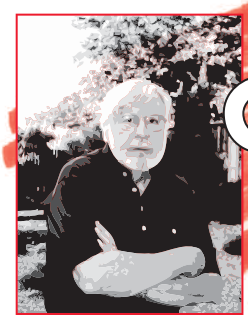

Outside the Lines

"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 2

Failure starts slow, but it grows. — James R. Childs[1]

In our last column[2], we reviewed recent events in which out-of-control Unmanned Aeronautical Vehicles/Systems (UAVs/UASs[3]) hazarded the health and welfare of persons and property under their flight paths. In those cases, the "system" part of "UAS" was insufficiently robust to prevent unanticipated human behavior from voiding whatever hazard control measures, if any, had been designed and built into the systems. Potential dangers came about because systems jeopardized their own safe operation by tolerating their human operators' deviant behaviors. Control measures, if any, sat idly by while humans forfeited control over their performance. The fact that the outcomes were seemingly benign to the public can be attributed solely to chance. Those unplanned outcomes happened despite the fact that myriad well-documented historical lessons have demonstrated that luck is a lousy barrier.[4] It seems to us that many lessons that have long been learned by rote in the manned aircraft world have yet to be recognized by persons and agencies responsible for protecting public lives and property from hazards posed by unmanned aircraft (UAs).

We quoted John Langford, chairman and president of Aurora Flight Sciences Corporation, in our prior column. He observed of robotic aircraft development:

"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." *[emphasis added]*

All previous lessons? Learning from past experience is fundamental both to developing safe and efficient new systems, and continuously improving the performance of existing systems. Those lessons are often expensive. They come at the expense of failures that were not anticipated, that occurred despite purported risk assessments. The people responsible analyzed those failures, and tested and effected countermeasures.

Lessons from failures are frequently applied across technological boundaries; all it takes is a little imagination. Hard-earned lessons should not be squandered by "not-invented-here" rejection or, worse, by misplaced belief in infallibility. In the case of the Predator B [Figure 1] crash in Arizona, the adverse scenario began when one pilot's operating console "locked up" during a U.S. Customs and Border Patrol mission.[5] Detailed procedures, including a checklist, were specified when

---

[1] From *Inviting Disaster: Lessons from the Edge of Technology*. New York, Harper Collins, 2001.
[2] *Journal of System Safety*, Vol. 44, No. 2, March-April, 2008.
[3] Acronyms depending on the image of complexity that those doing the naming desire to communicate.
[4] See *The Firebird Forum*, Vol. 11, No. 1, "Lucky Barriers."
[5] See NTSB Report ID CHI06MA121, available at www.ntsb.gov/ntsb/brief.asp?ev_id=20060509X00531&key=1.

Figure 1 — Predator UAV.

switching UAS operational control from the PPO-1 (pilot's primary) to PPO-2 (payload operator's primary) console. The functions of each console's condition lever depend on the role assigned to its console. It is critical that the levers' positions be "matched" prior to switching control. The pilot/operator stated that he was "in a hurry" to regain control. He did not use the checklist, and did not "match" the condition levers' positions. He didn't notice that the lever to which he transferred control was in the "fuel shutoff" position. Upon switching, the fuel supply to the Predator's engine shut off, as it should have. Even then, the pilot/operator did not analyze the situation correctly. By the time additional personnel were called in to take control, the Predator had descended below line-of-sight radio control capability, and continued its unpowered descent until crashing.

System safety lessons from past errors should have been applied during the development of the Predator systems' and its operating procedures' design, and during the training of its operating personnel. An early applicable lesson occurred on Oct. 30, 1935, when Boeing's Model 299, prototype of the WWII B-17 "Flying Fortress," crashed on takeoff during a demonstration flight at Wright Field in Dayton, Ohio. Investigators determined that the control surface locks had not been released by the crew. Boeing pilots' analyses concluded that the airplane was "too complex" for operational procedures to be entrusted to memory. They developed aviation's first four checklists: takeoff, flight, before landing, and after landing, in the aftermath of the crash.[6]

> "Learning from past experience is fundamental both to developing safe and efficient new systems, and continuously improving the performance of existing systems. Those lessons are often expensive."

Before lessons can be learned, they must be taught. Most of us learned the utility of lockouts in system safety's pre-school. They're used effectively in elevators, automatic doors and nuclear weapons. They have been used in cars for decades to prevent shifting out of "Park" without applying the brake. A lockout could have prevented shifting UAS control from one console to the other unless their condition levers' positions matched. A lockout would have been the last, lucky chance to overcome the uncritical assumptions of those overseeing Predator's transition from a wealthy military weapons system to a comparatively indigent civilian workhorse.

Robustly funded maintenance and adequate spares support are lessons that have been learned by the manned aircraft community as essential contributors to safe operations. Prior to the accident flight, the "crew" was unable to establish communication between the PPO-1 console and the aircraft. An avionics technician swapped main processor cards between the PPO-1 and PPO-2 consoles, which appeared to mitigate the problem. After the accident, maintenance personnel reported that parts swap-

[6] See www.atchistory.org/History/checklst.htm.

ping had become commonplace because "…there were very few spare parts purchased with the UAS…."[7] A log at the ground control station revealed 16 "lockups" in the four-and-a-half months prior to the accident, yet no data were recorded to explain the deficiencies.[8] The lesson of Normalizing Deviance, or "drift into failure,"[9] was bought dearly in NASA's losses of the space shuttles *Challenger* and *Columbia*.[10] It is equally applicable to UAV/UAS programs.

> "Competent oversight of government aviation operations is a necessity, especially now that increasing numbers of local agencies each want their own 'eye-in-the-sky.'"

Neither the operating agency nor its contractors had specified minimum essential equipment required to be operational for safe flight, another fundamental safety requirement in manned aviation.[11] Nor had they documented a maintenance program specifying how maintenance tasks were to be performed, especially after repeated similar anomalies. No formal procedures stipulated how, when or by whom UA maintenance was to be inspected, or released for return to flight after maintenance — still another basic aviation tenet. These and other safety criteria have long been specifically required for manned aircraft. What ignorance lay behind the belief that similar concerns weren't needed for UAV/UASs — if they were considered at all?

It is apparent from the NTSB investigation report[12] that neither the UA's manufacturer nor its operator, nor the FAA, gave credible consideration to the transition from their military applications. Military UAs operate in aeronautical environments sparsely populated by other aircraft. In civilian roles, they must operate in, or adjacent to, areas dense with air traffic. A significant example cited by the NTSB relates to the Predator's electrical system functional priorities:

"…after the console lockup and transfer of control to PPO-2, the engine shut down and the UA functionality degraded quickly as it began to operate on battery power. On battery power, the UA automatically shuts down some aircraft systems to conserve electrical power, including the satellite communication system and the transponder.

"The transponder is vitally important to ATC[13] because it provides an enhanced electronic signature, an identification code, and altitude information that are presented on the controller's radar display. … Without an operational transponder, the secondary radar return, identification, and altitude information are not available to ATC. Thus, when the transponder stopped working about 0333, ATC lost secondary radar contact with the UA and was no longer provided altitude information. About 0339, ATC lost primary radar contact with the UA and could no longer provide separation from other aircraft as the UA descended below the TFR-protected airspace.[14]"[15]

FAA regulatory criteria for airplane electrical systems specify that electrical power for essential load equipment "…can be maintained within the limits for which the equipment is designed during any probable operating conditions."[16] Transport category airplane design criteria are more specific on load-shedding in emergencies: Priorities are assigned to ensure the greatest longevity for

---

[7] NTSB Report, *op. cit.*
[8] A "lockup" is any malfunction that causes the ground-control station PPO screens to "freeze."
[9] Dekker, Sidney. *Ten Questions About Human Error.* New York, Lawrence Erlbaum, 2005, Chapter 2.
[10] See Vaughan, Diane, *The Challenger Launch Decision; Risky Technology, Culture and Deviance at NASA*. University of Chicago Press, 1996, for a discussion of how normalizing deviance led to the loss of space shuttle *Challenger* in 1986.
[11] The FAA and manufacturers specify minimum equipment lists for all aircraft.
[12] See footnote 5.
[13] FAA's Air Traffic Control.
[14] The FAA had issued a Temporary Flight Restriction blocking altitudes between 14,000 feet and 16,000 feet for UA operations, and warning other aircraft to avoid those altitudes between certain hours.
[15] NTSB Safety Recommendation Letter dated October 24, 2007, to FAA Acting Administrator Robert Sturgell, pp. 2-3.
[16] FAR ¶23.1351(a)(5)(iii) – for commuter category airplanes, which are characteristically equivalent to the Predator, even in the absence of passengers.

the systems most essential for safe operation in the ATC environment.[17]

The NTSB Safety Recommendation letter states:

"All public-use aircraft operations (both manned and unmanned) are exempt from certain aviation safety regulations, and, therefore, operators supervise their own flight operations without oversight from the FAA. For example, Federal aviation regulations pertaining to flight crew training and licensing, aircraft certification, and continuing airworthiness (maintenance) are not applicable to public operations. As a result, the CBP was solely responsible for overseeing the safety of its Predator B operations."[18]

In our opinion, the NTSB erred by choosing to ignore the FAA election not to intrude into the "public aircraft" issue. We believe that to be a serious misjudgment that will lead to increased public risk. Competent oversight of government aviation operations is a necessity, especially now that increasing numbers of local agencies each want their own "eye-in-the-sky."

On the same page of its recommendation letter in which it exonerates the FAA from inaction, the NTSB states: "UAS operation in the NAS[19] is an evolving activity. The FAA informed Safety Board Staff that public-use UAS operations have more than doubled over the past year." Yet none of the five NTSB recommendations cites the FAA's failure to anticipate potential conflicts between public-use UAs and civilian aircraft operating within the NAS, and to take pro-action to assure compatibility between the vehicles, their operators and their operations. In our opinion, from this and other recent unplanned UA events and from predicted future "public aircraft" UA initiatives, the qualifications and fitness of all varieties and sizes of government agencies to manage aviation operations must be critically analyzed and tested before being certified to operate within the NAS.

There is nothing less at stake than the safety of the population underlying the National Airspace System.

---

[17] FAR Part 25.

[18] NTSB Safety Recommendation Letter to FAA, *op. cit.*, p. 7.

[19] National Airspace System.