Operating Highly Complex and Hazardous Technological Systems Without Mistakes: The Wrong Lessons from ValuJet 592

Dr. Brian Stimpson, P.Eng.
Chair of the Communications Committee, Association of Professional Engineers and Geoscientists of Manitoba
and
Professor and Head of the Geological Engineering Department, University of Manitoba

Published in the October 1998 edition of the Manitoba Professional Engineer (now "The Keystone Professional")
Reprinted with the permission of the Association of Professional Engineers of Manitoba

Fishermen ducked for cover as the twin-engine DC-9 banked vertically to the right and went straight down into Everglades Holiday Park, Florida, on a warm, May afternoon in 1996. The first fisherman called the emergency dispatcher on his cellular phone within a minute. Part of his cryptic message - "It will not be in one piece" - was tragically true, and two pilots, three flight attendants, and 105 passengers lay dead in a watery grave. Investigators soon determined the physical cause - a fatal cargo of old oxygen canisters and three tires stowed in Flight 592's forward hold. Ignition of the canisters precipitated an inferno that quickly overwhelmed vital control systems; the pilot had no means to divert the craft from its deadly vertical dive.

What happened is clear, but why did it happen? In the May 1998 issue of *The Atlantic Monthly*, William Langewiesche makes the case that the disaster was a "system accident," a kind of incident that cannot be prevented by conventional solutions, and that more lie in wait, and not only in the airline business. Is the goal of a zero-accident future a tantalizing but unattainable goal? In studying the events and decisions that led to the crash of Flight 592, Langewiesche argues that other serious failures of systems that require complex organizations for their control and operation - in power generation, chemical manufacturing, nuclear-weapons control, and space flight, for example - are "virtually guaranteed to occur".

The two most common forms of accidents are the procedural and the engineered. Obvious mistakes such as forgetting to put on a face mask while using resins or chemical sprays occur daily. These are procedural accidents. "Engineered" accidents are those unexpected failures that usually lead to improved designs and/or materials following detailed examination by experts. "God-like" designers or more prolonged testing at the prototype stage would have uncovered them earlier. From such accidents - sometimes tragic - progress is made and the technology is made safer for those who follow.

The ValuJet accident was, according to Langewiesche, different in that it falls into the elusive category of a "system accident". Perrow, the Yale sociologist, prefers a different term - a "normal accident" - because he considers that at our current stage of technological development in which we are using complex organizations to manage and operate dangerous technologies, accidents of this kind are "normal", i.e. they should be expected. Risk is accepted in these ventures but is usually obscured. It is not that tradeoffs are deliberately made between profit/convenience and safety, but in a complex system bad choices or mistakes will inevitably occur. Most of the time these do not result in tragedy because "Murphy's Law is wrong" - what *can* go wrong usually goes *right*." But, just once in a while, a chain of bad choices, oversights, and mistakes leads to catastrophe, as in Flight 592. Three tires and five cardboard boxes of old oxygen generators - an inferno-in-waiting - somehow found their way on board.

Step 1 in the fateful train of events took place with the removal of the small oxygen generators (steel canisters) from three twin-jet MD-80's, which ValuJet had bought and was having refurbished in a hangar at Miami Airport by an outside firm called SabreTech. Airline travellers are familiar with instructions on how to use an oxygen mask in the event of a loss of cabin pressure. In the MD-80 canisters, oxygen generation was by means of an exothermic chemical reaction initiated by a displacement of a firing pin and detonation of a minute explosive charge when the passenger pulled on the lanyard attachment on the face mask. Most of the generators on the MD-80's had come to the end of their licensed lifetime, i.e. had "expired".

ValuJet had provided SabreTech with explicit instructions on how to remove the generators and with general

warnings about the fire risk: *If generator has not been expended, install shipping cap on firing pins.* Seventy two SabreTech workers, many of them temporary, logged 910 hours replacing canisters. Working to a tight deadline and occupying, as Langewiesche puts it, "a world of boss men and sudden firings, with few protections or guarantees for the future", they removed the generators, taped or cut off the lanyards, and stored them without plastic safety caps in five cardboard boxes that were conveniently lying around in the hangar. Two mechanics signed off the work, including the line indicating that safety caps had been attached. Under time pressure, the distinction between expired and expended canisters, which was clear to those who wrote the technical manuals, was not clear to the hard-pressed mechanics. In reality, many of the canisters being removed were expired but were not expended, i.e. they could still be fired.

Mechanics also attached green tags to most of the removed oxygen generators to indicate that they were "repairable", which, in fact, they were not. Clearly, supervisors and inspectors failed to provide clear, detailed instructions. The simple instructions of the work cards appeared in stark contrast to the huge MD-80 manual in which instructions for the storage, disposal, and destruction of oxygen generators was described. Most of the canisters should have been destroyed and have never made their way on to an aircraft. However, if plastic caps had been provided and their placement properly verified, Flight 592 would never have burned. Some mechanics later claimed to have made known their concerns about the lack of safety caps. If that was, indeed, the case, their concerns were not acted upon. Other mechanics had, out of curiosity, fired off some of the canisters, but the possibility of the devices being shipped does not seem to have occurred to any SabreTech mechanics.

Step 2. The unmarked cardboard boxes, stored for weeks on a parts rack, were taken over to SabreTech's shipping and receiving department and left on the floor in an area assigned to ValuJet property.

Step 3. Continental Airlines, a potential SabreTech customer, was planning an inspection of the facility, so a SabreTech shipping clerk was instructed to clean up the work place. He decided to send the oxygen generators to ValuJet's headquarters in Atlanta and labelled the boxes "aircraft parts". He had shipped ValuJet material to Atlanta before without formal approval. Furthermore, he misunderstood the green tags to indicate "unserviceable" or "out of service" and jumped to the conclusion that the generators were empty.

Step 4. The shipping clerk made up a load for the forward cargo hold of the five boxes plus two large main tires and a smaller nose tire. He instructed a co-worker to prepare a shipping ticket stating "oxygen canisters - empty". The co-worker wrote, "Oxy Canisters" followed by "Empty" in quotation marks. The tires were also listed.

Step 5. A day or two later the boxes were delivered to the ValuJet ramp agent for acceptance on Flight 592. The shipping ticket listing tires and oxygen canisters should have caught his attention but didn't. The canisters were then loaded against federal regulations, as ValuJet was not registered to transport hazardous materials. It is possible that, in the ramp agent's mind, the possibility of SabreTech workers sending him hazardous cargo was inconceivable.

Step 6. The ramp agent discussed the load with the co-pilot, who should have known better than to accept the material. The last line of defence was breached; the five boxes were taken into the forward cargo hold and stacked around the outer edge of one of the large main tires which was lying flat. The other main tire was leaned against the bulkhead.

Step 7. Flight 592 took off. Six minutes later there were signs of instrument failure and one minute later the last message was recorded on the flight recorder, "Completely on fire". The precise sequence of events in the cargo hold will never be known.

The investigation into the accident noted the procedural and "engineered" problems and responded with obvious recommendations, including the installation of fire detectors and extinguishers in all cargo holds. But were elements of this crash also in that disturbing category of a "normal" accident, as described by Charles Perrow in his book *Normal Accidents: Living With High-Risk Technologies?* These occur, he says, in unforeseeable ways in complex organizations that are characterized by "interactive complexity" in which components or elements -

material, organizational, or psychological - are connected in multiple and often unpredictable ways, and by "tight coupling" in which the speed and inflexibility of the operating system (e.g. Flight 592 when airborne) frustrate or prevent the human operator from recovering the system when a series of events cascade in an accelerating fashion. Under conditions of "interactive complexity", Langewiesche writes, "If the system is large, the possible combinations of failures are practically infinite. Such unravellings seem to have an intelligence of their own: they expose hidden connections, neutralize redundancies, bypass 'fire-walls';, and exploit chance circumstances that no engineer could have planned for."

Langewiesche concludes his *Atlantic Monthly* article with the ominous statement, "Conventional accidents - those I call procedural or engineered - will submit to our solutions, but as airline travel continues to expand, we can expect capricious system accidents to blossom. Understanding why might keep us from making the system even more complex, and therefore, perhaps more dangerous, too."

Is the operation of highly complex systems without "system" accidents an impossibility? Todd La Prote, Karlene Roberts, and Gene Rochlin at the University of California, Berkeley (*Beyond Engineering: A New Way of Thinking About Technology,* Oxford University Press, 1997; an excerpt from the book appeared in *Technology Review*, July 1997) think not. They examined a number of systems involving great technological complexity and many hazards, including aircraft carriers and air traffic control towers, that operate essentially without mistakes. An aircraft carrier must land and launch weapons-loaded planes of various types on a short "see-sawing" runway. At the same time as one plane is being accelerated to 140 knots (160 miles per hour) every 50 seconds by steam catapult, another craft is just touching down at full throttle and is decelerated to a standstill in about two seconds by four arresting wires. On a Nimitz-class carrier, this is just part of a huge operation involving 5000 men and women who are predominantly teenagers. Mistakes are rare. Little wonder LaPorte and his colleagues wanted to study this organizational and technological feat first-hand to look for answers that might be applied elsewhere.

At first glance, the organizational structure on an aircraft carrier appears hierarchical and the thick operating manuals and training activities look no different than those found in a complex manufacturing plant. However, when the aircraft carrier goes into "active" mode and planes are landing and being launched, there is a vital change. Co-operation and communication largely override hierarchical position. There is no time for instructions to move up and down a chain of command. Team play, constant communication (telephone, radio, hand signals, writing), watching colleagues' actions, and the oversight of more experienced personnel who monitor activities, mean that mistakes are rare and can often be corrected before harm is done. Safety is everyone's responsibility. Crew members are encouraged to think for themselves and to act without authorization from anyone else if they perceive any threat to safe operation. This can even include the lowest rating suspending flight operations and, even if wrong, he/she will not be penalized. The steady turnover of officers and crew also means that the aircraft carrier is a "floating school", with little chance for operations to become routine.

The Diablo Canyon Nuclear Power Station, California, also has all the initial signs of a rigid hierarchy and an almost literal tower of regulations and procedures. However, Paul Schulman, a collaborator with LaPorte, Roberts, and Rochlin, discerned another side of the operation. While there are well-established rules which guard against errors of omission, there is also a process for avoiding errors of commission, i.e. actions that can have unexpected consequences. Continuous learning and improvement and constant questioning of accepted practice and thinking about what you are doing are cultivated. Employees who become too confident or stubborn are seen as undesirable.

Communication flow and co-operation rather than bureaucratic channels permit the employees to organize themselves into different patterns to meet the needs of the moment: hierarchical, yet also collegial when required; rule-bound but also learning-centred; centralized but decentralized when appropriate. By contrast, poor communications and deference to hierarchy in a strict chain of command cultivate, over time, an environment of false security. According to LaPorte et al, the Challenger accident; the 1982 crash of a Boeing 737 into the Potomac River, Washington; the collision of two 747s in the Canary Islands in 1977; and the deaths of thousands from a cloud of methyl isocynate in Bhopal, India, all contained such elements. Why, then, view Flight 592, as Langewiesche does in his *Atlantic Monthly* article, as a capricious accident that occurred through a chain of

unpredictable events? It would appear that a different work environment, one in which communication, co-operation, responsibility, team work, and learning were valued and cultivated, would have prevented the deaths of 110 souls.

Greater organizational reliability, some would argue, comes with an economic cost. But, if we can reduce technological costs while increasing the reliability of technology as we have done, why should it not be possible to have smarter organizations with reduced cost? Above all, for the engineer, failure is not a design option.

[CNS Manitoba]

[CNS home page]