An ethical imperative for engineers

Note: In observance of National Engineers Week, celebrated this year Feb. 17-23, the Lab News *asked Executive VP and Deputy Labs Director John Stichman to write about a subject that is very close to him — that is, the importance of ethics in engineering. John's article here is based on his Sandia Technology Symposium presentation: An Ethical Imperative — Drawn from Engineering Mishaps. You can see the presentation at http://ln.sandia.gov/engineering-ethics.*

To "engineer" is to create and to create according to a professional discipline. In fact, the term "engineer" goes all the way back to the Latin *ingeniarius* and the *-gen-* part of the word traces to the Greek term for "create." Yes, "engineer" has roots that relate to terms we recognize, like "genesis" and "ingenious."

We engineers would do well, then, to be mindful that what we create — our products, hardware or software, large or small, are new additions to our world. They are things that have not existed before, at least not in their particular form or placement or usage. And human experience teaches us this: That which is new will also have unforeseen consequences.

Mary Shelley's classic book *Frankenstein* offers us an allegory on the unintended consequences of a creative endeavor. In the book, Victor Frankenstein experiences exhilaration and triumph as his creation stirs to life. Very soon, however, things begin to go terribly wrong. As the behavior of the Creature goes awry, Victor is consumed with trying to find a solution to what he has done. A particularly telling point in the story occurs when Victor and the Creature come face to face, and the Creature says, "You are my creator, but I am your master."

As professionals, we engineers are expected to have and use special knowledge in serving a beneficial societal need. In doing so, we are expected to obey the moral minimum — "first of all, do no harm." Each major discipline within engineering has a code of ethics to help us to govern our actions, and these can be viewed and studied by going to their respective websites or other materials.

Still, there is one very basic ethical imperative that is not typically discussed, yet is at the very foundation of good, sound engineering: Take positive steps to avoid avoidable errors.

Norman Augustine, the former CEO of Lockheed Martin and former chair of the National Academy of Engineering Council, has said "Engineers who make bad decisions often don't realize that they are confronting ethical issues." Yet, it is all too true that an engineering error can pose risk to life and limb, jeopardize a critical mission, or wreak economic havoc.

The above imperative is easy to say, even obvious in concept, but what does it mean in the day-to-day practice of our profession?

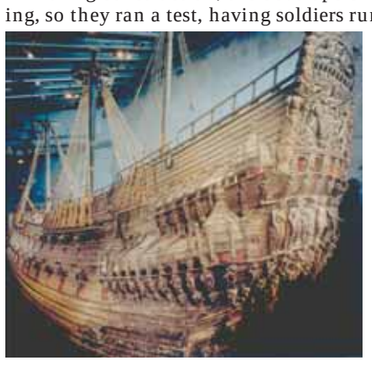
Like many other engineers, I have tried to learn lessons from the misadventures of others. Humbly, I offer some maxims for achieving the imperative and some discussion of the incidents that inspired these maxims.

By John Stichman

1. Demonstrate utter integrity with respect to the engineered object

Consider the Swedish warship, the *Vasa*. In 1628, Sweden was a major European power, and King Gustavus Adolphus had commissioned a warship to showcase this power for all to see.

During construction, the developers feared the ship would be prone to capsizing, so they ran a test, having soldiers run back and forth across the deck. The ship rocked so much that the test was stopped. But the king really wanted the ship, so the developers ignored the test and finished the ship. It sank after sailing only a nautical mile, with great loss of life.



KING GUSTAVUS ADOLPHUS wanted his warship, *Vasa*, to join the Swedish fleet. Engineers allowed the king's wishes to trump their own best judgment. Disaster ensued.

The saga of the *Vasa* offers us an example of "ballistic thinking" rather than "critical thinking." When we think ballistically, we are essentially bound on a fixed trajectory, ignoring information that would correct our path to our "target."

When we run a test, we are asking a question of our product, and it behooves us to listen to its answer. We must be extraordinarily evenhanded in doing so, because there are often great forces, as in the case of the *Vasa*, that would have us do otherwise. In any case, we must not let the desirability of a successful outcome cloud our engineering judgment. Surely, we can think of more modern situations, like the space shuttle *Challenger*, in which such ballistic thinking has played a part.

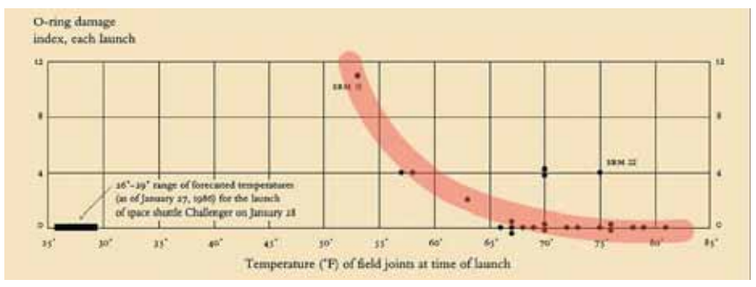
2. Communication is an ethical endeavor

Our management, our customers, and the public rely on our special knowledge as professionals. And clearly, our advice and our insights must be communicated to have an effect. To be effective, though, we must go beyond sharing information to sharing *meaning*, or interpretation. Recall, again, the case of the *Challenger*.

The spacecraft's engineers desperately needed to get across the seriousness of the effect of low temperature on the booster O-rings. Their plea was factual and passionate, but the temperature data was obscured by other data, making the relationship between temperature and O-ring failure unclear, and so the fateful launch decision was made.

LIVES RIDE on the decisions made by engineers. Here, members of the space shuttle *Challenger* crew stand in the white room at Pad 39B following the end of the preflight Terminal Countdown Demonstration Test. From left to right they are: Christa McAuliffe, Gregory Jarvis, Judy Resnik, Dick Scobee, Ronald McNair, Michael Smith, and Ellison Onizuka. (NASA photo)

Consider what might have happened if the following equally factual but clearer graph had been shown. The link between O-ring degradation and temperature is clear and compelling.

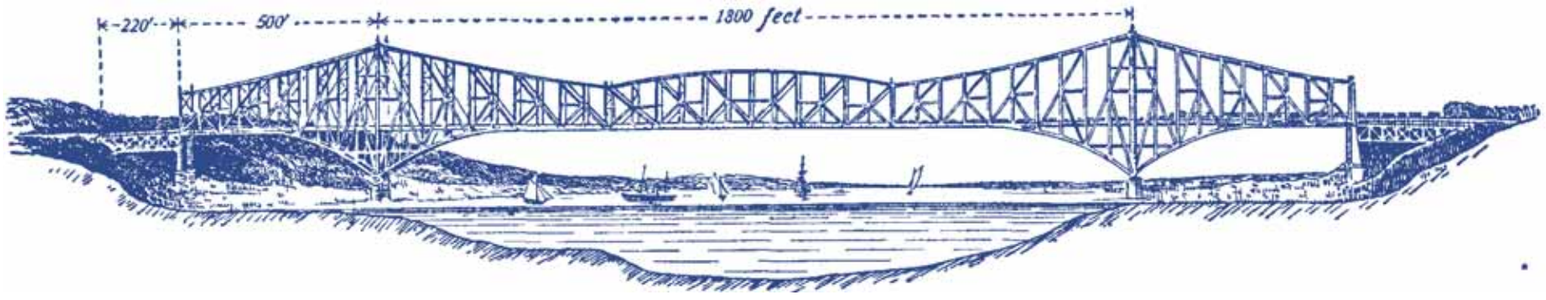


3. Consider the human factor

The burgeoning of automated systems has brought great benefits to quality of life of people everywhere, but it also has made more serious a longstanding conflict between human autonomy (self-governance) and machine automation (self-acting).

Case in point: The Airbus A320 was only indirectly controlled by the pilot, with software supplying the commands to the flight control elements. The A320 in the photo here crashed during a 1988 air show at Habsheim, France. Subsequent analysis determined that the aircraft's flight control software prevented the A320 from climbing out during a low-altitude maneuver. Had the human/machine interface been more effectively implemented, allowing the pilot to more readily assume control when necessary, the aircraft almost certainly wouldn't have been lost. As it happens, three of the 136 passengers on board the aircraft were killed.

THE AIRBUS A320 in 1988 was a new state-of-the-art aircraft that was a showcase for the integration of flight control software with pilot control. Three passengers were killed when the software didn't yield control of the aircraft to the pilot in a specific situation.



THE QUEBEC BRIDGE over the Saint Lawrence River was to have been the longest cantilevered span ever attempted. Critical considerations were omitted from the engineering plan. When the bridge collapsed in August 1907 — it was nearly completed at the time — 75 workers were killed. A second attempt several years later to build the bridge also failed. A third bridge now spans the river.

4. Plan: It's the essence of engineering

A plan is more than a project schedule; it is a product of deliberation in which the structure of the work, interdependencies, resources, and risks are defined, considered, and turned into a disciplined process for managing the work. Someone once said, "If you are failing to plan, you are planning to fail."

This deliberative character of planning is of crucial importance. This is the project phase, according to James Reason, author of *Human Error*, during which one runs the risk of making mistakes in judgment about the content and importance of necessary steps in completing a project. A tragic example is the planning and construction of the Quebec Bridge over the Saint Lawrence River. It was to be the longest (1,800 feet) cantilevered span ever attempted, yet the designer was so sure of his design approach, and the contractor was so short of funds, that critical calculations of the "dead load" (weight of the bridge itself) were left out of the plan. Furthermore, the project plan did not maintain clear responsibilities and authorities for work to proceed or to be halted, especially in view of the fact that the design engineer would not be on-site due to health problems. As the span continued to be built, the beams began to bend, but there was no definitive authority for stopping work. Then on Aug. 29, 1907, only minutes before quitting time, the bridge came crashing down, with 86 workers on site. Only 11 survived.

THE QUEBEC BRIDGE lies in a tangled heap after its collapse, which may well have been prevented with proper planning.

5. Obtain thorough, objective, and authoritative reviews of the work

The concept is simple: It is just too easy to overlook one's own mistakes. Reviews are not to be a box-checking exercise, but rather a value-added means to check our work. The Ariane V launch of June 4, 1996, was to be a glorious demonstration of the European Space Agency's capability in satellite deployment.

Instead, 36.7 seconds into the flight, one guidance software routine handed off control to another, incompatible one, and the result was a $500 million, highly embarrassing disaster for the ESA.

THE HOPES AND AMBITIONS of the European Space Agency rode with the Ariane 5 in this 1996 launch. The rocket was intended to move the agency to the forefront of the satellite launch business.

THE ARIANE 5 disintegrated less than a minute into its flight. The $500 million loss very likely could have been averted with a rigorous and objective outside review process. The Ariane's early problems were resolved and the rocket has become an ESA workhorse.

The official finding of the ESA board reviewing the accident went right to the point:

"The failure of the Ariane 501 was caused by the complete loss of guidance and attitude information 37 seconds after start of the main engine ignition sequence (30 seconds after lift-off). This loss of information was due to specification and design errors in the software of the inertial reference system.

The extensive reviews and tests carried out during the Ariane 5 Development Programme did not include adequate analysis and testing of the [software based] inertial reference system or of the complete flight control system, which could have detected the potential failure."

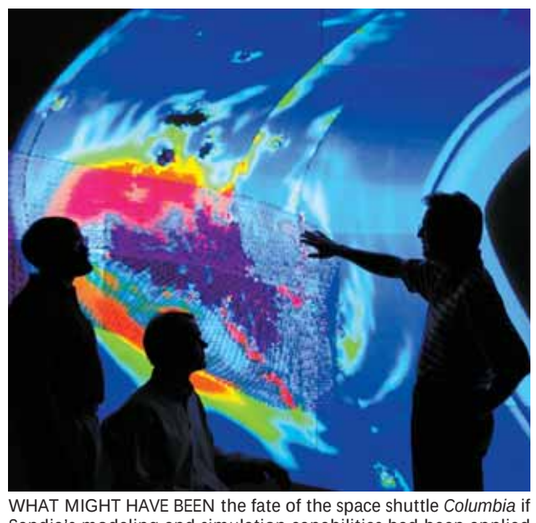
The software incompatibility encountered during the Ariane V launch was the type that could have been — and obviously should have been — caught in an appropriately planned set of reviews.

Those reviews should have been conducted by objective experts who themselves were not too close to or personally invested in the actual mission.

6. Know thy product (with apologies to Socrates)

The more we can do to establish an in-depth understanding of what we're engineering, the more we can gain insight into how the product functions, what's going on inside it, etc., the more we can discover and correct problems before they cause catastrophe.

As engineers, we gain insight through the models that we study, and here I mean models in a broad sense: theoretical, computational, and physical (testing). When invoked in a robust, balanced way, we can gain great insight. Today we have unprecedented capabilities in computational modeling that can make transparent what has previously been hidden behaviors of our systems, and therefore we have extraordinary new depths of insight available to us.



WHAT MIGHT HAVE BEEN the fate of the space shuttle *Columbia* if Sandia's modeling and simulation capabilities had been applied earlier in the shuttle program? (Photo by Randy Montoya)

Sandia's computational and physical modeling expertise contributed greatly to the understanding of the shuttle *Columbia's* problems during its fateful flight. Unfortunately, that insight and expertise were only sought out after the fact. We can now ask "What if this had been done earlier in the program?"

7. Work with discipline and prudence

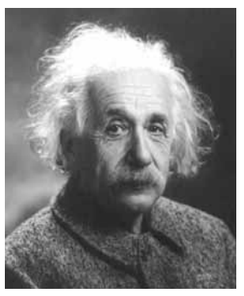
Engineering is a disciplined approach to the creation of things. Still, it is very tempting to take a shortcut because the rewards for doing this are pervasive, immediate, and temporary. Time and again we can trace a disastrous mishap to some deviation from accepted practice or an official procedure.

CHERNOBYL, the Soviet-era nuclear power plant that suffered a disastrous failure in 1986, stands as a stark reminder of the consequences of not doing things the right way from the start.

We would be wise to heed the advice of a former DOE quality official who told us to "beware of superstitious learning," which he defined to be those situations where we did something wrong, but everything turned out right, so we concluded that this is the way to do it.

Final thoughts

Having opened this essay with a statement by a prominent person, let me close with another. "Concern for Man [sic] himself and his fate must always form the chief interest for all technical endeavors in order that the creations of our mind shall be a blessing and not a curse to mankind. Never forget this in the midst of your diagrams and equations." — *Albert Einstein*



About the author

Executive VP and Deputy Labs Director John Stichman came to Sandia in 1972. Before assuming his present position, John was VP of Sandia's Weapons Systems division, where he was responsible for all aspects of Sandia's nuclear weapon engineering. John is a senior member of the Institute for Electrical and Electronics Engineers and is a recipient of the "Award for Exemplary Civilian Service" from the US Air Force.

John's published papers and conference presentations cover instrumentation and control, implantable medical electronics, and real-time optical computing. He holds two US patents.

John received a BS, MS, and PhD in electrical engineering from the University of Wisconsin.

John plans to retire from Sandia in March.