

Testing

Fatal Defect

CHAPTER I



INSIDE RISKS

SLUMPING WITH AGE, the rounded, heavily wooded peaks of the Vosges massif in northeastern France bear their long history with stolid fortitude. Castles, monasteries, and ancient fortifications guard the heights; medieval towns and patchworks of vineyards crouch in verdant valleys opening onto the plains of Alsace, adjacent to the Rhine River. In this part of France, summers tend toward the warm and sunny, though winters in the highlands can be markedly snowy and severe.

Near the northern tip of the Vosges, Mont Sainte-Odile rises to a height of nearly 2,500 feet above sea level. Pilgrims flock to the cluster of buildings that crown the peak to pay homage to Sainte Odile, who founded a convent on this site in the eighth century. Tourists trek the serpentine road to its summit for the magnificent view. On a clear day, they can glimpse the city of Strasbourg, about thirty-five miles to the northeast, and the Black Forest in neighboring Germany.

On January 20, 1992, a jet airliner plowed into a pine forest in the highlands near Mont Sainte-Odile. Just seven minutes away from the airport serving Strasbourg, the sleek Airbus A320 aircraft should have been flying at an altitude of nine thousand feet and descending slowly. Instead, it was at roughly twenty-four hundred feet when impact occurred at 7:45 in the evening. The airliner sent

4 FATAL DEFECT

out no distress signal before the crash. It simply broke radio contact and abruptly vanished from radar. The nine passengers who survived the crash reported they had noticed nothing out of the ordinary until the moment of impact.

Eighty-seven people died in the crash. Darkness, freezing temperatures, thick fog, gusty winds, and deep snow hindered rescue efforts. It took more than two hours for a relief party to locate the wreckage and begin ministering to the survivors. By that time, news of the disaster was already spreading throughout the world by way of a vast electronic web of telephone lines, radio links, microwave transmitters, and the rest of the paraphernalia that constitutes our communal nervous system. As details of the crash emerged, radio and television reports, followed by newspaper articles, conveyed to a receptive audience the raw material to feed an age-old, ghoulish fascination with disaster and tragedy.

The next morning in Washington, D.C., James H. Paul, a staff member of the investigations and oversight subcommittee of the U.S. House of Representatives, noticed a report of the crash distributed by the Reuters news agency. The story bore the provocative headline: "Latest Crash Heightens Controversy over Airbus A320."

The A320's notoriety stems from the innovative technology incorporated in the airliner. Built by a consortium of French, German, British, and Spanish firms working together as Airbus Industrie, this narrow-bodied, twin-engine, 150-seat aircraft was the first of a new breed of airliner in which pilots control the airplane entirely through computers.

Paul's interest in the A320 crash arose in part from his role as one of the authors of a 1990 study called *Bugs in the Program: Problems in Federal Government Computer Software Development and Regulation* and in part from a concern he shared with others in the computer world about the difficulties of coping with the faults, or bugs, that plague just about any computer system.

Paul activated his computer's link with the Internet, a labyrinthine,

computer science and software engineering offered no assurance that the immense difficulties posed by developing the required system could ever be overcome. In a devastating critique of the state of the art in computer science research, he argued: “Good software engineering is far from easy. Those who think that software designs will become easy [via new technologies] and that errors will disappear have not attacked substantial problems.”

Four weeks after the inaugural issue, Neumann distributed its sequel, which featured varied reactions to items in the first issue and to the whole notion of an electronic Risks forum. In addition, it introduced several new topics, including problems with spacecraft software and with diagnostic aids that rely on intricate webs of rules to answer medical questions. Two days later, a third issue appeared, and the pace of publication has rarely slackened since, except for the brief intervals when Neumann has gone on vacation or when his own computer system has suffered a glitch.

In the early days, most of the contributors to the Risks forum were Neumann’s friends or colleagues. But the number of contributors and the forum’s audience grew rapidly. Nowadays, it’s not unusual for Neumann to receive submissions from people he doesn’t know at all, and his audience is so diverse and widespread that he has no real idea of its full extent.

BY JANUARY 22, 1992, the Risks forum had reached volume 13, number 5, and James Paul’s submission on the A320 crash was just one of fifteen items mentioned in this issue. The four issues that followed all included comments on the A320 accident. Based largely on sketchy newspaper reports, these early, inconclusive speculations on what may have gone wrong turned on the resemblance between this disaster and two previous A320 crashes. In each in-

stance, the pilot appeared to think that the aircraft was higher than in fact it was.

In June 1988, one of the first A320 models sold to Air France had brushed a patch of trees and crashed at the end of a demonstration flight at an air show. The commission of inquiry into the crash concluded there was nothing wrong with the airliner. In fact, the aircraft's computers had kept the plane's wings level to the end, preventing the plane from tumbling and making the accident worse. The commission's report accused the pilot of recklessness in flying too low. But the pilot, who survived the crash, insisted the airplane's equipment had failed to warn him of the loss of altitude just before the crash.

On a clear day in February 1990, an A320 operated by Indian Airlines was making its final approach for a landing at Bangalore airport when the airplane's speed dropped to a dangerously low level. Descending rapidly, the aircraft slammed heavily into a golf course just short of the runway. Ninety-two people died. Apparently, the pilot had inadvertently pushed the wrong button, setting the plane's engines on idle—a maneuver normally used for making a descent from higher altitudes but not immediately before a landing. Some critics of modern cockpit design have argued that the pilot had been lulled into a false sense of security. Following the accident, Airbus engineers altered the engine-regulating software to prevent the plane from flying more slowly than a certain speed.

Initially, the most puzzling aspect of the A320 crash near Mont Sainte-Odile was the pilots' apparent failure to realize that their airplane was descending rapidly and getting too close to the ground. Most airliners now have an alarm system that automatically calls out warnings in a loud, authoritative voice whenever the airplane descends too quickly or nears the ground. However, the system is mandatory only for international flights. Air Inter, the domestic French airline operating the A320 that crashed, had chosen not to

install these alarms in all its planes. Company officials had complained that the alarms gave too many false warnings, and they noted that they were unnecessary anyway because the airline's pilots were quite familiar with the terrain across France.

In fact, when the alarm system had originally become mandatory nearly two decades ago, it was so unreliable that pilots quickly developed a hatred of its wrongly insistent voice, and many learned to ignore it. Subsequent improvements brought the error rate down considerably, but Air Inter believed the system was still too fallible. It's possible that even if the alarm had been functioning, the crew would have ignored it.

The A320 did have a separate system that uses a radio beam reflected from the ground to determine the aircraft's altitude and, in a simulated voice, calls out the reading at certain height intervals during maneuvers such as landing. It's the kind of task a copilot used to perform—and sometimes still does—to help the pilot, who must focus on flying the airplane. A recording of cockpit sounds during the last moments before the crash revealed that the pilots did get an automatic warning when the plane had dropped to just two hundred feet above the mountain's slope. But that left only one or two seconds before impact.

The question of how the pilots got into this untenable situation in the first place brought renewed attention to the A320's "glass cockpit." Instead of the round-dial instruments and toggle switches found in the cockpits of older planes, A320 pilots face an array of computer screens for monitoring the airplane and keyboards for typing in commands and making choices. Instead of dealing with separate dials and gauges for airspeed, altitude, rate of climb, and so on, they see the necessary information compactly displayed on their screens. But such a system also makes it more difficult for pilots to monitor long-term trends in airspeed and other flight parameters, so they must rely on automatic alerts or warnings to tell them about significant changes in the plane's status.

Computers handle so many functions that pilots spend a con-

able amount of time typing in data, in effect programming the computers to set routes and prepare the plane for certain maneuvers. The computers automatically take into account such factors as efficiency and aircraft safety, and they present the most economical and safest choices to the pilots. The crew can enter a flight plan, review it on the display, and command an efficiency factor. When coupled with the autopilot, the airplane's flight management system can control virtually the entire flight.

As a result, increased automation has brought the pilot's role closer to that of a manager. Airplane designers have shown a strong preference for taking the pilot out of the control loop as much as possible. One manufacturer's preflight procedure simply requires that certain buttons be "punched out." The system isn't touched by the pilot except in abnormal situations.

In 1991, David Woods, a professor of industrial and systems engineering at Ohio State University, and his coworkers published an opening study that highlighted the problems of such a high level of automation. The study concluded that automation actually makes flying more difficult for pilots, even for those with considerable experience in glass cockpits. Of the pilots surveyed, most showed significant gaps in their knowledge of how computers run an airplane, and many admitted they had encountered situations in which they were surprised at what the plane did under certain circumstances.

Nearly all the pilots complained that the computer system was decidedly unfriendly, for example, flashing the notably opaque message "invalid entry" instead of explaining why a certain typed command was unacceptable. Faced with complicated instructions and multiple screens filled with information, pilots tended to adopt a cookbook mentality and use memorized "recipes" in their interactions with the computers. Even the option of having different ways of accomplishing the same task presented problems. Individual pilots developed alternative styles of programming, and that sometimes made it difficult for another pilot to step in and take over at