Aircraft operators have built a generic hazard model for use in developing safety cases

Development of an aviation safety case is essential as it focuses a company’s top management and staff on the real risks that need to be managed and ensures that every reasonable effort is taken to provide safe operations.

SAFETY improvements have been achieved over the years through numerous developments, including better aircraft design, redundant systems, improved working practices and the introduction of quality assurance programmes, to name just a few.

Despite all that has been accomplished, experts predict an increase in the number of aircraft accidents as worldwide air traffic continues its steady growth in the years ahead. Unless significant changes are made to improve the nearly flat accident rate, by 2010 there could be an average of one airline accident per week. Left unchecked, this level of accidents would alarm the public and could place many aircraft operators in financial difficulty or even out of business. For that reason alone, the cost of enhancing safety systems is easily justified.

The introduction of a safety case offers a company’s senior management the opportunity to identify the major safety risks. Based on this knowledge, a company’s board can establish controls that reduce the likelihood of such risks causing an accident.

The commitment and organization that assures continuing safe operations is achieved through the introduction of a safety management system. A safety management system must be led by top management and must address all aspects of the business that have the potential to cause harm.

HAZARD IDENTIFICATION AND CATEGORIZATION

Figure 1.

The key steps in developing a safety case require that a corporate safety management system exists or at least is being developed. The safety case draws on corporate safety objectives and policy, which must make safety an explicit priority, at least equal to any other business imperative. Based on corporate decisions as to what safety level is to be managed, hazards are identified and risks assessed and controlled. Management must also develop and maintain a supportive culture that is “just” and “learning.” In aviation, this cultural change requires a willingness to learn from hazards and threats as well as from accidents and incidents. At the same time, management must deal sensitively with those responsible, unless reckless or deliberate behaviour warrants disciplinary action. It is essential that training provide all staff with an understanding of safety management and the extent of the corporation’s commitment to safe operations.

A safety case is the “systematic and structured demonstration by a company to provide assurance, through comprehensive evidence and argument, that the...
The company identifies and assesses major hazards and safety risks and then manages them to levels of risk which are as low as reasonably practicable. A safety case may cover all or part of an operation and, where more than one case is developed, each is described and controlled locally but managed through a corporate safety management system. Delineating cases is a management choice, but the resulting package of safety cases should cover all safety-critical activities. Safety cases may be set up for operations, for engineering, or both, or even used for specific projects such as the introduction of a new aircraft type.

Development of a safety case begins with identification of what should be managed, and by describing the boundaries of each case and establishing how a corporate safety management system is applied. The safety case should list safety-critical activities undertaken by a company and who is accountable; it also should identify which hazards pertain to each activity. Hazards are listed and analysed to identify threats, escalations and controls necessary to forestall hazards; this forms the hazard management section, an output of which is the hazard register. The safety case should list measures required to improve safety. At the completion of the exercise, and each time the safety case is renewed or updated, conclusions must be drawn on how it meets the case objectives, and a statement of “fitness for purpose” provided.

An additional benefit delivered by the safety case is the interface with other service or product providers where there are shared hazards. Interfacing in this instance describes the contractual relationship between companies where a supplier is responsible for part of an activity or product. Typically, an airline’s fuel supplier is responsible for delivering the correct product, while the flight or ground crew are responsible for its acceptance. Each shared safety-critical activity is covered by an interface document that defines precisely the point at which responsibility changes hands. The document assures mutual awareness of hazardous activities and ensures each party is clear about its responsibilities. Interface documents are typically attachments to the contract between the parties and may have legal connotations.

Central to a safety case is the identification and management of hazards. Clearly, without a robust list of hazards, a company cannot assure itself that it has established effective controls. Hazards, once identified, are assessed by utilizing a safety assessment matrix to determine their level of risk. The result of these assessments requires management to make decisions as to what, if any, actions need to be taken. Without such a systematic review, it would be difficult for management to ensure that all parts of the operation needing risk assessments have been identified.

The generic hazard model developed in workshops set up by Shell Aircraft was designed to cover only those hazards that would be common to a wide range of airlines or helicopter operations. Each individual company, using the generic hazard model, needs to account for specific hazards (i.e. the aircraft type, the location, or the existence of non-standard operations). A hazard, once identified, must be contained through procedural, organizational or physical controls. These measures alone are not enough as they can be circumvented if their purpose is not well understood, or if there is a lack of commitment by anyone involved. Training, assurance, awareness and accountability are all needed (see Figure 2).

Identification of hazards started with the definition of each hazard and what analysis tools would be used to define them. In the safety case described here, standard tools and definitions that had been used successfully elsewhere were employed. The primary tools were the “bow-tie” analysis model and a risk matrix. The bow-tie has proactive and reactive elements (Figure 3) that systematically work through a hazard and its management, using a methodology that Shell Aircraft calls the hazards and effects management process (HEMP). This requires that the hazards be identified, assessed and controlled — and also sets out recovery measures.

The bow-tie output is tested against a risk assessment matrix adapted for aviation (Figure 4). Judgements are made as to the probability or frequency of a hazardous event and the severity of its consequences. The hazardous events that are seen as safety-critical to the operator are added to the company’s hazard register. Senior management must then decide what level of risk the company will accept in order to manage hazards. If the likelihood of an occurrence is judged to be extremely remote, it may not be worth expending significant energy or resources on managing the risk. Conversely, if hazardous events are frequent and the consequences are minor, but could escalate, it would be appropriate to manage such risks within the safety case. Although the likelihood of occurrence or consequences is minor, it is appropriate to deal with them through normal workplace management. However, if the outcome of a hazardous event is significant and there is a likelihood of its occurrence, risk reduction measures should be taken to minimize the risk. This principle requires that if a control is technically possible, reasonable and achievable without causing financial distress, then the control must be put in place.

The hazard model

Shell Aircraft set up and facilitated two
workshop groups, one focusing on fixed-wing airline type services, and the other on offshore helicopter operations. The workshops involved pilots and engineers from a number of airlines and aircraft operators. Hazard management techniques learned in the workshops required that a hazard, once identified, is controlled. For instance, an aircraft in flight is an example of a controlled hazard, in that it has the potential for harm through its inherent energy. If the aircraft is not maintained in a controlled state a hazardous event may occur, and therefore measures are required to prevent the situation from worsening. The intent is that crew action, in accordance with procedures and checklists, will restore operating equilibrium. If these measures fail, the aircraft will likely suffer a consequence.

The initial task of the workshops was to identify hazards and list these as an entry point. Defining a hazard as “something with the potential to cause harm” enabled participants to identify hazards and confirm they had energy which could be released and cause harm. The process then continued, identifying potential flight and ground hazards, including locations. The presence of a hazard in different locations could warrant different controls or recovery measures.

The workshops moved on to identify primary hazards and, specifically, the hazardous events that resulted from first release of a hazard. Each event required the bow-tie analysis. Typical in such a complicated industry as aviation, this could have led to an unmanageable number of analysed events. The number of analyses was reduced through additional identification of hazards which were prime sources of energy. For example, dealing with the problem after landing.

In documenting development of a safety case structure, the workshops agreed that the safety case would need to cross-reference company manuals using signposting techniques. This significantly reduces the textual volume of a safety case. The other principle was to ensure that all controls identified to manage threats or escalation factors were embedded in operator or manufacturer processes, procedures and checklists. Within the safety case, the hazard analysis information produced in the bow-tie exercise is also processed into operator checklists.

The final safety case output was to produce the conclusion and statement of fitness (SOF). Normally this would be signed by the company’s chief executive officer. The SOF is crucial in that it confirms fulfilment of commitments needed to implement a comprehensive and structured approach to safety management. Also, the SOF is a visual demonstration to staff, regulators and customers of how well objectives, as defined by the safety management system, are being met.

The work of identifying hazards and hazardous events has not resulted in any major breakthroughs in finding new hazards. However, it was ground-breaking to gain an understanding of all hazardous events and highlighted that much of what is needed to control hazards is already in place. The 85 per cent of controls already in place are not necessarily as robust as they should be. Additional controls can be listed as remedial actions that need management continued on page 27.

The author is the Quality and Safety Manager for Shell Aircraft, the London-based aviation safety and standards adviser to the Shell Group for worldwide contracted aviation support. Shell Aircraft also operates Shell Group’s corporate fleet. Mr. Edwards may be contacted directly via email at cliffj.edwards@si.shell.com.

This article is an adaptation of a paper presented to a safety seminar organized jointly by the Flight Safety Foundation (FSF), International Federation of Airworthiness (IFA), and International Air Transport Association (IATA) in Rio de Janeiro in November 1999.
Appropriate data from different airlines should be pooled to support arguments for improvements that need to be made by manufacturers, ATC, regulators and airports. Finally, broadband satellite communications would allow cost-effective transmission and analysis of FOQA data in real time.

**Family assistance programme**

continued from page 6

Knowledge of the investigative process. The aviation investigation specialist spends much of his time with the investigator in charge and the various investigative groups. By understanding what is occurring in the investigation and coordinating the factual information which the investigator in charge will release to the public, the aviation investigation specialist can brief family members with up-to-date information on a daily basis. It is important to emphasize that the victims and their family members must receive the same factual information as the media.

The development of any family assistance programme requires a partnership among many organizations and a commitment to the shared goal of assisting victims and their family members. This is especially true for air carriers, which have a fundamental responsibility to victims and their families following an aviation disaster. It has been demonstrated in the past three years that by planning, coordinating and communicating with one another, positive changes can take place in the way the aviation industry and government respond to the needs of aviation accident victims and their families.

**Generic hazard model**

continued from page 14

Dealing with which to address, and when.

Safety improvements. Many of the improvements identified could be made without much effort or cost. Even so, some additional controls were identified that would have real costs. The prime findings of the process were that:

- Management reviews must be more active to ensure that intended improvements take place;
- Safety competence and accountability are often ill-defined or missing in the organization, in particular the ability to trace accountability from the CEO down;
- Training in non-flying/technical areas was lacking, especially when staff are promoted to management with significant changes in skill and knowledge requirements;
- There was a significant amount of work being done with the best of intentions but without regard to procedural requirements;
- Use of procedures, notably in engineering, was not systematic and often not assessed by supervision or audit;
- Workplace monitoring and supervision practices were inadequate;
- Processes to manage change were ineffectual;
- Audit processes were frequently inadequate;
- Human factors were not well addressed, with shortfalls in training and/or application of the principles; and

- Incident investigation often addressed effect rather than cause and therefore denied the company the chance to learn.

The hazard modelling workshops were carried out over eight months in 1999 with pilots and engineers from eight airlines and five helicopter operators. These workshops produced two generic hazard models, one each for fixed- and rotary-wing application. Nineteen generic hazards were identified. Each of the hazardous events was discussed at length, and control methodologies defined. It became clear that the means of controlling a hazard varied depending on whether the aircraft was in flight, undergoing maintenance or moving on the ground. In all, four fixed-wing and six rotary-wing locations were defined. To aid with generation of bow-tie models for each hazardous event, generic threat and threat control lists were assembled. These included descriptions for each threat and the source where the threat or control would be relevant. These generic models can be adopted for any aircraft operation. The generic hazard model is now being translated into the field by a number of operators who are customizing it to specific operations.

**Conclusion.** Development of a safety case involves significant effort by aircraft operators. However, projected growth in the number of accidents is unacceptable. Current efforts are somewhat piecemeal and are not reducing the accident rate. A positive, integrated approach with support structures is required to improve the situation. To make further progress will require changes in corporate culture, including management's approach to safety. Some would argue that the industry is over-regulated, but this viewpoint is insupportable when the costs of human life and corporate liability are taken into consideration.

**Accident report**

continued from page 20

A flight service station specialist, as opposed to a tower controller, at the Fredericton airport at the time of the arrival of the flight was not material to this occurrence.

**Safety action taken.** Procedures outlined in Air Canada's Aircraft Technical Bulletin and Bombardier's All Operator Message, issued following this occurrence, will reduce the possibility of ice accumulation on the CL-65 aircraft. Nevertheless, there is still a risk that while an aircraft is operating below 400 feet AGL, ice could accumulate to an extent that aircraft performance would be materially affected without the pilots being aware that they had entered icing conditions, or that ice had accumulated. If the amber ICE light was not inhibited below 400 feet, however, an extra safeguard would be in place to alert pilots to the presence of ice. In a TSB Aviation Safety Advisory to Transport Canada on 9 April 1999, it was suggested that Transport Canada consider taking action to remove the inhibition of the ICE light below 400 feet.

In February 1998 the TSB, in an Aviation Safety Advisory, suggested that Transport Canada consider eliminating the ELT carriage exemption for turbojet aircraft. In response,