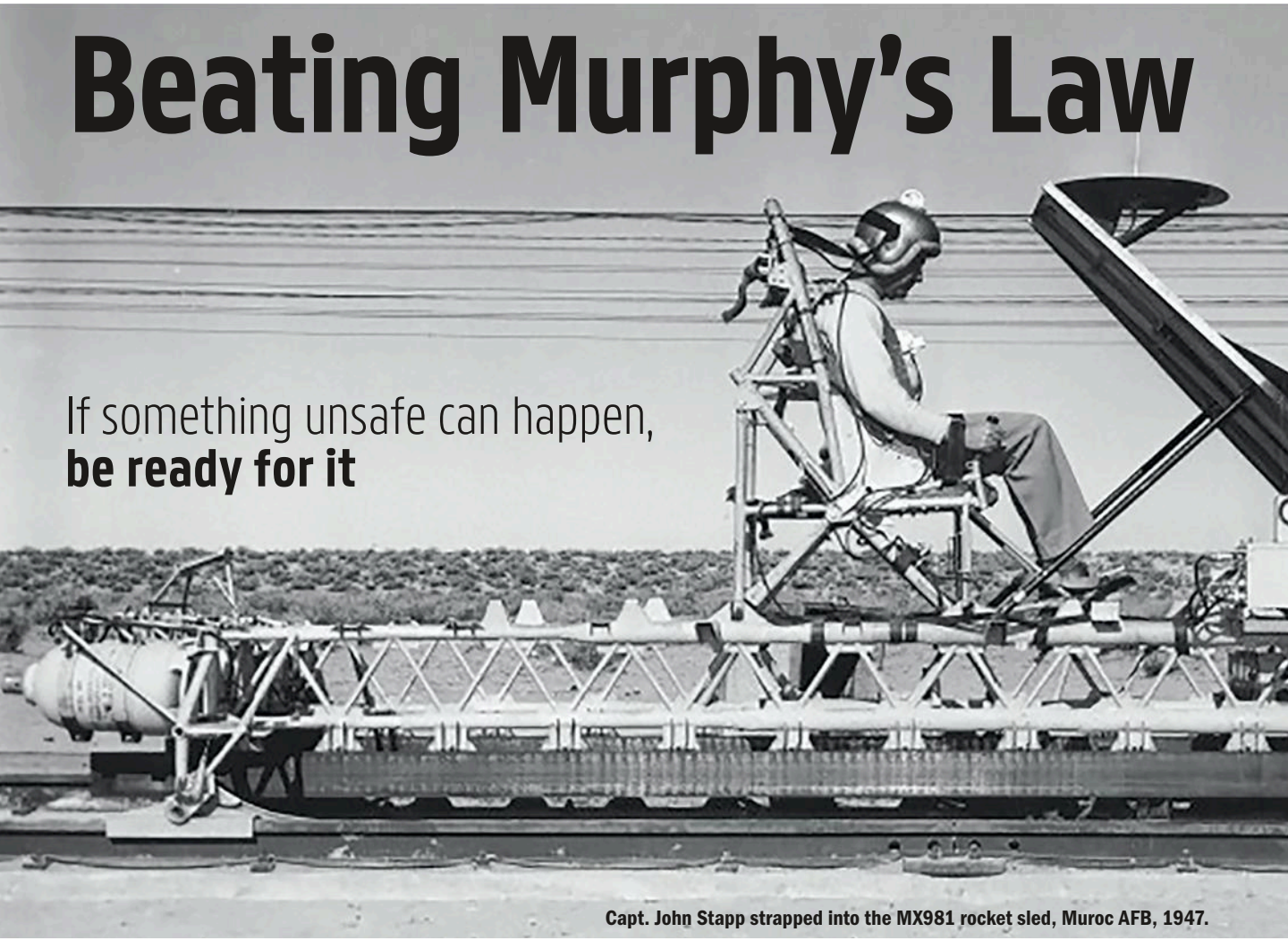
Beating Murphy's Law



If something unsafe can happen, **be ready for it**

Capt. John Stapp strapped into the MX981 rocket sled, Muroc AFB, 1947.

BY **JAMES ALBRIGHT** james@code7700.com

The patron saint of industrial engineering is U.S. Air Force Capt. Edward Murphy, to whom is credited the rather dubious saying, "Anything that can go wrong, will go wrong." Besides being a misquote, the phrase's negative implications may encourage us to just give up on making things better.

These "will go wrong" moments quite often result in tragedy, followed by hand wringing and a few lessons learned to prevent recurrence. There has to be a better way.

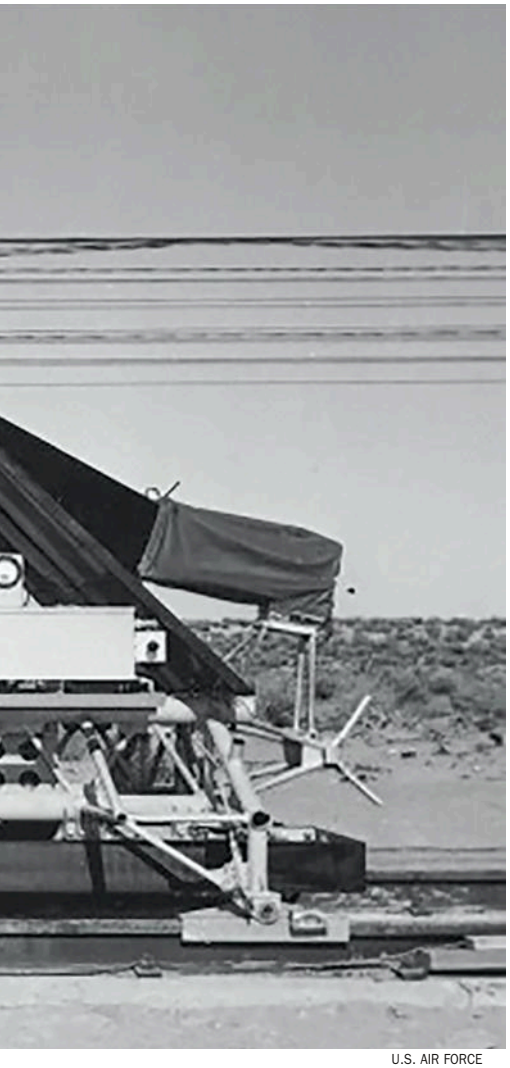
Examining the origins of the phrase reveals valuable lessons for aviators trying to keep the act of flying from Point A to Point B as safe as humanly possible. The engineering behind the saying helps explain the history of Murphy's Law, and that history can help us understand how to apply its lessons to flight.

Industrial engineering encompasses systems, safety and reliability considerations and can be summed up as the optimization of complex processes, systems or organizations. Industrial engineers aim to eliminate the waste of time, money, material, person-hours, machine time, energy and other resources that do not generate value. Reliability engineering furthers this aim by assuring critical systems and processes behave as intended, even when subcomponents fail. The common understanding of Murphy's Law would seem to have little to do with safety engineering; if things are destined to go wrong, what is the point of trying to stop it? Murphy's Law's true history, however, does have a lesson to teach.

The Provenance of Capt. Murphy's Law

The dawn of the jet age was ushered in by military aviation and the early test programs pushing the envelope to get aircraft to go higher, faster and farther. Of course, there was a large amount of danger involved and crashes were inevitable. Military cockpits were designed with the idea that the human occupant could not tolerate more than 18 Gs of force. (A "G" is the force of gravity acting on a body at sea level.) Evidence from World War II air crashes suggested this number was too low, but no research existed to reveal the actual number.

In 1947, the U.S. Air Force's Aero Medical Lab at Wright Field, Ohio, contracted with the Northrup Aircraft Co. to build a rocket-powered sled called the "Gee Whiz" to hurdle a test dummy down a track at over 200 mph and then



U.S. AIR FORCE

brake to a sudden stop. The first sled was replaced by an even more powerful version, known as "The Sonic Wind."

The program's chief researcher, Air Force Capt. John Stapp, a medical doctor, supervised much of the testing at Muroc, now known as Edwards Air Force Base. Several runs by the test dummy were followed with chimpanzee "pilots." G-forces were figured mathematically by dividing the velocity change by the time needed to come to a stop. The program needed a quicker way to figure G-forces. And that's where Capt. Murphy entered the picture.

Murphy was an Air Force engineer who had developed strain gauge transducers capable of measuring G-forces. The Aero Medical Lab requested transducers capable of measuring G-forces up to, and perhaps beyond, recently demonstrated deceleration values. Murphy gave his technicians the instructions needed to wire several transducers to do the job.

After the first rocket sled run with the transducers, Stapp was surprised to see they registered 0 Gs, or no deceleration at all. An examination of the transducers revealed they could have been assembled in two different ways. Wired correctly, each transducer reported a portion of the total forces, which were added to produce an accurate result. Wired incorrectly, each transducer effectively canceled each other's readings. Stapp's team believed Murphy's schematic was unclear on how each transducer was to be wired and claimed that Murphy quickly blamed his technician back at Wright, saying, "If that guy has any way of making a mistake, he will."

With his transducers wired correctly, Murphy returned to Wright as Stapp and his team continued the rocket tests. Stapp couldn't resist the chance to experience the sled's full speed and sudden deceleration, soon doubling the previously believed G-limit. During his 29th and final rocket sled run, Stapp reached a speed of 632 mph, thus becoming the fastest man on earth. He then experienced a deceleration of 46.2 Gs. As one wit put it, it was "the most any human being had ever willingly experienced."

Following that, Stapp became a media sensation and was never shy about answering press questions. At one point, a reporter asked how it was no one had been severely injured in any of the tests. Stapp replied it was because, "we do all our work in consideration of Murphy's Law." That is, anything that can go wrong, will.

NASA

Capt. John Stapp during a high-G force test.

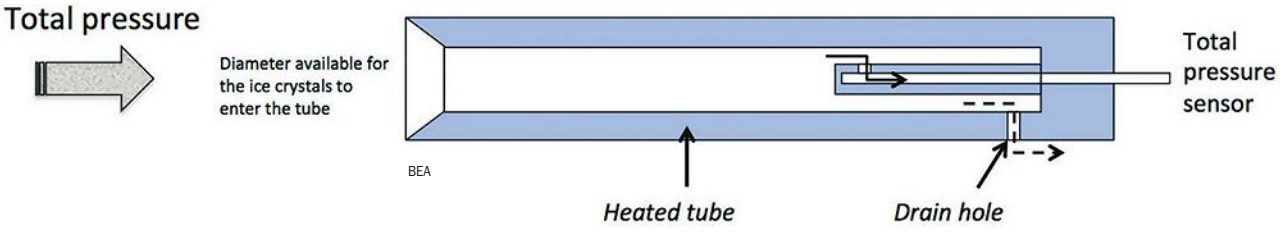
It appears that the research staff came up with the rule from Murphy's original statement and named it after him, perhaps a bit maliciously. They believed Murphy had violated several cardinal rules of reliability engineering: He didn't verify the gauges worked correctly before shipment; he didn't test them; and his written assembly instructions were ambiguous. Their version, however, was written with a positive spin: "If it can happen, it will happen."

It should come as no surprise that the aerospace industry is responsible for Murphy's Law; it is the heart of reliability engineering. If this part fails, how does the entire system react? What are the single points of failure? Which systems need redundancy?

Reliability Engineering and Airplanes

The need for redundancy in pitot-static systems is unquestioned and aircraft designers take great care to ensure a failure of one system cannot corrupt the other. A failure of any one system cannot, by design, rob pilots of reliable airspeed measurement. We take the issue even further with a third system, so as to provide a "tie breaker" between the two primary systems. We are so worried about having this final backup, we do not allow the flight data software that massages primary data anywhere near the standby hardware. But what happens when all three systems stop working?

On June 1, 2009, an Airbus A330 operating as Air France Flight 447 from Rio de Janeiro to Paris encountered ice crystals in sufficient quantity to block all three pitot-static total pressure sensors. While such an occurrence is rare,



Air France 447 pitot probe diagram (Bureau d'Enquêtes et d'Analyses, BEA)

experience has shown the total pressure sensor heat will limit the duration of any data loss to around 1 or 2 min. in even very severe conditions.

Loss of all three inputs, however, may have two consequences that can take Airbus pilots by surprise. First, the autopilot may disengage, requiring pilots to hand-fly the aircraft at high altitudes, something they rarely do. Second, the aircraft's fly-by-wire (FBW) computer will revert from "normal law" to "alternate law," with fewer safeguards. In combination, both factors conspired under Murphy's Law to overwhelm Flight 447's pilots.

Not many pilots have recent experience hand-flying large aircraft at high altitudes, where each control input needs to be made with a level of finesse not needed down in the traffic pattern. Where a few degrees of pitch change while on final approach can destabilize an aircraft's speed and glide path, at altitude the same magnitude of stick movement can lead to a stall.

The Flight 447 pilot flying (PF) faced with suddenly having to hand-fly the massive Airbus at 35,000 ft. was an "ab initio" hire. Air France employed him three years after he earned his private pilot's license and within a year put him at the controls of an Airbus. The captain was in the cabin for a rest period, as was common with these "long haul" international flights. The pilot not flying (PNF) in the other seat was also a low-time copilot.

Both of these low-timers were also faced with what may have seemed to be a subtle difference in the way their aircraft normally flew and the way it would fly under this extraordinary circumstance. Most (if not all) of their airborne Airbus experience will have been under what the manufacturer calls "normal law." While in flight, other than when in the landing flare, pilot sidestick inputs are interpreted as "demands" that are filtered by computers. Theoretically, these computers will prevent the aircraft from stalling or overbanking under normal law.

However, once the three pitot-static total pressure sensors were blocked, the computers could no longer fly the aircraft under normal law and reverted to "alternate law." In this new mode, high angle of attack protection that prevents the stall is replaced by conventional stall warning systems. At that point the aircraft is very capable of an aerodynamic stall.

This normally reliable computer was designed to fly the aircraft at altitude, so the pilots rarely experienced having to hand-fly in the thin air at 35,000 ft. The aircraft's avionics normally prevented its pilots from stalling the aircraft. But the inexperienced pilot flying the aircraft instinctively pulled back on his control stick and the aircraft started to climb. In the next 10 sec. he increased the pitch from about 5 to 11 deg. At least one of the airspeed indicators came back within a minute but the pitch continued to rise. At one point the PNF took control of the aircraft without making a callout, then the PF retook control, again without a callout.

The captain returned to the cockpit 1 min., 37 sec. after the initial autopilot disconnect. At this point the aircraft's pitch was over 16 deg. nose up and the vertical velocity was in excess of 10,000 fpm down. The flight data recorder stopped 4 min., 23 sec. after autopilot disconnect. The vertical velocity was 10,912 fpm down, the ground speed was 107 kt., and the pitch was 16.2 deg. nose up.

There is no doubt the two pilots were dealing with a situation they were ill-prepared to handle. There can also be no doubt the captain was presented with a catastrophic situation with very little time to assess and recover. But we can also say the record of the Airbus points to an airplane that is quite safe, and yet is occasionally unreliable in the worst possible ways. One can debate the aircraft's design, but there are things pilots can do to accommodate an airplane that can at times be unpredictable and unforgiving.

Industrial Engineering and Pilots

While a reliability engineer may focus on mechanical systems and their impact on safety, an industrial engineer takes this one step further by looking at the people involved with the processes. Saying that mechanical causes of accidents have dramatically decreased while pilot errors have not is not only trite but wrong. (Both have decreased dramatically, the former more than the latter.) But an industrial engineering examination of the human in aviation accidents can help us improve even more.

On Sept. 19, 2008, a Learjet 60, N999LJ, was destroyed after a high-speed takeoff abort at Columbia Metropolitan Airport (KCAE), South Carolina. The NTSB report cites two probable causes: severely underinflated tires leading to multiple tire failures during the takeoff roll, and the captain's decision to reject the takeoff above V1.

Learjet 60 N999LJ wreckage, Sept., 19, 2008.

Either problem in isolation should not have resulted in the loss of the airplane and the death of six of its eight occupants. Even in combination, the resulting tire failures should have been survivable.

But, as Murphy's Law would have it, the loss of tires and the high-speed abort were more complicated than the usual simulated failures seen in most training events.

Learjet procedure called for checking the tires before the first flight of each day or every 10 days they are not in use. Furthermore, the maintenance manual stipulated that a tire should be replaced if its pressure falls below 15% of its loaded pressure. However, the flight department's director of maintenance was unaware of

these requirements and the tires had not been checked in three weeks. While the tires were relatively new, post-crash analysis revealed all four main gear tires had significant sidewall damage. This damage was consistent with over-deflection and flexing fatigue caused by taxi-cycle operations while underinflated by about 36%. The first tire appears to have failed about 2 sec. after the first officer called, "Vee-one."

The pilots then heard a loud rumbling noise. Within a second of that, the first officer said, "Go." The captain's next words were unintelligible. The first officer repeated, "Go, go, go." The captain then asked, "Go?" At this point the aircraft's speed reached a peak of 144 kt. (8 kt. above V1). They had traveled more than 2,500 ft. down the runway and had about 6,100 ft. remaining.

The aircraft initially veered to the right (the side of the first blown tire), but the captain was able to correct back toward the runway's centerline. The captain momentarily reduced engine thrust for about 1 sec., then increased it for another second, at which time the first officer said, "No? Ar-right." The captain then reduced engine thrust again, applied wheel brakes and activated the thrust reversers. The reversers fully deployed and the aircraft appeared to decelerate. By this point, all four main landing gear tires had failed.

Tire fragments resulted in substantial collateral damage. The wheel brakes were compromised due to hydraulic system damage. A main landing gear speed sensor and squat switch appear to have sustained damage from the tires, changing the system's logic from the "ground mode" needed for nosewheel steering and thrust reversers, to the "air mode" where those systems were deactivated. The thrust reversers, as a result, stowed. But the engines remained at high power settings, resulting in forward thrust, even with the throttle reverse levers pulled aft.

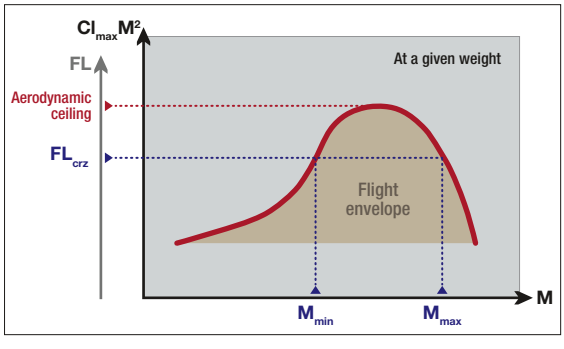
The aircraft was about 2,500 ft. from the end of the runway at a ground speed of 123 kt. when the uncommanded forward thrust began. The aircraft accelerated for several seconds before the first officer recognized the problem and shut down the engines. The aircraft departed the end of the runway in excess of 100 kt.

The captain and the first officer were trained that rejecting a takeoff is acceptable for any anomaly occurring before the airplane reaches 80 kt. and that for speeds between 80 kt. and V1, the takeoff could be rejected for major anomalies, such as catastrophic failure, engine fire, engine failure, thrust reverser deployment or loss of directional control. Their training and standard operating procedures indicated that, because of the high risk of runway overrun and other dangers, rejecting a takeoff at speeds greater than V1 should be performed only when airplane control is seriously in doubt. It appears the crew could have successfully rejected the takeoff had the thrust reversers remained fully deployed or not resulted in forward thrust once stowed. The effect of the disabled squat switch on the thrust reversers was unknown, another consequence of Murphy's Law.

Repealing Murphy's Law in Your Cockpit

Framing Murphy's Law as it is popularly known — "If anything can go wrong, it will go wrong" — might be useful as a way of analyzing systems failures. But stated negatively, the law may not be as helpful as needed when trying to devise methods of accident prevention. Case in point: the impact of pitot-static probe icing on the Airbus A330.

We often cover systems failures in classrooms and simulators as exercises in troubleshooting the items we've lost and learning to make do with backups. In the case of pitot-static systems, this usually involves reverting to a standby instrument. We can modernize these procedures by using Global Positioning Satellite (GPS) signals for altitude and a ground speed that can be converted to airspeed. Our focus, it seems, is on fixing the problem itself. "Check the pitot heat circuit breaker." "Oh well, we'll make do with the standby." But adding the startle factor to the challenge of hand-flying an airplane near the top of its flight envelope complicates things greatly.



An example aircraft's flight envelope at high altitude (Bureau d'Enquêtes et d'Analyses, BEA).

Turning Murphy's Law back to its origins — "If it can happen, it will happen" — helps refocus our attention to dealing with the issue positively. You could very well lose all three pitot-static systems, for example, now what? In the case of the Air France Airbus, this means you will be without the normally engaged autopilot. Even an airplane with a surplus of thrust in normal flight conditions will find itself near what some call the "coffin corner" but is more accurately called the top of an airplane's aerodynamic flight envelope.

You don't need to be an aeronautical engineer to fly high-performance airplanes, but a little knowledge of aerodynamics will make you a better pilot. An aircraft's flight envelope can be drawn on a graph placing altitude on one axis and airspeed on another. Some manufacturers publish these under different names and choose one axis or another for the variables. But however presented or titled, the graph encloses the flight regime; straying from the inside of the envelope means your airplane ceases to fly under your control. This is critically important when flying at high altitudes because the envelope narrows as you climb. The difference between minimum and maximum speeds narrows and you have less of a margin between aerodynamic stall and overspeed. Changes in pitch, therefore, must be smaller at high altitudes than at lower.

Both pilots at the controls of Air France 447 appeared to have been unaware of this characteristic of high-altitude flight when the pitot-static systems iced over. The pitch angle of the aircraft just a few seconds after losing airspeed indications was inappropriate for high altitude, regardless of the thrust setting. The lesson learned translates across all aircraft types: You should know a safe pitch angle for your aircraft for all regimes of flight with the engines at maximum thrust, including one engine out for multiengine aircraft.

A pilot should be able to answer this question instinctively: What pitch will keep my airplane climbing safely with all engines at full thrust, even with one engine out, at high altitude or in the traffic pattern? In the case of many high-powered business jets, such as a

Checking the tire pressure of a modern aircraft tire.

Gulfstream G550, the answer is 3 deg. nose up at high altitudes, 15 deg. nose up in the traffic pattern. Armed with this knowledge, you can survive even the worst pitot-system failures long enough to keep the airplane flying so you can sort out the problem later.

Another problem with framing Murphy's Law in its negative terms is we can resign ourselves that there is nothing to be done. If something wrong is going to happen, then we'll just have to deal with it when it happens. But if taken positively, we know that if it can happen, it will happen; so we must prepare ourselves. Take, for example, the mundane task of checking aircraft tire pressures.

Any Airframe and Powerplant (A&P) mechanic should be schooled on the effects of low tire pressures on the integrity of an aircraft tire. The Goodyear "Aircraft Tire Care & Maintenance" manual, for example, sets out several cardinal rules:

- Tire pressures must be checked when tires are cool, at ambient temperature.
- Tire pressures increase 4% under load.
- Tire pressures decrease after mounting due to the stretching caused by inflation (which increases the tire's volume) and must be rechecked after 12 hr.
- If tire pressure drops more than 5% in 24 hr., there may be a leak and troubleshooting is required.
- A tire found to be inflated between 90 and 95% of loaded pressure should be inspected for signs of leakage.
- A tire found to be inflated to less than 90% of loaded pressure should be removed from the aircraft and returned to the manufacturer for inspection.

Of course, these are just one manufacturer's rules and mechanics should refer to guidelines for their specific make and model of tire. In the case of the Goodyear Flight Eagle tires installed on Learjet N999LJ, a daily tire pressure loss of 2.2% had been documented. The aircraft's maintenance manual required the pressure be checked before the first flight of each day. Mechanics, of course, should be keenly aware of aircraft specific tire pressure measuring requirements. But if the airplane is on the road, shouldn't the pilot also be aware?

As stated in the NTSB's N999LJ accident report, there is an issue regarding pilots checking tires, citing the FAA's Feb. 26, 2009, response to Learjet regarding the Learjet 60. It noted that in the letter, the FAA stated that "checking the tires on a Learjet 60 is preventive maintenance, which pilots would not be permitted to do as part of a preflight check. However, the FAA further explained that a pilot flying a Learjet 60 under 14 CFR Part 91 may perform tire pressure checks but that a pilot flying a Learjet 60 under 14 CFR Part 135 may not."

In keeping with Murphy's Law, I've tracked tire pressure loss during extended trips for many of the aircraft I've flown. My current aircraft will lose less than a half psi every day on a trip, even when flying multiple legs each day. Since we normally depart our home base with fully serviced tires at 198 psi, we can fly for 19 days without breaching the 5% threshold. So, with an abundance of caution, we plan on hiring an A&P if we are away for more than a week. Since we operate under Part 91, we've trained each pilot how to measure tire pressures. (There is a specific technique to avoid losing too much pressure during the check.) But we do not train our pilots on servicing procedures, hence the need to hire contract mechanics when on the road.

Mechanics and pilots alike may not be tire experts and may need a refresher on what their aircraft and tire manufacturers require be done on a regular basis. We can extend this thought to just about every component on the aircraft. The learning never stops.

A third problem with applying Murphy's Law negatively impacts pilot training for these unusual circumstances. If you believe a tire failure during takeoff is inevitable, you train to deal with the problem specifically until your confidence level allows you to move on to the next potential problem. Combining multiple failures in the simulator can be seen as "bad form" or instructor sadism of a sort. But sometimes one failure can beget another. Moreover, sometimes these failures can bring on unforeseen consequences.

In the case of N999LJ, the captain's decision to reject the takeoff above V1 can be understood in the context of the aircraft and the runway. They had consumed less than half of the available runway and, with a good airplane, could have easily stopped. Years of experiencing high-speed simulator aborts on far shorter runways may have reinforced the captain's idea that aborting with over 6,000 ft. of runway remaining was a reasonable option. What was missing from her training was an understanding of how one failure can domino into others.

For example, we learn in training that a blown tire can cause an engine fire if rubber fragments find their way into intakes. But how many of us consider that a blown tire can take out a squat switch that can turn reverse thrust into forward thrust? The captain can be forgiven for not knowing this; it was apparently a surprise to Learjet as well. But understanding just how complicated a successful high-speed abort can be may have been all she needed to reinforce the need to go airborne, regroup, and then try landing after burning off some fuel, with full flaps, a lower speed, with more of the runway remaining and with ample time to marshal resources and plan the difficult task ahead. The broader lesson is that modern aircraft have so many interconnected systems that it can be foolhardy to assume you've considered every angle before making a hasty decision. Sometimes you need an extra margin of error for when "anything can happen" really does.

An Aviator's Corollary to Murphy's Law

We have a lot to gain from Air Force Capts. John Stapp and Edward Murphy. Our culture is filled with stories about Murphy's Law and corollaries designed with humor in mind. But we can offer our own version of the law that is designed to frame our efforts to increase our level of safety:

"If something unsafe can happen, it is up to us to be ready for it in case it does happen."

Both case studies had tragic outcomes that could have been prevented. But they only provide us with specific lessons for a couple of specific situations. A safety-conscious engineer will extrapolate from the specific to the general when possible. The real lesson of Murphy's Law in aviation is that we must anticipate when "anything can happen" and think through the adverse effects. In that way we will be better prepared to prevent the tragic outcomes and provide positive lessons for all who follow us. **BCA**