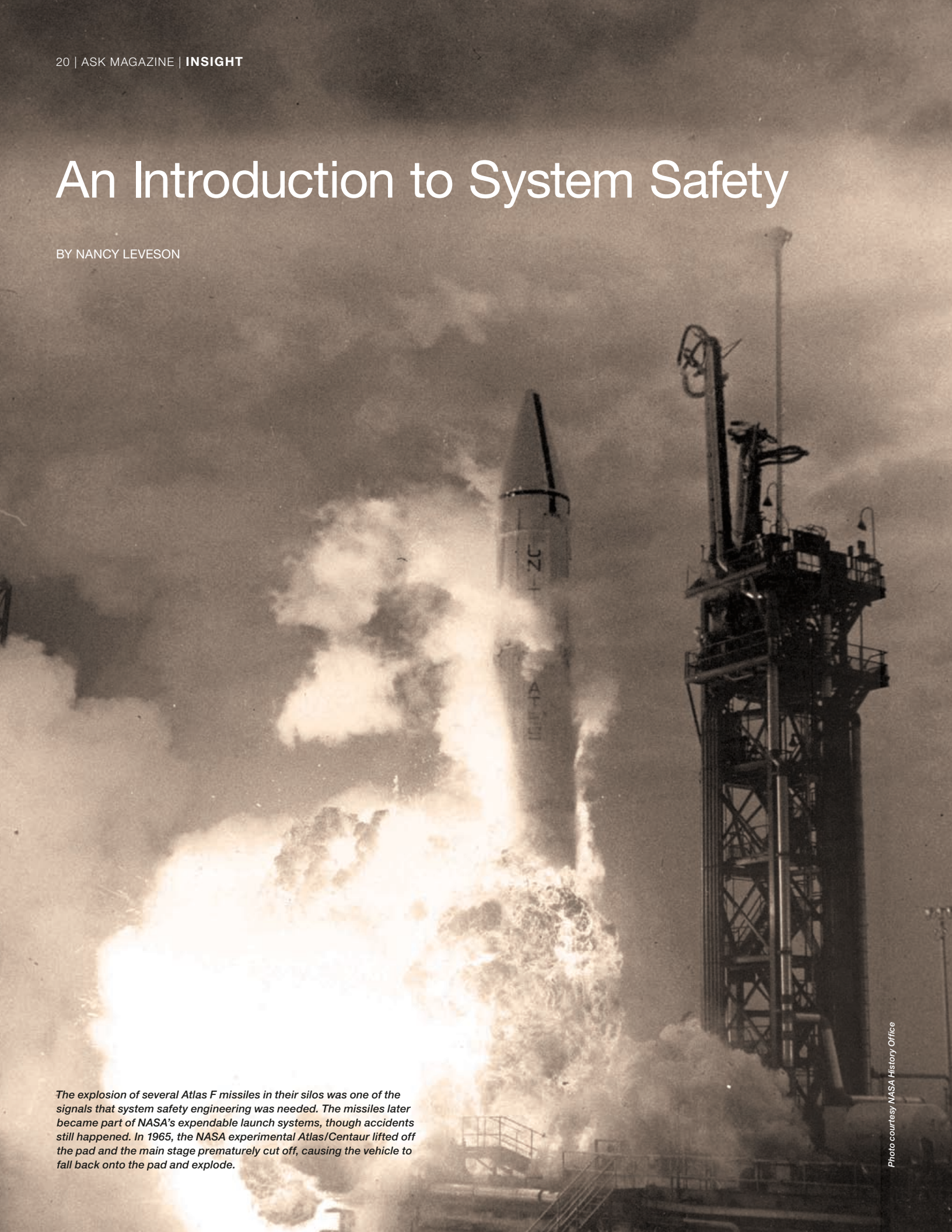
An Introduction to System Safety

BY NANCY LEVESON



The explosion of several Atlas F missiles in their silos was one of the signals that system safety engineering was needed. The missiles later became part of NASA's expendable launch systems, though accidents still happened. In 1965, the NASA experimental Atlas/Centaur lifted off the pad and the main stage prematurely cut off, causing the vehicle to fall back onto the pad and explode.

Photo courtesy NASA History Office

System safety uses systems theory and systems engineering approaches to prevent foreseeable accidents and minimize the effects of unforeseen ones. It considers losses in general, not just human death or injury. Such losses may include destruction of property, loss of mission, and environmental harm.

A Little History

Rigorous, defined approaches to safety engineering mostly arose after World War II, when the Atomic Energy Commission (and later the Nuclear Regulatory Commission) were engaged in a public debate about the safety of nuclear power; civil aviation was trying to convince a skeptical public to fly; the chemical industry was coping with larger plants, increasingly lethal chemicals, and heightened societal concern about pollution; and the Department of Defense (DoD) was developing ballistic missile systems and increasingly dangerous weapons. These parallel efforts resulted in very different approaches, mostly because the problems they needed to solve were different.

While the nuclear power, commercial aircraft, chemical, and other industries have taken a conservative approach to introducing new technology, changing designs slowly over time, defense and space systems have pushed the technology envelope, developing tremendously complex, novel designs that stretched the limits of current engineering knowledge, continually introducing new and unproven technology, with limited opportunities to test and learn from extensive experience. In response, a unique approach to engineering for safety, called system safety, arose in these industries.

When the Atlas and Titan intercontinental ballistic missiles (ICBMs) were being developed in the 1950s, system safety was not yet identified and assigned as a specific responsibility. Instead, each designer, manager, and engineer was responsible for the reliability of his particular component or subsystem. As a result, many interface problems went unnoticed until it was too late. Within eighteen months after the fleet of 71 Atlas F missiles became operational, four blew up in their silos during operational testing. The missiles also had an extremely low launch success rate. The air force had typically blamed most accidents on pilot error, but these new liquid-propellant missiles had no pilots to blame and yet blew up frequently and with devastating results. When these early losses were investigated, a large percentage of them were traced to deficiencies in design, operations, and management. The importance of treating safety as a *system* problem became clear and, as a result, systems engineering and system safety (a subdiscipline of systems engineering) were developed.

The Minuteman ICBM became the first weapon system to have a contractual, formal, disciplined system safety program. At first, few techniques that could be used on these systems existed, but specialized system safety practices evolved over time. Particular emphasis was placed on hazard analysis techniques, such as fault trees, which were first developed to cope with complex programs like Minuteman. While these techniques were useful for the technology of the time, new technologies, particularly digital technology and software, have made many of them no longer appropriate for the increasingly complex, software-intensive systems we build today. Unfortunately, recognition of these limitations has been slow. Attempts to apply techniques developed for the simpler and primarily electro-mechanical systems of the past continue, with only partial success.

The space program was the second major area to apply system safety approaches in a disciplined way. After the 1967 Apollo 1 fire that killed three astronauts, NASA commissioned the General Electric Company at Daytona Beach, among others, to develop policies and procedures that became models for civilian space flight safety activities. Jerome Lederer was hired to head safety at NASA. Under his leadership, an extensive system safety program was set up for space projects, much of it patterned after the air force and DoD programs. Many of the same engineers and companies that had established formal system safety defense programs also were involved in space programs, and the systems engineering and system safety technology and management activities were transferred to this new work.

But as time has passed without major new manned space flight development projects at NASA, many of the very effective NASA system safety practices have been replaced by reliability engineering and approaches to safety used by industries with very different requirements. For Constellation to be successful, traditional system safety practices will need to be reemphasized and extended to handle new technology, particularly extensive use of software and computers.

What Is System Safety?

The primary concern of system safety is the management of system hazards as opposed to emphasis on eliminating component failures in reliability engineering. Borrowing Thomas Huxley's definition of science, in 1968 George Mueller described the then-new discipline of system safety engineering as "organized common sense." It is a planned, disciplined, and systematic approach to identifying, analyzing, eliminating, and controlling hazards by analysis, design, and management procedures throughout a system's life cycle. System safety activities start in the earliest concept development stages of a project and continue through design, production, testing, operational use, and disposal.

Although system safety is a relatively new and still-evolving discipline, some general principles hold for its various manifestations and distinguish it from other approaches to safety and risk management.

- **System safety emphasizes building in safety, not adding protection features to a completed design.** System safety emphasizes the early identification of hazards so action can be taken to eliminate or minimize them in early design decisions; 70 to 90 percent of the design decisions that affect safety are made in concept development, requirements definition, and architectural design. The degree to which it is economically feasible to eliminate or minimize a hazard rather than to control it depends on the stage in system development at which the hazard is identified and considered. Early integration of safety considerations into the development process allows maximum safety with minimum negative impact. The usually more expensive and less effective alternative is to design first, identify the hazards, and then add on protective equipment to control the hazards when they occur. A recent demonstration project for the Jet Propulsion Laboratory showed how safety can be designed into a spacecraft (an outer-planets explorer, in this case) from the early concept formation and trade study stages. New hazard analysis approaches that include software were used. (See http://sunnyday.mit.edu/papers/IEEE-Aerospace.pdf.)

- **System safety deals with systems as a whole rather than with subsystems or components.** Safety is an emergent property of systems, not components. One of the principle responsibilities of system safety is to evaluate the interfaces between the system components and determine the effects of component interaction. (The

The Minuteman ICBM became the first weapon system to have a formal, disciplined system safety program. Here, a Minuteman II launches successfully.

Photo Credit: U.S. Air Force

FOR CONSTELLATION TO BE SUCCESSFUL, TRADITIONAL SYSTEM SAFETY PRACTICES WILL NEED TO BE REEMPHASIZED AND EXTENDED TO HANDLE NEW TECHNOLOGY, PARTICULARLY EXTENSIVE USE OF SOFTWARE AND COMPUTERS.

set of components includes humans, machines, and the environment.) Safety is an *emergent system property*. It is not possible to determine whether a spacecraft design is acceptably safe, for example, by examining a single valve. In fact, statements about the "safety of the valve" without information about the context in which it is used are meaningless. Conclusions can be reached about the *reliability* of the valve (defined as the probability that the behavior of the valve will satisfy its specification over time and under given conditions), but safety can only be determined by the relationship between the valve and the other spacecraft components, in the context of the whole.

- **System safety takes a larger view of hazard causes than just failures.** A lack of differentiation between safety and reliability is widespread at NASA and elsewhere. Hazards are not always caused by component failures, and all failures do not cause hazards. Reliability engineering concentrates on component failure as the cause of accidents and a variety of techniques (including redundancy and overdesign) are used to minimize them. As early missile systems showed, however, losses may arise from interactions among system components; serious accidents have occurred when the system components were all functioning exactly as specified. The Mars Polar Lander loss is an example. Each component worked as specified but problems arose in the interactions between the landing leg sensors and the software logic responsible for shutting down the descent engines. Reliability analysis considers only the possibility of accidents related to failures; it does not investigate potential damage that could result from *successful* operation of individual components. Software, ubiquitous in space systems today, is an important consideration here. In most software-related accidents, the software operates exactly as intended. Focusing on increasing the reliability with which the software satisfies its requirements will have little impact on system safety.

  Reliability and safety may even conflict. Sometimes, in fact, increasing safety can decrease system reliability. Under some conditions, for instance, shutting down a system may be an appropriate way to prevent a hazard. That increasing reliability can diminish safety may be a little harder to see. For example, increasing the reliability (reducing the failure rate) of a tank by increasing the burst pressure–to–working pressure ratio may result in worse losses if the tank does rupture at the higher pressure. System safety analyses start from hazards, not failures and failure rates, and include dysfunctional interactions among components and system design errors. The events leading to an accident may be a complex combination of equipment failure, faulty maintenance, instrumentation and control inadequacies, human actions, design errors, and poor management decision making. All these factors must be considered.

- **System safety emphasizes analysis in addition to past experience and codes of practice.** Standards and codes of practice incorporate experience and knowledge about how to reduce hazards, usually accumulated over long periods of time from previous mistakes. While the use of such standards and learning from experience is essential in all aspects of engineering, including safety, the pace of change today does not always allow for such experience to accumulate. System safety analysis attempts to anticipate and prevent accidents and near misses *before* they occur, in addition to learning from the past.

- **System safety emphasizes qualitative rather than quantitative approaches.** A system safety approach identifies hazards as early as possible in the design stage and then designs to eliminate or control those hazards. At these early stages, quantitative information usually does not exist. Although such information would be useful in prioritizing

Seated at the witness table before the Senate Committee on Aeronautical and Space Services hearing on the Apollo 1 accident are (left to right) Dr. Robert C. Seamans, NASA deputy administrator; James E. Webb, NASA administrator; Dr. George E. Mueller, associate administrator for Manned Space Flight; and Maj. Gen. Samuel C. Phillips, Apollo Program director. In an effort to prevent another such tragedy from occurring, NASA commissioned the General Electric Company and others to develop policies and procedures that became models for civilian space flight safety activities.

hazards, subjective judgments about the likelihood of a hazard are usually adequate and all that is possible when design decisions must be made. In addition, probabilistic risk analyses that exclude potential causes of an accident, including interactions among non-failing components, design errors, software and hardware requirements errors, and poor management decision making, can lead to dangerous complacency and focusing engineering efforts only on the accident causes for which those measures are possible. If enough were known about factors such as design errors to define a probability for them, then safety would be more effectively enhanced by removing the design error than by measuring it in order to convince someone that it will never cause an accident. In the case of the Mars Polar Lander, if the scenario that unfolded had been known and could have been included in a probabilistic risk analysis, then the engineers would have had enough information to change the software so the unsafe control command would not be issued.

- **System safety is more than just systems engineering and must incorporate management and safety culture concerns.** System safety engineering is an important part of system safety, but the concerns of system safety extend beyond the traditional boundaries of engineering. In 1968, Jerome Lederer, then the director of the NASA Manned Flight Safety Program for Apollo, wrote:

  > System safety covers the total spectrum of risk management. It goes *beyond* the hardware and associated procedures of system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment, and many other nontechnical but vital influences on the attainment of an acceptable level of risk control. These nontechnical aspects of system safety cannot be ignored.

Using these general principles, system safety attempts to manage hazards through analysis, design, and management procedures. Key activities include analyzing system hazards from the top down, starting in the early concept design stage to eliminate or control hazards and continuing during the life of the system to evaluate changes in the system or the environment; documenting and tracking hazards and their resolutions (establishing audit trails); designing to eliminate or control hazards and minimize damage; maintaining safety information systems and documentation; and establishing reporting and information channels. ●

For more information see the following:

- *http://sunnyday.mit.edu/papers/jsr.pdf*
- *http://sunnyday.mit.edu/accidents/safetyscience-single.pdf*
- *http://sunnyday.mit.edu/ESMD-Final-Report.pdf*

NANCY LEVESON is a professor of aeronautics and astronautics at Massachusetts Institute of Technology. She has been associated with NASA for more than twenty years, was a member of the NASA Aerospace Safety Advisory Panel at the time of the *Columbia* loss, and was a consultant for the *Columbia* Accident Investigation Board. She is a member of the National Academy of Engineering.