Safety and Mission Assurance: Independent Yet Engaged

BY BRYAN O'CONNOR

When I was a test pilot at the Naval Air Test Center, I worked closely with the engineers designing the first American version of the British Harrier, a vertical/short takeoff and landing (V/STOL) fighter, for two years before the first flight of the prototype. The main aim of my involvement, based on my own cockpit experience, was to keep the pilot's workload at a manageable level, especially during takeoff and landing. I worked with the engineers on the design of the head-up display, which projects vital information into the pilot's field of view, and the design of the throttle and stick to minimize circumstances that required the pilot to let go of them.

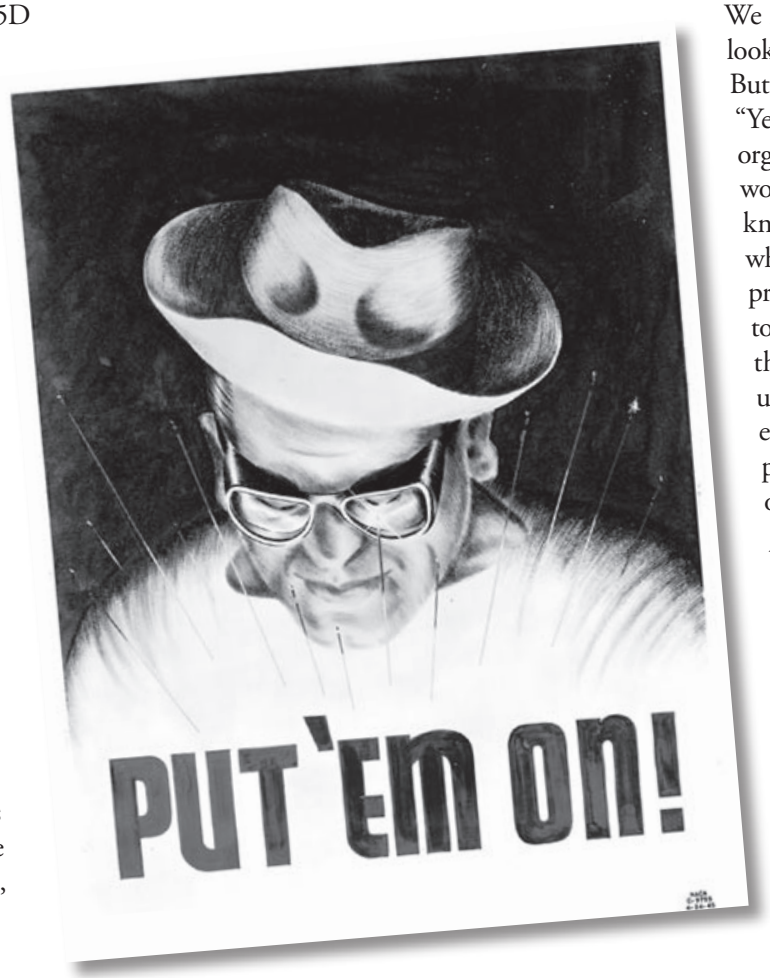
LIKE GOOD TEST PILOTS, MEMBERS OF THE SAFETY AND MISSION ASSURANCE COMMUNITY SPEND A LOT OF TIME THINKING ABOUT "WHAT IF" SITUATIONS (WHAT IF THE ENGINE QUITS? WHAT IF ONE OR ANOTHER SYSTEM FAILS?), TRYING TO REDUCE THE SET OF POSSIBLE PROBLEMS THAT NO ONE HAS THOUGHT ABOUT YET AND TRYING TO MAKE SURE THERE IS ALWAYS A WAY OUT IF SOMETHING GOES WRONG.

As NASA's Chief Safety and Mission Assurance Officer, I apply and promote a lot of the lessons I learned then as a test pilot and later as a Space Shuttle pilot and director of the Space Shuttle program. One of them is the value of drawing on different perspectives and types of expertise early on, as with the development of the American version of the Harrier. We have a history in the Agency of not involving the safety and mission assurance (SMA) community during the entire project life cycle. No one disagrees with the idea, but they tend to think of SMA as the "back-end folks." An important element of the new 7120.5D practices and policies is that they give safety and mission assurance an explicit, active role from the beginning of every project.

"Can Do" vs. Caution

Like good test pilots, members of the safety and mission assurance community spend a lot of time thinking about "what if" situations (what if the engine quits? what if one or another system fails?), trying to reduce the set of possible problems that no one has thought about yet and trying to make sure there is always a way out if something goes wrong. NASA's culture is a famously optimistic, problem-solving, and goal-oriented one; the SMA community is supposed to look for potential problems and question engineering and operational assumptions. In so doing, its members can sometimes be seen as naysayers. Over time, this perception can wear down a motivated SMA engineer. I have seen people burned out by the stress of this negative role.

I think part of the responsibility for resolving the tension between can-do optimism versus problem-seeking pessimism lies with the SMA team itself. "No, because" is a legitimate starting point for safety and mission assurance. We need to take a realistic, unbiased look at barriers and assumptions. But "no" shouldn't be the last word. "Yes, if" is an important goal in an organization like NASA. In other words, we need to be not only knowledgeable enough to know when there is a safety or reliability problem but persistent enough to help the larger team define the solutions to the problems we uncover. SMA engineers must be engaged from the beginning as part of the design team, figuring out how to make things work, not just explaining why they might not and then leaving the scene.



A tension also exists between being fully and actively engaged in projects from the beginning, as safety and mission assurance will be under 7120.5D, while at the same time maintaining the independence of perspective and action we need to do our work well. Our job is to

challenge and test the assumptions of design engineers, providing the checks and balances needed to ensure safe, successful missions. So we need to look at project plans, analysis results, design options, and other project elements with independent eyes and ensure design engineers are not drinking their own bathwater. We at NASA can sometimes get carried away by an overabundance of confidence in ourselves, but I think of the advice Tommy Holloway gave me while we were working on the space station together: "Remember, you're not as smart as you think you are." No matter how good you are, you can't think of everything, foresee every problem, or recognize all the potential weaknesses in your assumptions, so reach out for the independent look.

I remember a clear example of skilled professionals being led astray by an excessive belief in their competence in the late seventies. We arranged training dogfights between a dozen navy F-14 pilots and an equal number of marines flying the AV-8A, the first American version of the British V/STOL aircraft. The first F-14 pilot to face a Harrier unswept his aircraft's wing to lower its speed and increase maneuverability, but he couldn't match the Harrier, which had vectored thrust capability and could be almost stationary by comparison. The Harrier easily dropped behind the F-14 and "destroyed" it. Although the second and third F-14 pilots saw what happened, they tried the very same thing, with the same result: they also lost their dogfights. Why didn't they learn? They assumed they were better pilots than the ones who had failed and ignored the possibility that the tactic itself was faulty.

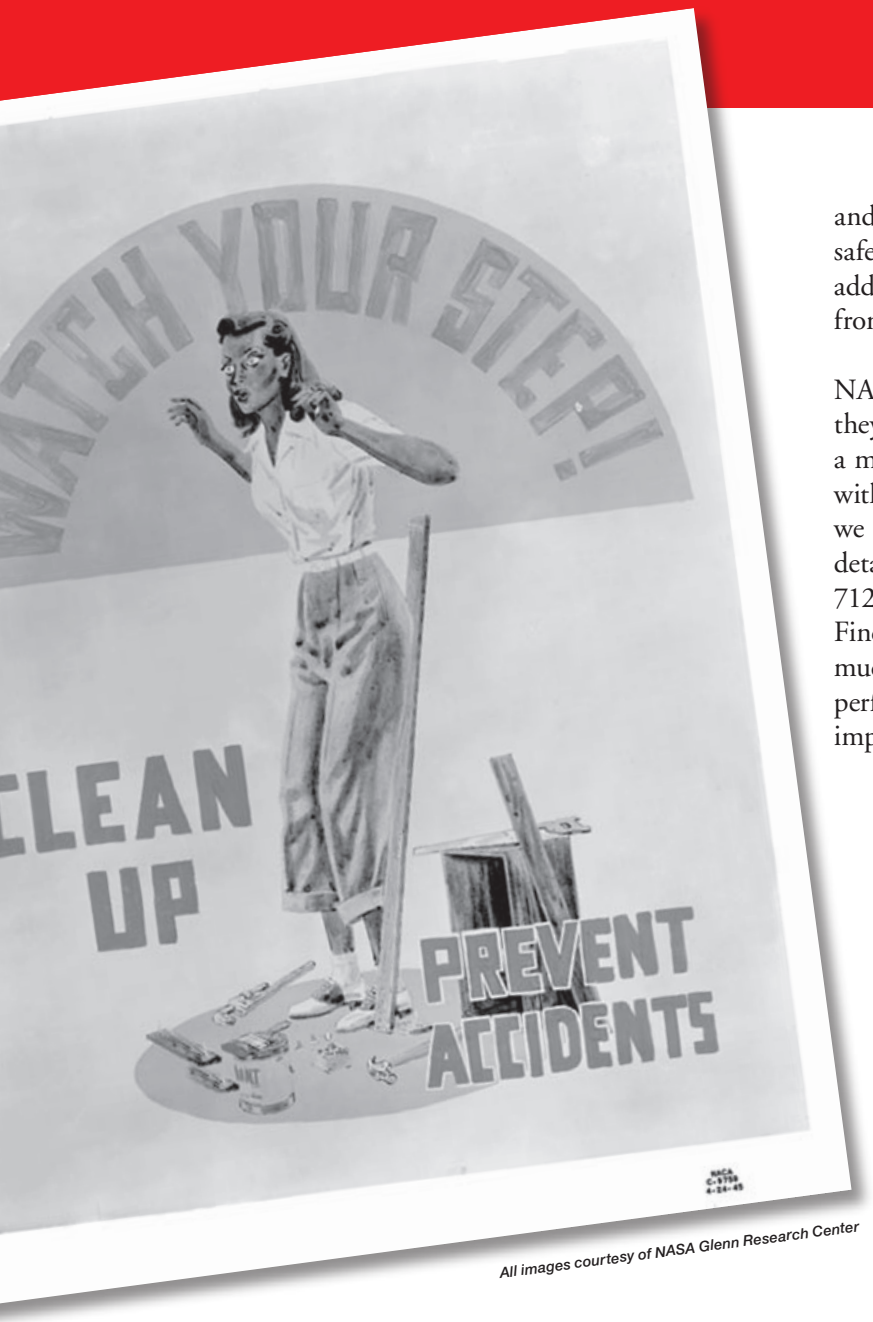
Learning from Mishaps

A similar overconfidence factor may get in the way of NASA's ability to learn from mistakes. The Agency is required to investigate all occurrences of damage and injury. Investigating close calls is encouraged but not required, so they are often ignored. In the past, when we experienced a close call, we tended to focus on the one thing that saved us (and our own skill at avoiding disaster) rather than the three that almost killed us. But close calls are a gift—an opportunity to learn important lessons without scraping bodies from the floor. We are doing better, though. I recently sat in on a class B–level mishap investigation final report briefing, not for a class B mishap, but for a close call. A young worker was knocked down but not injured when he cut through a "hot" electrical wire that had 22,000 volts of electricity running through it. The focus of the investigation was not on what saved his life—the fact that the ground was dry, that he was wearing gloves, that he was young enough to tolerate the jolt—but on what caused the accident—bad procedures, out-of-date drawings, inadequate supervision. The center director, through the mishap board, made the best of this "gift" and allowed the center to take steps toward preventing similar, possibly fatal mishaps in the future.

Safety and Mission Assurance and 7120.5D

The safety and mission assurance community has been deeply involved in the process of rewriting 7120.5D, with some members spending almost all their time on the work. Their contribution helps ensure that SMA, one of the three legs of the check-and-balance "milk stool" that supports programs and projects, has as well-defined a role as program management

SMA ENGINEERS MUST BE ENGAGED FROM THE BEGINNING AS PART OF THE DESIGN TEAM, FIGURING OUT HOW TO MAKE THINGS WORK, NOT JUST EXPLAINING WHY THEY MIGHT NOT AND THEN LEAVING THE SCENE.



All images courtesy of NASA Glenn Research Center

and engineering. The new processes make clear that system safety, reliability, maintainability, and quality assurance are not add-ons that come toward the end of projects but are integral from the beginning.

The Columbia Accident Investigation Board concluded that NASA lacked the discipline needed to avoid serious accidents; they pointed to navy submarine requirements and discipline as a model. 7120.5D takes a step toward the necessary discipline without mandating processes that are too rigid. One of the ways we have tried to keep from getting bogged down in excessive detail is to look for the optimal mix of processes spelled out in 7120.5D and references to other policy and process documents. Finding the sweet spot between not enough process and too much is not easy. 7120.5D alone is not going to create that perfect balance—that's where good people come in—but it's an important step in the right direction. ●

BRYAN O'CONNOR is a former Marine Corps test pilot and aeronautical engineer. He served at NASA as a Space Shuttle commander and program director and is currently serving as the Agency's Chief of Safety and Mission Assurance.