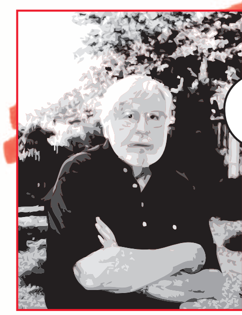

Outside the Lines

"Problems cannot be solved by thinking within the framework in which the problems were created." – Albert Einstein

by Ira J. Rimson
and Ludwig Benner, Jr.

The Sky Isn't Falling — Or Is It? Part 1

"Truthiness: The quality of preferring concepts or facts one wishes to be true rather than concepts or facts known to be true." — American Dialect Society's definition of Stephen Colbert's term

In the old joke about the first pilotless passenger flight, the preflight crew announcement ends with "… and you can rest assured that nothing can go wrong — can go wrong — can go wrong…."

Imagine this: You are asleep in your warm bed at 3:50 a.m. when suddenly a 10,000-pound flying machine crashes through your roof and out through the sliding patio doors. You shriek, "What the …?" and leap out into the chilly house, the temperature of which is now falling rapidly from the cold air rushing in through holes in your roof and wall.

No, Virginia, that wasn't Roswell.

That's what *could* have happened at 0350 on April 25, 2006, 10 miles north of Nogales, Arizona. But it didn't — quite. The unmanned General Atomics Predator B missed the house by less than 100 yards.

The Predator B is a 10,000-pound MGTOW[1] unmanned air vehicle[2], 36 feet long, with a 66-foot wingspan. A Honeywell TPE 331-10Y turboprop engine turns a pusher propeller at the rear of the fuselage. Its 3,900-pound-plus fuel capacity permits it to stay aloft for more than 30 hours at altitudes up to 50,000 feet above mean sea level (MSL). The Predator's employment by U.S. forces in Iraq and Afghanistan, first as an "eye-in-the-sky" and later as an attack "system" with on-board Hellfire missiles, helped it evolve from a technical curiosity to a reliable aeronautical device.

In 1818 in France, Charles Rozier developed the first recorded unmanned balloon from which bombs could be delivered.[3] UAVs were actively employed as a weapons system in 1849 by Austrian forces attacking Venice with unmanned balloons loaded with explosives. The Austrian plan was:

"Venice is to be bombarded by balloons, as the lagunes prevent the approaching of artillery. In a favorable wind the balloons will be launched and directed as near to Venice as possible, and on their being brought to vertical positions over the town, they will be fired by electro magnetism by means of a long isolated copper wire with a large galvanic battery placed on the shore. The bomb falls perpendicularly, and explodes on reaching the ground."[4]

---

[1] Maximum Gross Take-Off Weight.

[2] The descriptive nomenclature for aircraft that fly with no human crew on board has evolved over the years in keeping with the complexity of boffin-babble: Originally called "drones" (through the 1970s), they have graduated to "UAVs" (Unmanned Air Vehicles), and most recently to "UASs" (Unmanned Air Systems), ostensibly in recognition of the complex supporting systems required for their successful operation.

[3] Tobias Nisser & Carl Westin, *Human Factors Challenges in Unmanned Aerial Vehicles (UAVs): A Literature Review*. TFHS 05:1, Lund University School of Aviation, November, 2006, p. 1.

[4] *Scientific American*, March 17, 1849, p. 205.

At least some of the balloons launched from the Austrian ship Vulcano worked as planned. Others were caught in a change of wind and, much to the planners' chagrin, were blown back over Austrian lines.[5]

Military use of UAVs expanded widely during the Vietnam war, and state-of-the-art UAVs and UASs have seen regular use in Iraq and Afghanistan in both surveillance and attack roles. In April 2001, a Northrop-Grumman Global Hawk flew non-stop for 22 hours from Edwards Air Force Base, California, to RAAF Base Edinburgh, Australia, the first pilotless aircraft to cross the Pacific Ocean.

"Unfortunately, some eager civil agencies have neglected to ensure that public safety achieves similar protection from errant unmanned aeronautical systems as it does from mismanaged manned aircraft."

Potential civilian users recognize the operational and economic benefits of unmanned air systems to conduct surveillance tasks: patrolling borders and coastlines, evaluating environmental calamities, surveying disaster sites, patrolling pipelines and transmission cables, and myriad additional roles currently performed by manned aircraft. But do they recognize the risks?

Unfortunately, some eager civil agencies have neglected to ensure that public safety achieves similar protection from errant unmanned aeronautical systems as it does from mismanaged manned aircraft. For example:

The Houston, Texas Police Department was embarrassed in November 2007 when it was caught by a local television channel's helicopter conducting an unannounced test flight of Insitu, Inc.'s, "Insight" UAV[6] over isolated real estate in Waller County. Despite a professed joint FAA/HPD "test project," conflicts with other aircraft could have occurred because the FAA did not issue a public "NOTAM" — Notice to Airmen — to announce that the UAV operations were scheduled to take place in the area. The FAA had merely been issuing Certificates of Authorization for more than 100 test flights as "…part of a pilot program to help identify the hazards and associated risks of operating unmanned aircraft by law enforcement agencies and to determine if appropriate mitigations can be developed."[7] We fervently hope that the hazards and risks are identified and mitigated prior to a mid-air collision between a UAV and a manned aircraft.

At the closing session of the FAA's First Annual International Aviation Safety Forum in 2004, John Langford, chairman and president of Aurora Flight Sciences Corporation, observed:

"We have high reliability controls today, but the question is how do you get them down to maintain the statistical levels of safety but you dramatically reduce the cost. *[sic]*[8] There are technological approaches that can do that. They don't involve today's approaches, which are primarily based around hardware redundancy where you have multiple levels of the same type of hardware integrated in such a way that they have voting schemes, or if one fails, you can go to a backup system.

"There are many issues, and one of the fundamental ones is that in robotic systems, in an important way, you capture all of the lessons of all the previous mistakes and incidents that have gone before you. On any given day, on a flight, in a manned aircraft, the reliability, the safety of that system is strongly dependent on both the equipment and on the pilot up front, in terms of their training, their readiness for that operation.

"In the UAV sector, obviously, the paradigm is shifted as you're trying to get higher reliability, longer lifetimes on the systems and lower training costs. There is no human immediately in the front of the aircraft. The systems today that are used in robotic planes are much less reliable than their counterparts that we see in the national airspace system today, but that is a transient, that's changing very quickly."[9]

Those systems may not be changing quickly enough: On August 24, 2007, a Raytheon Cobra

---

[5] Demonstrating the impotence of both the planners' meteorological prognostications and their probabilistic risk assessment skills.

[6] See www.insitu.com.

[7] http://aero-news.net/genav, November 30, 2007.

[8] In our professional opinion, Mr. Langford (and the FAA) should be more concerned with real levels of safety than with the kind of statistical manipulation employed to meet regulatory requirements.

[9] John Langford, Proceedings of the First Annual FAA International Aviation Safety Forum, Closing Session, pp. 9-11.

unmanned aircraft system (UAS)[10] crashed near Whetstone, Arizona, after an uncontrolled descent.[11] Of note in the preliminary report is the statement: "The ground-based flight crew was not injured." (That may be an advantage of unmanned aircraft systems, but it doesn't bode well for any future plans for pilotless transport aircraft.)

The National Transportation Safety Board (NTSB) determined that neither mishap resulted from hardware or software failures; both resulted from human error — "Pilot Error," if you choose to apply the euphemism to pilotless aircraft. That should be a wake-up call for system safety analysts.

In the General Atomics' Predator instance, the "pilot" switched control between operator consoles without using the checklist because he was "in a hurry." As a result, he didn't "match" the control positions of the two consoles before making the switch. The condition lever (fuel and propeller controller) of the console to which he shifted control was in the "fuel shut-off" position, thus cutting off fuel to the Predator's engine when the shift was made. The "pilot," unable to determine why the UAV was descending, tried to establish emergency procedures until it descended below line-of-sight communication capability.[12]

In the Raytheon Cobra case, the "student pilot" became involved in attempting to control two UAVs using both a computer-interfaced pilot console and a manual pilot console. He lost track of the specific addresses on each of the consoles, and which aircraft each controlled. His incorrect assumption of switch positions resulted in improper directives being addressed to one of the craft. Its autopilot disconnected, and it rolled and dived into the ground.

As a result of its investigation of the Arizona Predator accident reported above, the NTSB issued five recommendations to the FAA[13] and 17 to the U.S. Customs and Border Protection Agency,[14] which we will examine in detail from a system safety perspective in forthcoming columns. One lesson to be learned is

[10] See http://www.cloudcaptech.com/misc/Cobra_UAS_Data_Sheet.pdf.
[11] See NTSB Docket SEA07LA237, available via links at www.ntsb.gov.
[12] NTSB docket CHI06MA121, Narrative, p. 2.
[13] NTSB Recommendations A-07-65 through A-07-69.
[14] NTSB Recommendations A-07-70 through A-07-86.

clear: Despite frequent similarities, task demands for pilots of unmanned flying machines differ distinctively from those for operators of manned aircraft. They must be analyzed and compared in detail before they can be clearly understood, and their hazards mitigated.

In 1977, Gerard Bruggink of the NTSB's Bureau of Air Safety observed that, "All accidents result from the uncritical acceptance of easily verifiable assumptions." That argument is especially applicable to accidents that resulted from hazards and risks that were not thoroughly analyzed during systems' conceptual and developmental stages. Whether analytical flaws are in assumptions, data, methodology, knowledge, procedures or skills, they represent a category of "human error" that is seldom acknowledged.

We previously posed the argument that current system safety analysis methodologies fail to account for the kinds of human errors that led to the two cited mishaps, because they fail to deal with potential outcomes that result from reasonably foreseeable acts. System safety analytical methodologies and practices that fail to examine the full range of plausible human responses cannot reliably limit or mitigate all likely undesired outcomes.