Diagnosing What Hasn't Happened Yet

Bill Voss's editorial (*ASW*, 7/08, p. 1) prompts these comments.

While a safety management system (SMS) is a great process, that does not mean every organization should do it in the same way. Each SMS should be tailored as a function of the James Reason risk/defense model of that organization.

An original equipment manufacturer (OEM) for aircraft, engines or propellers usually has — at least in Europe — a design organization approval (DOA) and a design organization manual. Both follow strict regulatory rules. The processes used mimic SMS processes almost one to one, but are mostly valid for "Reason" defenses: management (fallible decisions); organization (error-inducing structure); and conditions (psychological factors). So, primarily, latent failures.

Airlines, airports and ATC perform millions of operations per day, so are heavily involved in production and last defenses (both active and latent failures).

That does not mean that an OEM does not have incidents, but they are of an entirely different nature and magnitude (tens versus millions of events). Furthermore, there are strict processes for dealing with these nonconformance reports.

No matter how good the SMS or DOAs, any organization will be faced with two major issues: In which domain is the incident, accident or issue, i.e. historic, diagnostic or prognostic? And is the CEO of the organization prepared to spend the money?

As we move from historic to diagnostic to prognostic, the difficulty of making that investment decision gets progressively tougher. While industry already has a hard time incorporating, for example, all fuel flammability measures, let alone introducing nitrogen inerting following the TWA Flight 800 accident [July 1996], this will turn into a monumental process to spend money on a defense for something that has yet to develop into a full-blown crisis, such as UAVs [unmanned aerial vehicles] crashing into other aircraft or on cities, or widespread hacking and/or inadvertent malignant viruses affecting aircraft computer systems such as data base updates of electronic flight bags via the Internet.

We also appear not smart enough to have a diagnostic event-finding structure in place to catch the events that preceded the British Airways Boeing 777 accident at Heathrow [January 2008]. I will bet that eventually someone will find that the accident precursors were there but not noticed.

The problem we face today is that safety is at a standstill because of the scarcity of accidents, hence the aerospace industry is not learning anymore, so we have to face these difficult issues and come to grips with them if we want to improve safety.

Rudi den Hertog
Chief engineer
Fokker Services

AeroSafety World encourages comments from readers, and will assume that letters and e-mails are meant for publication unless otherwise stated. Correspondence is subject to editing for length and clarity.

Write to J.A. Donoghue, director of publications, Flight Safety Foundation, 601 Madison St., Suite 300, Alexandria, VA 22314-1756 USA, or e-mail <donoghue@flightsafety.org>.