to OEs.

## Developing a Methodology for Assessing Safety Programs Targeting Human Error in Aviation

Shappell, Scott; Wiegmann, Douglas. U.S. Federal Aviation Administration (FAA) Office of Aerospace Medicine. DOT/FAA/AM-06/24. Final report. November 2006. 13 pp. Figures, references. Available via the Internet at <www.faa.gov/library/reports> or from the National Technical Information Service.*

According to studies based on the Human Factors Analysis and Classification System (HFACS), the percentage of accidents associated with flight crew error — classified in the system as skill-based errors, decision errors, perceptual errors and violations — has remained essentially stable. In other words, it appears that no intervention program has been clearly effective.

But, the report says, unlike the validated HFACS framework for investigation and analysis of human error, there is no similar framework for evaluating the benefits of current and proposed human error intervention strategies. This report describes two studies conducted using recommendations from U.S. National Transportation Safety Board (NTSB) investigators and several joint FAA and industry working groups, intended to validate a proposed framework for developing and examining initiatives targeting human error.

The first study was based on 622 unique safety recommendations contained in NTSB aviation accident reports, which were analyzed and classified. Researchers found that these recommendations, also called intervention strategies, could be subdivided into four broad categories: administrative/organizational, human/crew, mechanical/engineering and task/procedure. The report said that "surprisingly few" — 11.5 percent of interventions — were in the human/crew category, given the importance of flight crew human error in today's understanding of accidents.

The four categories might be expanded with further study, the report said, but categories are important because "to ensure that safety professionals generate effective intervention strategies, rather than a single 'knee jerk' fix to a problem, knowledge of all viable interventions is required."

The second study was designed to develop a way of mapping the types of human error described in HFACS against the kinds of intervention strategies identified in the first study. This entailed the creation of a grid called HFIX — the Human Factors Intervention Matrix — with human error categories on the vertical scale and five types of intervention strategies on the horizontal scale. Researchers calculated the percentages of recommendations by joint safety analysis teams (JSAT) and joint safety implementation teams (JSIT), created by the U.S. Commercial Aviation Safety Team as part of the FAA's Safer Skies Initiative, according to intervention type. These were then correlated with the four types of HFACS errors. "Perhaps not unexpected, interventions aimed at decision errors were associated with nearly three out of every four JSAT/JSIT recommendations examined," the report said. This represented an apparent incongruity: "Roughly one-third of the accidents were associated with decision errors, yet 72.6 percent of the interventions have some component that will potentially affect pilot decision making."

The report said, "Also noteworthy, few interventions attempted to modify/change the task itself or the environment. A closer examination of the actual types of errors may suggest changes in routes people fly or the actual type of flights being flown."

### WEB SITES

## Aerospace Acronym and Abbreviation Guide, <www.aviationtoday.com/av/acronym/a.html>

A is for *autotuned navaid.* Z is for *Zulu* — coordinated universal time, formerly called Greenwich Mean Time. Between A and Z are abbreviations and acronyms for technologies, procedures, jargon and organizations in the aerospace world.

This is the go-to site when you want to know the meaning of BOP/COP — *bit-oriented protocol/character-oriented protocol*; MALE — *medium-altitude, long-endurance*; DREAMS — *disaster response and emergency medical*

*services*; SPEAR — *system performance evaluation and analysis reporting*; and many other useful terms.

*Avionics* magazine has compiled and published this reference guide. Now in its third edition, the list has grown to 2,966 entries. The list is indexed by letters of the alphabet for faster locating. X has the fewest entries, with 14.

The publisher says, "Though it is not an exhaustive list, we trust it will serve you well."

It certainly should. No one in the industry could get through a day's work if everyone had to fully write or speak the phrases for which acronyms and abbreviations have been adopted. IAAWT — In Abbreviations and Acronyms We Trust.

## Air Accident Digest, <www.airaccidentdigest.com>

This new aviation safety Web site describes itself as "the place for real-time cutting-edge news and analysis of aviation safety." The Web site has two parallel publications, *Air Accident Digest Newsletter* and *Air Accident Digest Blog*. One is a traditional, factually oriented newsletter and the other is a personal-opinion Web log or blog. The two publications cover similar topics, but there are significant differences in writing style, information delivery and publishing technology.

The site says the "newsletter [is] dedicated to nonpartisan reporting on aviation safety and security." In-depth articles include color photos, graphics and Internet links to references and sources, as appropriate. Each newsletter has a table of the previous month's accidents and incidents for airline, corporate, general aviation, helicopter and military aviation. The newsletter can be read online, downloaded or received via e-mail at no cost.

While the newsletter aims at factual reporting, the blog is written from the author's subjective viewpoint and opinions. The blog contains commentary on aviation safety and security news; activities surrounding accidents and incidents; and noteworthy industry events. Each discussion item contains the time and date of posting and gives readers the opportunity to comment using a submission form.

The blog uses Internet technology to permit readers to respond to the discussions, track back from another Web site to this blog, and use RSS — "really simple syndication" — feed software to follow blog commentary and responses. ●

### Source

* National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161 U.S.A.
Internet: <www.ntis.gov>

— *Rick Darby and Patricia Setze*