August 2020

THE SPACE SAFETY INSTITUTE

ISSF
INTERNATIONAL SPACE SAFETY FOUNDATION

PROPOSAL FOR A MODERN INDUSTRY-GOVERNMENT PARTNERSHIP TO ADVANCE COMMERCIAL SPACEFLIGHT SAFETY

INDEX

INTRODUCTION

For the past 15 years the debate on commercial human spaceflight safety has revolved mainly around suborbital tourism vehicles and has been grounded on the misconception that safety regulations can be established only when enough operational experience is gained, (several years, perhaps decades from now). While the initial enthusiasm for suborbital spaceflight seems to be fading away following continuous delays, accidents and bankruptcies, the area of potential space commercial services is widening and gaining momentum. Within a decade, human spaceflight operation in Low Earth Orbit (LEO) may become predominantly commercial. There could be also important elements of private participation to government Moon and Mars exploration missions, which because of high costs could also include international partners (see ESA/Airbus DS cooperation with NASA/LMCO on Orion Spacecraft development). The suborbital industry may evolve away from space tourism to follow a similar mixed-users path (see recent agreements to buy/operate Virgin Galactic SS2 in Italy and UK), in particular in the perspective of developing point-to-point transportation. As a consequence, there is a strong need to establish harmonized safety requirements and a system of recognition of safety certifications to better fit commercial space programs into a mixed private-government environment.

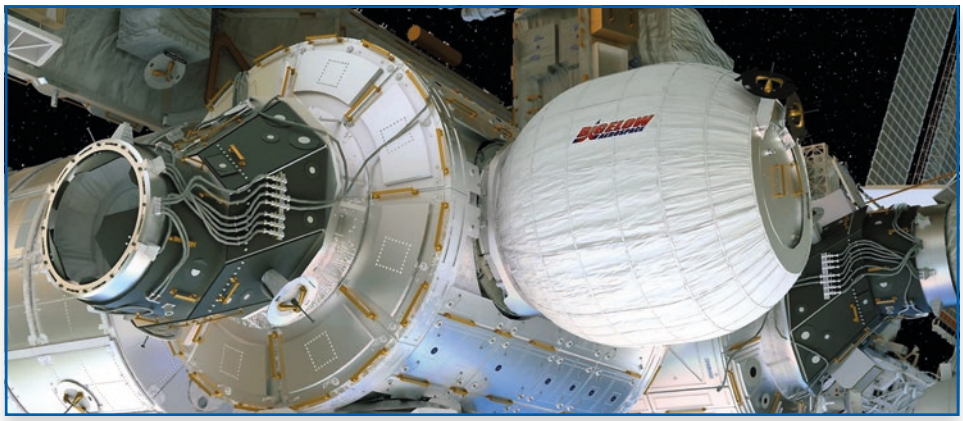
The purpose of this report is to provide the rationale for the establishment of a (commercial) Space Safety Institute in the U.S. as “regulated self-policing” entity. It would be an open consortium of industry, space agencies and regulators to efficiently perform standardization and certifications activities, conduct joint research, and provide educational and professional training opportunities, within a broad framework of mandated policies and rules.

The need for such organization is both practical and strategic. Government as responsible for public welfare (health, safety and environment), and sometimes as customer, needs assurance that the commercial space industry can deliver on promises. However, system safety is multidisciplinary and there is a relatively limited numbers of people with the requisite expertise and updated experience in writing performance requirements and supporting safety peer-reviews, making it hard for regulators to be able to rely solely on its own personnel. In addition, all the parties involved need assurance that commercial competition takes place on a level playing field and that safety is not compromised by cost cutting efforts. Sharing data, transparent communication and independent risk assessment can provide such assurance. But above all, industry must recognize and act on the strategic business value of improving on the poor safety record of space programs and for such purpose leadership commitment and coordinated research and educational efforts of all stakeholders are paramount.

The proposed Space Safety Institute builds on concepts, experience and practices of various programs and sectors and may be archetypal of future direction in other fields (e.g. aviation). First the report introduces the principles of system safety, which is the systematic application of engineering and management principles, criteria and techniques to attain an acceptable level of system risk control. System safety engineering, also known as risk-based design or safety-by-design, represents a major departure from the traditional rules-based design applied to “evolutionary” commercial products. The pillar of system safety engineering is to consider the actual system’s hazards instead of pre-defined safety rules as design drivers. In other words, the safety features of a system under development are not pre-defined design rules but the specific risk-mitigation measures selected by the designer based on hazard analysis and generic safety goals. The organizational component of system safety, system safety management, is also essential because it establishes the conditions and processes that allow to achieve the organization’s safety objectives. Through leadership commitment, trained and competent personnel, safety culture, hazards documenting and tracking, and risk management, system safety management provides on one side assurance on the capabilities of the organization, and on the other side it proves their effective and successful use.

The report then goes on describing the socio-technical evolution of system safety at NASA and shows how accidents prevention techniques and safety organization evolved through the years. The early NASA approach to space missions safety, in the sixties, was called ‘man-rating’ and consisted of components testing to improve rockets reliability, adding escape systems, and selecting flight profiles that would keep accelerations within human tolerance limits. Safety was essentially considered the ‘natural’ by-product of good design. The idea that accidents could be prevented by applying systematic risk mitigation techniques came years later. The turning point was the Apollo 1 fire accident during ground testing in 1967. The accident’s cause was the use of 100% pure oxygen atmosphere in the capsule without any care on selecting compatible materials and removing potential ignition sources. It was surprising that the

oxygen fire hazard, at the time already well known and documented in many industries and in the medical field, went uncontrolled. Suddenly it was realized at NASA that making a spacecraft reliable was in itself not sufficient to make it safe. Reliability assessments and testing could not account for certain hazardous interactions, for human errors or software faults. The Apollo 1 fire was a fully preventable accident that happened because there was no program for systematic risk identification and control. The accident demonstrated the need for performing hazard analyses throughout design, development and operation phases. Years later, a different kind of accident, an 'organizational accident', led to the destruction of the Shuttle Challenger. During Shuttle development, the hazard of hot gas leaking from solid rocket booster joints was identified and controlled by use of redundant O-rings. However, the design was deficient as revealed by frequent erosions of outer O-ring witnessed by post-flight inspections. Eventually, the Challenger launch of January 1986 in freezing weather conditions (outside the qualification envelope) led to hot gases leaking and impinging on the main tank which exploded. The underestimation of the anomaly and the launch decision that led to the Challenger disaster were the result of schedule and costs pressures on the Shuttle program, and of poor risk management. Fifteen years later, something similar happened to the Shuttle Columbia, although the technical anomaly was different, and the decisional process failed differently. Those accidents demonstrated that human errors, hardware failures and software faults are proximate causes of accidents, and that ultimate causes originate from unfavorable organizational conditions. Those conditions can be prevented by applying adequate controls on the organization in charge of design, development and operation. In other words, the organization's safety culture, trained personnel, robust processes, independent checks are as important in preventing accidents as safety technical requirements. Over the years, human spaceflight safety at NASA matured from the initial 'man-rating' narrow scope into an encompassing socio-technical control system. The technical part consists of human-centered design processes aimed to ensure human protection and health while accounting for human performance, accommodating human needs, and giving to crew ultimate control of the vehicle. The social part consists of a check-and-balance system in management and decisional processes, involving program organization, independent oversight, and separate safety authority.



Bigelow Aerospace BEAM.

Having discussed the experience gained over almost 60 years of government space programs, the report goes to present a general overview of principles and practices governing the establishment and use of commercial products standards in U.S. and the associated *conformity assessment* activities. Standards may have different purposes than safety, and be of three different types (de-facto, consensus, and mandatory). Conformity assessments can also vary from manufacturing statement of conformity, to third-party testing and certification. A variety of organizations perform safety certifications: independently (e.g. UL), under delegation from government (e.g. American Bureau of Shipping), or in support of regulators (e.g. Institute of Nuclear Power Operations). The principle that a standard can be established only when experience is gained is well established. We can even say that it reflects the most traditional approach to standards development. However, it fits only products slowly evolving over many decades or even centuries. It is based on the idea of developing "prescriptive standards" that give details rules about the design. For example, aviation has been (until now, but things may change soon) a typical "evolutionary" industry. Aviation safety standards consist of detailed prescriptive requirements built on a large number of lessons learned from mishaps and close calls over a period of more than a century and aimed to specific types of vehicles. Instead, since the 80's, space programs (and many other fields of advanced technologies) have been using a risk-based approach to system development and so-called "performance standards". The risk-based approach consists in identifying the potential conditions for mishaps starting in the early phases of design and implementing risk mitigation and control measures consistent with broad safety goals.

Finally, the report discusses the current U.S. commercial human spaceflight regulatory framework. On December 23, 2004, President Bush signed the Commercial Space Launch Amendments Act of 2004 (CSLAA). The CSLAA made the Department of Transportation and the Federal Aviation Administration (DOT/FAA) responsible for regulating commercial human space flight. The law established a moratorium (also called 'learning period') for safety regulations of flight participants (crew and passengers) of 8 years, later extended until 2023, unless an accident happens. Unfortunately, the rhetoric linked to benefits of certain deregulations in eliminating trade barriers was exploited by some parties to promote the moratorium on safety regulations. A lose-lose situation because not having minimum safety regulations is against the interest of the customer while

defeating the fundamental interest of industry to operate within a stable set of rules. The CSLAA just requires operators to provide prospective customers with written information about the risks of spaceflight and a statement of the fact that the U.S. government has not certified the vehicle as safe for carrying crew or spaceflight participants. However, there is one remarkable exception to such rule. The commercial vehicles providing services to the International Space Station (ISS) must comply with the safety requirements of the ISS program and be certified by NASA. (ISS - Intergovernmental Agreement (IGA)). Currently the commercial human spaceflight industry is developing suborbital systems (Virgin Galactic SS2, Blue Origin New Shepard, etc.) and orbital systems (SpaceX Dragon, Boeing CST-100 Starliner, Bigelow Aerospace BEAM, and Dream Chaser for Resupply Services). A de-facto double regulatory regime exists (no-regulation/full-regulation) for safety on-board space vehicles depending if the customer is a private entity or NASA ISS Program.

By not requiring industry to establish safety rules up-front, in line with the experience gained through government space programs, the unintended effect of CSLAA has been to encourage industry to set the clock of their safety practices back to the early 1960s. The CSLAA may have planted the seeds of the first suborbital flight accident, the Oct. 31 fatal crash of Virgin Galactic's SpaceShipTwo.

SpaceX Crew Dragon.

The CSLAA allows companies to apply whatever level of failure tolerance they like in the design, without even requiring independent verification of the correct implementation.

Curiously, the argument of inflexibility, costs, and barrier to innovation used by the commercial human spaceflight industry to push the case for the moratorium enshrined in the U.S. Congress Commercial Launch Amendments Acts (CSLAA) of 2004, is the same that other advanced industries and the U.S. Government have used to promote the transition from old-fashioned "prescriptive standards" to modern "performance standards".

The final part of the report looks to what kind of regulatory framework should be in place when the current moratorium expires in 2023. It proposes the establishment of a Space Safety Institute, as a cooperative endeavour between industry, space agencies and regulators. The discussion in this report on how to set-up and operate the Space Safety Institute is heavily influenced by the analysis of such institutions performed few years ago by the Presidential Committee that investigated the Deepwater Horizon oil drilling rig disaster of 2010 in the Gulf of Mexico. There are in fact some remarkable analogies between the negative attitude shown by the oil industry before the disaster, (they fought for 20 years against introducing safety management best practices), and that of the "New Space" community in the past 15 years. An additional justification for establishing the Space Safety Institute is to help transferring unique space safety experience, knowledge and skills available at NASA.

In conclusion, the Space Safety Institute would support a regulatory model that can react quickly and efficiently to technological advancements while exercising effective controls on commercial space systems developments. The Space Safety Institute would perform standardization and system certification activities, as well as educational and research activities. The regulator would establish broad policies and keep a general oversight role of institute's processes and activities, while concentrating on other issues, which lie outside the Space Safety Institute scope, as space traffic management and international coordination.

Blue Origin New Shepard.

Chapter 1
SYSTEM SAFETY

1.1 WHAT IS SYSTEM SAFETY?

To be absolutely safe, a system, product, device or material should never cause or have the potential to cause an accident; a goal practically impossible to achieve. In the development and operation of systems, the term "safety" is used to mean an acceptable risk level, not absolute safety.

System safety is the planned, disciplined, and systematic application of engineering and management principles, criteria and techniques to achieve the safety goals of a system. The system safety process consists in the identification of safety related risks and their elimination and/or control by design and/or procedures, based on pre-established performance safety requirements and criteria meant to represent the optimum achievable objective at the state of art, and within project's constraints. The system safety process activities start in the earliest concept development phases of a project and continue through design, production, testing, operational use, and disposal. The core technique used for system safety is the Hazard Analysis that has several variants, from Functional Hazard Analysis (FTA), to Preliminary Hazard Analysis (PHA), System Hazard Analysis (SHA), etc.

To be absolutely safe, a system, product, device or material should never cause or have the potential to cause an accident; a goal practically impossible to achieve

Sometimes terms as risk-based design, or safety-by-design are used as synonyms for system safety engineering. 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 [safety] 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 phase 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.

System safety covers the total spectrum of [safety] risk management

1.2 WHY SYSTEM SAFETY WAS DEVELOPED?

Rigorous, defined approaches to system safety 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.

Within eighteen months after the fleet of 71 Atlas F missiles became operational, four blew up in their silos during operational testing

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

On September 19th, 1980, a Titan II Missile exploded in Damascus (Arkansas) and blew its nuclear warhead out of the silo. It was a day we nearly lost Arkansas (Courtesy: Greg Devlin).

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 sub-discipline 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

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.

1.3 KEY PRINCIPLES OF RISK-BASED DESIGN

Although system safety engineering is a relatively new and still evolving discipline, some general principles hold for its various manifestations.

- System safety engineering 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

Apollo 1

Apollo 1 - Fire kills 3 Disaster:

Ed White, Roger Chaffee and Gus Grissom die in launch pad fire while inside their Apollo 1 capsule. Fire was a result of 100% pure oxygen inside capsule, redesigned hatch that opened in instead of pushing out, and a short, a spark that ignited the fire.

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.

- System safety engineering 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 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 engineering takes a larger view of hazard causes than just failures. A lack of differentiation between safety and reliability is still widespread at major organizations. 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

Safety is an emergent system property

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. 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 engineering emphasizes analysis in addition to past experience and codes of practice. Rule-based 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 prescriptive 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 engineering 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 hazards, subjective judgments about the likelihood of a hazard are usually adequate and all that is available 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

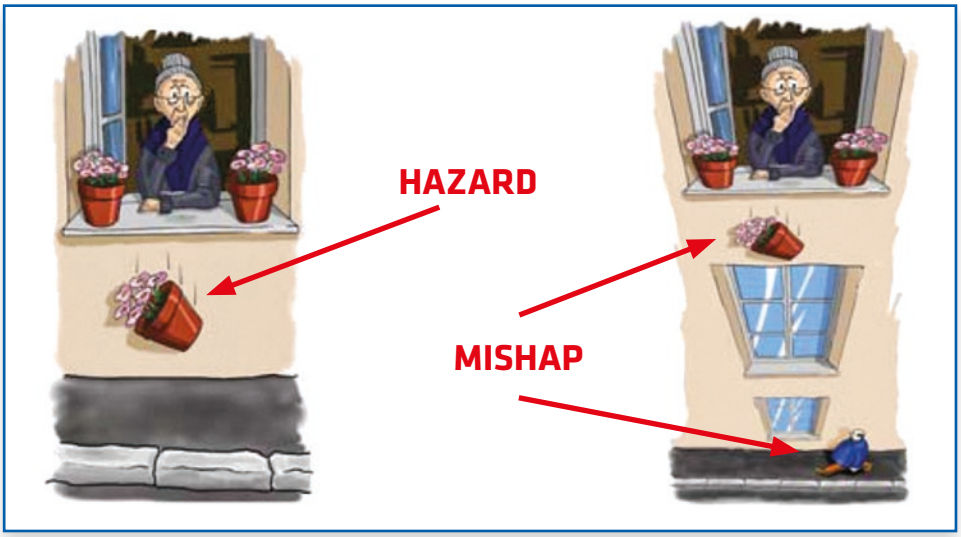
System safety analysis attempts to anticipate and prevent accidents and near misses before they occur, in addition to learning from the past

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.

1.3.1 Hazard, Mishap & Risk

System safety is achieved by thoroughly exploring systems risks starting with conceptual design and progressing with implementation of architectural and detailed risk mitigation measures as the design evolves and becomes more detailed. The initial top down system risk analysis will be progressively and iteratively refined and combined with bottom up sub-systems and components risk analyses until compliance with systems safety goals is achieved.

Recognizing the elements of a hazard and understanding the relationship between hazard and risk, allows designers to select and implement hazards controls that effectively mitigate the risks.



In the development of a system, we can distinguish risks with consequences on "safety," on "mission success," or on "development/programmatic". Here, we refer solely to safety risks.

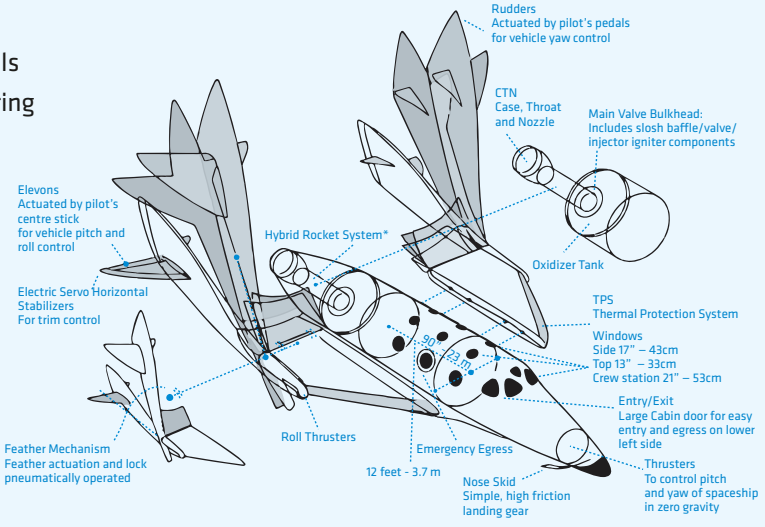
A hazard is a potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment. Instead, a "mishap" or accident is an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. In other words, a mishap is a hazard that became actualized, a transition from hypothesis to fact.

There are three kinds of hazards: functional hazards, inherent hazards and induced hazards.

- **Functional hazards.** A safety-critical function is either a 'must-work' function or a 'must-not-work' function. A must-work-function is an active function vital for keeping the crew

Example of triple safety critical system: SpaceShipTwo feather mechanism

- The feather system consist in the rotation of the tails of the vehicle to create higher aerodynamic drag during descent to improve stability and limit deceleration
- The feather system is a safety-critical mechanism. It is **must-not-work** system (1 time) during the ascent phase, and **must-work** (twice) during the descent phase
- Must not deploy too early, must deploy at descent, must retract before starting the gliding



alive (e.g. life-support system of a spacecraft). A must-not-work function is instead a function that if operated inadvertently or untimely (e.g. propulsion ignition, or access to a live high-power laser) can kill or injure the crew or cause damages. A function may be a 'must-not-work' function for some periods of a mission and a 'must-work function' for remaining time.

- **Inherent hazards.** A system function may not be safety-critical yet include some inherent hazards such as high voltages, high temperature, toxic compounds, etc. For example, a microgravity experiment using a metal melting furnace. Inherent hazards exist in a system due to its basic nature and function. They can be controlled, but not eliminated (without changing the basic technology associated with the system). Usually system design is a trade-off between inherent hazards of different technologies. Examples of inherent hazards are contacts hazards like sharp edges, stored energy hazards like a gas pressurized tank, or chemical hazards like toxic compounds (e.g., ammonia) or flammable materials.

- **Induced hazards.** They exist due to the design or operation of the system. They can be putted there by the designer and can generally be removed or controlled without disabling the operational capability of the system. Sometimes induced hazards are due to interaction between components, between systems, between human and system or component, or between system and environment. Examples are collision between space systems, decompression of a habitable volume in space, or entanglement in rotating parts.

Risk is an expression of the impact and possibility of a mishap in terms of potential severity and probability of occurrence. Risk can be assessed qualitatively or quantitatively against risk acceptance criteria (see table below)

Acceptable risk level is not the same as personal acceptance of risk, but it refers to risk acceptability by stakeholders' community or by society in a broad sense. Acceptable risk levels vary from system to system and evolve with time due to socio-economic changes and technological advancement. Implementing proven best-practices is a prerequisite for achieving an acceptable risk level. Best-practices are traditionally established by government regulations and norms, and/or by industrial standards. Without such reference, the term safety, or acceptable risk, becomes meaningless. In other words, compliance with regulations, norms and standards represents the safety yardstick of a system.

HAZARD CATEGORY / FREQUENCY	CATASTROPHIC	CRITICAL	MARGINAL
FREQUENT ($X > 10^{-1}$)	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
PROBABLE ($10^{-1} > X > 10^{-2}$)	UNACCEPTABLE	UNACCEPTABLE	HIGH
OCCASIONAL ($10^{-2} > X > 10^{-3}$)	UNACCEPTABLE	HIGH	HIGH
REMOTE ($10^{-3} > X > 10^{-6}$)	HIGH	HIGH	LOW
IMPROBABLE ($10^{-6} > X$)	LOW	LOW	LOW

Hazard Risk Assessment Matrix.

A hazard mitigation measure is either hazard elimination or hazard control. A hazard control is any design feature, device, or operational procedure that will reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood that a mishap will occur. Residual risk is the remaining risk that exists after all hazard mitigation measures have been implemented or exhausted in accordance with the applicable safety requirements and the project risk management process.

1.3.2 Hazard Elements

For hazard's correct identification, description and risk assessment, hazard's basic elements need to be understood. The concept of hazard triangle is particularly useful when applied to inherent hazards (Clifton, 2005). A hazard is comprised of the following three basic components: hazardous element (HE), initiating element (IE), and target element (TE).

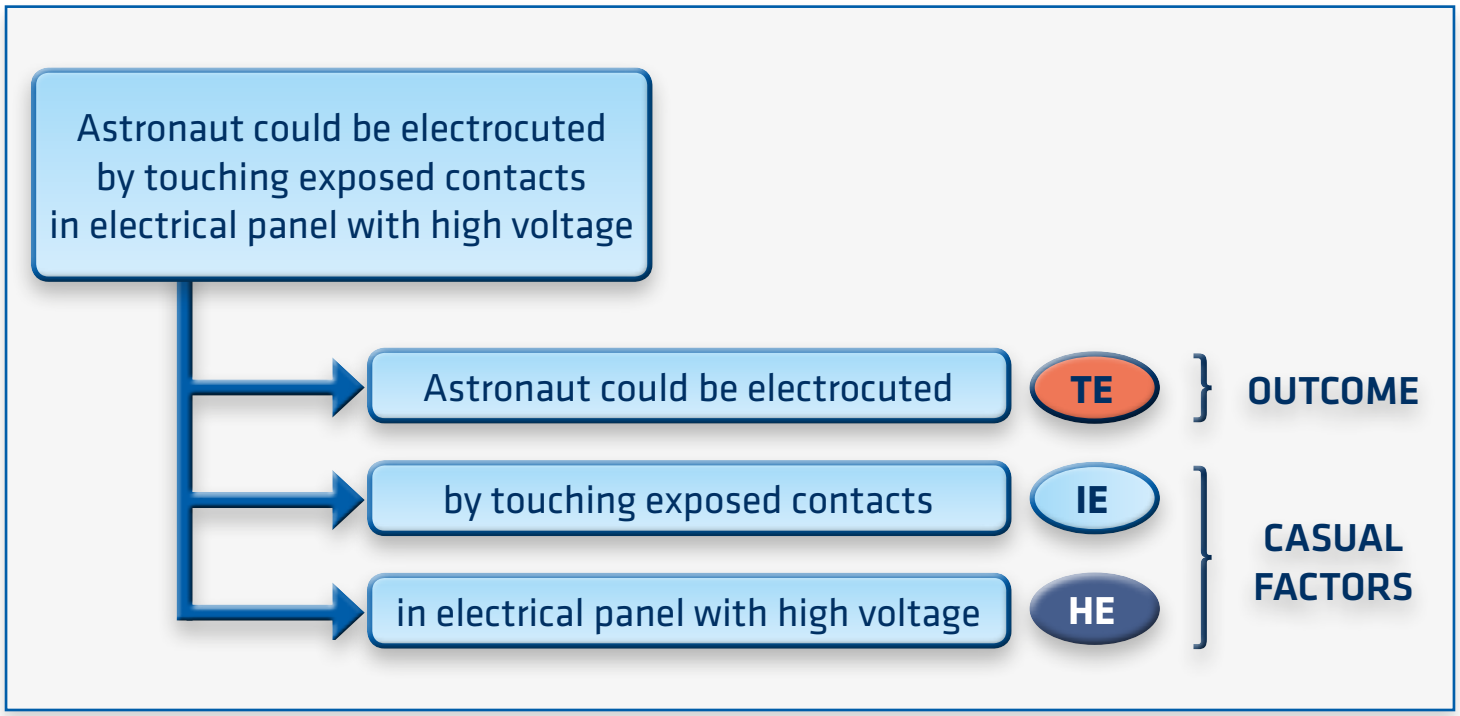
- **Hazardous Element (HE):** basic hazardous resource such as an energy source.

- **Initiating Element (IE):** trigger or initiator event that creates the impetus for the hazard. There could be several distinct casual factors leading to the initiating element.

- **Target Element (TE):** person, property or environment that are vulnerable to injury, damage, or degradation. They can be affected separately or not under different circumstances.

Examining the constituent element of a hazard helps ensuring that the hazard description is complete and correct, which is a key starting step of any hazard analysis.

When a hazard is actualized it is the effect on the TE or outcome (injury, death, damage, destruction, contamination)



Example of hazard description and of its constituent elements.

that defines the severity of the mishap. All three sides of the triangle are essential and required for a hazard to exist.

1.3.3 Hazard theory and risk probability

The key principle of hazards theory is that mishaps can be predicted via hazard identification, and prevented via hazard elimination or control:

Mishaps can be predicted via hazard identification, and prevented via hazard elimination or control

- Hazards may lead to mishaps
- Hazards are into a system or induced by its design and operations
- Hazards are recognizable by their components elements (triangle)
- Hazard causes are predictable and controllable
- A design flaw can be a hazard cause

A hazard is a deterministic entity (it is there or not), while relevant mishaps are probabilistic. A hazard exists when all three hazard components are present. Mishap probability is the probability that IE actuates when HE and TE are present. Reduce the probability of the IE and the mishap probability is reduced. Mishap severity is dictated by TE being present. Reduce the HE or TE and the mishap severity will be reduced.

1.3.4 Hazard identification

Hazard identification is a prerequisite for hazard elimination and control.

A hazard is a deterministic entity (it is there or not), while relevant mishaps are probabilistic

Hazards checklists and basic hazard groups are used for helping in the hazard identification process. Hazards can be identified from a variety of sources such as:

- general knowledge of system energy sources experience gained from previous space projects
- hazards grouping or checklists used in other fields
- detailed analysis of design for components failure modes
- detailed analysis of operations for potential human errors
- known or pre-established undesired outcomes or mishaps and following backward to hazards
- review and analysis of good design practices

- use of key state questions (what must the system always do, what it must never do).

1.3.5 Hazard reduction order of precedence

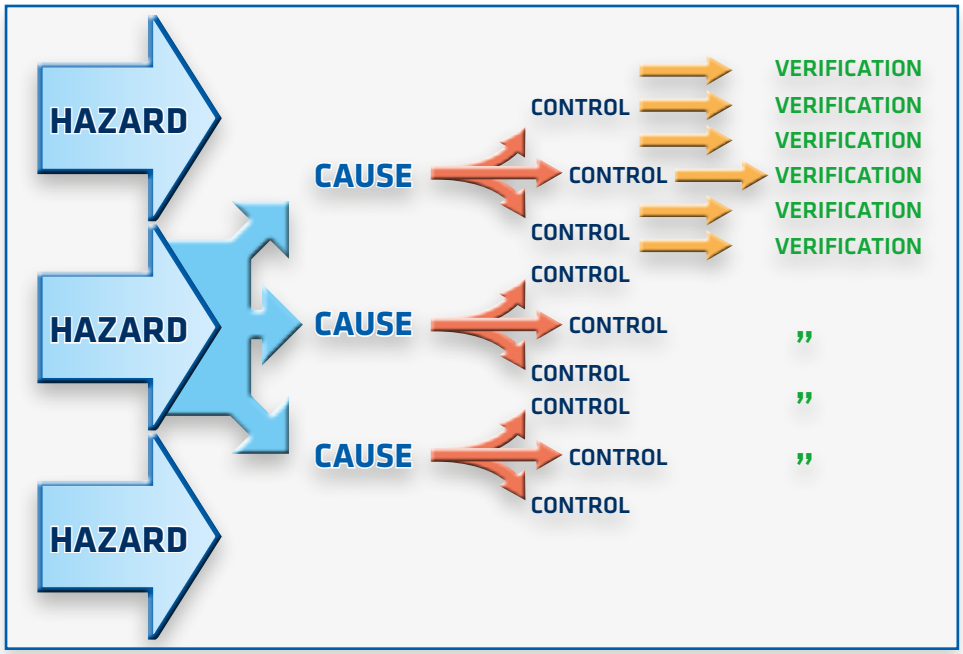
Actions to eliminate hazards or control the risk are undertaken during the design in the following order of precedence:

a) eliminate the hazard
b) develop design solutions and/or use safety devices
c) provide detection and warning/ caution means
d) develop special procedures and training (including personnel protective equipment)

A lesser degree of desirability exists for each succeeding method.

1.3.6 Hazard elimination and limitation

Hazards oftentimes can be eliminated by the proper selection of a design solution. For example, the choice of a nominal air atmosphere for a spacecraft instead of one of enhanced or pure oxygen greatly diminishes the risk of fire. As another example, designing a pressure vessel to leak-before-burst avoids the potentially violent rupture and fragmentation that can cause additional damage, disable redundant systems, or injure a crewmember. Often, however, a hazard cannot be eliminated without concomitant loss of some major system functionality. Still, the level of a hazard can be limited by proper selection of design parameters. For electric power distribution efficiency, a high voltage system can be selected. However, if the power distribution system is designed so that the power is converted locally to provide low voltage at most electric outlets utilized by the crew, the risk of electric shock is limited.



Hazard Analysis sequence from hazard identification and hazard causes determination to hazard controls (design controls and/or operational controls) and relevant verifications.

1.3.7 Hazard design controls

In the development of a system, safety is designed-in through a combination of hazard controls and relevant verifications that are identified by hazard analysis.

Barriers, inhibits and interlocks

Barriers, sometimes called inhibits for certain applications, are a means for physically isolating a hazard. A barrier can be a physical interruption between an energy source and some function, a means of separating incompatible materials, or for isolating materials that when mixed would constitute a hazard (Musgrave, Larsen, Sgobba 2009).

Shields used to protect a spacecraft from meteoroids and orbital debris are safety barriers. They perform an energy absorption function, thus preventing impact damage to the vehicle and its systems. This is similar to the concept of structural containment, which is used as a means of protection for rotating items. Other examples of barriers are the use of relays between a battery and a pyrotechnic initiator, and a latch valve installed between a propellant tank and thrusters. It is important to realize, however, that commands, personnel, computers and software, panel switches, and procedures are not inhibits, and should not be considered as such in any design.

In the case of fire, combustion requires the presence of a fuel, an oxidizer, and an ignition source. Isolating any one of the three from the other would effectively prevent a fire. The use of a slightly pressurized inert gas, such as nitrogen, in leak tight fuel container represents an effective barrier to prevent air from coming into contact with the combustible fuel.

Some materials and compounds possess harmful characteristics such as toxicity or radioactivity. In such cases, barriers selected during design can be in the

Fail-safe Design

- ***Fail-passive:*** The equipment is automatically de-energized, and ceases operation until corrective actions are taken. Fuses and circuit breakers are typical fail passive devices
- ***Fail-active:*** The equipment remains energized. The design includes standby redundancy that maintains the system in a safe mode until corrective action is taken. Redundant fastener arrangements in structures are examples of fail active design
- ***Fail-operational:*** The failure causes the equipment to revert to a mode that allows continued operation in a safe manner; however, functionalities that would otherwise present an unsafe situation could be lost.

form of containers (isolating the material), or as masks and other protective gear and equipment (isolating the crew). In a microgravity environment, metallic chips and glass fragments are potentially harmful if inhaled. In such cases, barriers can take the shape of filters with adequately fine meshes. Additionally, metallic debris can cause shorts in avionics equipment, or become lodged in critical mechanisms. The barriers applied in this situation are comprised of layers of conformal coatings over electronic circuitry, or guards and enclosures placed over mechanisms.

Sometimes barriers are intended to be temporary, such as the use of interlocks to prevent inadvertent access or exposure when a hazard source is present. An interlock can be used to prevent access to an energized laser, rotating equipment, or high temperature surfaces by locking covers or access doors while power is applied. As well, interlocks can function by automatically removing the hazard source, e.g., power to a laser when a protective cover (another barrier) is removed.

Fail-safe design

The purpose of fail-safe design, basically, is to place a system in safe mode following some failure. In this safe mode of operation, some system functionality can be lost. Nevertheless, the primary intent is to prevent harm to people, and secondly to prevent further system damage.

There are three fail-safe design approaches, fail-passive, fail-active, and fail-operational. The option selected is determined by the specific purpose and functionality of the system:

Sometimes the term, fail-safe, is used as a synonym for redundancy, although in general these are different concepts. A fail-safe design does not maintain or ensure safety by enhancing system reliability. A fail-safe design, indeed, can be unreliable, and yet ensure safety.

Redundancies

Redundancies can be established at any product-tree level, including components and system functional level. Single-point-failures can be removed locally by implementing redundant parts, items or equipment, or more than one distinct, sometimes dissimilar, complete hardware/software functional chain is implemented for accomplishing a system function.

As general rule, “must-work” functions require system functional redundancies. In all other cases, single-point-failures can be mitigated by introducing parts, components, or equipment redundancies locally.

A redundancy is called hot (active) when redundant elements nominally are fully energized, and it is not necessary to switch in the redundant element or switch out the failed one. Conversely, a redundancy is referred to as cold (standby) when secondary or tertiary redundant elements are non-operative until they are intentionally switched into operation upon failure of a primary element.

An important general principle is that all redundancies (as well as inhibits and barriers) included within a design must be verifiable. It is essential that redundancies are independent, in the sense that no single credible failure, event, or environment can eliminate more than one.

Redundancies are used for safety and also to enhance mission success. It is generally accepted that by implementing a number of independent safety redundancies as a protection against the possible consequences of a failure, i.e., whether they are catastrophic or critical, the overall risk associated with operating the system becomes acceptable because the event probability becomes more remote.

Design for minimum risk

Design hazard controls, other than those utilizing redundancies and barriers, meant to avoid failure fall collectively within a category called design for minimum risk. These requirements rely upon safety factors and safety margins established by analysis and test, past experience, and international safety standards to ensure an established level of acceptable risk. Cases in which design for minimum risk is appropriate for use include structures, pressure vessels, pyrotechnic devices, flammability, and design for electromagnetic compatibility.

The concept of design for minimum risk is probably the earliest design method used to minimize failure probability. It typically results in overdesign to

account for various uncertainties encountered such as environmental conditions, analyses and test methods, materials variability, and manufacturing processes variances. For the engineer, overdesign essentially is a way for distancing the statistical distributions for cumulative stress and strength curves that are not known with requisite precision, thus preventing them from overlapping. Safety factors and safety margins change and are refined as our knowledge in pertinent areas advances.

The equivalent concept in electronic design is sometimes called fault avoidance. It consists in reducing the possibility of a system failure by increasing the reliability of individual items through the use of electrical design margins, derating criteria, high reliability components, application of workmanship standards, et cetera.

if CABIN FIRE:

10. CAB FAN A,B (two) – OFF (max 20 min)
11. Locate source (see matrix, facing page)
12. Unpwr source of smoke

If smoke persists or source cannot be unpwrd:

WARNING
Discharge is propulsive

13. Discharge handheld FIRE EXTGHR

If Ascent:

14. Post MECO, go to POST-FIRE CABIN CLEANUP (ASC PKT, ECLS) >>

If Entry and prior to TIG:

15. Go to ECLS FRP-3, FIRE/HAZ SPILL O2 CONTROL, step | 3 (MAL)

Shuttle cabin fire-fighting flight procedure.

1.3.8 Hazard operational controls

An operations hazard control (e.g. the action of removing power, or performing an inspection, etc.) can be defined as the control of a hazard by crew real-time action either on the basis of procedures, or through the implementation of a preplanned decision by the flight control team, so-called flight rules. Sometimes, special crew training is used as operational hazard control too. Operational hazard controls should be allowed only when an alternate means of reduction or control of a hazard by design is not available. Criteria for evaluating operational hazard controls are:

- It can be accomplished by the crew
- There is sufficient time available for performing it
- There is sufficient telemetry available to monitor its execution
- It does not create new hazards.

Crew procedures, also called flight procedures, are the primary method used for an operational control. Generally, procedures and checklists are meant as memory aids to help the crew avoiding errors such as missing a step of a task or altering its sequence. When a procedure includes an operational hazard control, it will specify:

1. What the procedures is for
2. When it must be performed
3. What are the step-by-step actions
4. What is the correct sequence of actions
5. Warning note of hazard
6. Description of hazard control action (if not obvious)
7. Expected feedback and/or accept/reject criteria (if applicable)

Flight rules are the secondary method used for implementing operation hazard control. They are also used to guide reactions to unexpected events. Flight rules are normally used for items that cannot be contained in a nominal crew procedure. For example, suppose that a hazard is identified that a payload transmitter on a space station would interfere with the docking system of a visiting vehicle in its proximity. The developer may identify an operational hazard control consisting in switching off the transmitter at a certain time during the rendezvous operation. The proposed control would be evaluated by safety, engineering and operations experts and if agreed a Flight Rule would be issued by the Flight Control Team to ensure that the crew will be instructed to power off the transmitter prior to proximity operations. Mission planners would ensure that the crew's plan contains these activities explicitly when required (Barriero, 2010). Over the course of several missions, the specific details of the constraint may change like the number of transmitters to be turned off, or the specific operations that require transmitter turned off.

1.3.9 Safety technical requirements and criteria

Safety requirements and criteria are used to inform the designer about the acceptable level of risk control that the system must achieve. Safety requirements and criteria can be grouped under two broad categories of *Failure Tolerance*, and *Failure Avoidance*. In addition,

certain contingency response capabilities, for example for allowing escape, are included.

Failure-Tolerance criteria refer to the ability of the system to maintains through the designed-in characteristics prescribed functions or services to users despite the existence of failures or faults. *Fault-Avoidance*, used when Failure tolerance is not doable, consists instead in reducing the probability of a failure or fault by increasing the reliability of individual items (design margins such as factor of safety, designing to worst case scenarios, materials selection, use of hi-reliability components, de-rating, quality control, testing, etc.). Fault avoidance is generally achieved through the use of proven best practices for the design of subsystems.

A system is made safe by implementing hazard controls (i.e. redundancies, barriers, safety factors, etc.) and capabilities to prevent, tolerate, and mitigate hardware failures, software faults, and human errors. Differently from evolutionary industries like aviation and shipbuilding, in space projects those safety features are not prescribed by detailed safety codes or regulations but left to be selected and developed by the designer through hazard analysis in compliance with the prescribe level of risk control. The resulting design and operational solutions (hazard controls) are relevant verification methods are then carefully validated for compliance with safety requirements and criteria by an independent multi-disciplinary panel of experts.

Typically, safety requirements and criteria for a space program (i.e. including a large variety of systems from a coffee machine to a robotic arm) are collected in a single safety standard that addresses the following topics:

- Hazard severity categories (catastrophic, critical, marginal)
- Failure Tolerance requirements (driven by hazard severity categories) (*must-work/must-not-work* safety-critical functions, commands, etc.)
- Failure Avoidance (i.e. Design-for-Minimum-Risk) (structures, materials, avionics/EEE, mechanisms, RF emission etc.)
- Environment and Habitability (noise, life-support system, thermal hazards, sharp edges, etc.)
- System Capabilities (hazard detection/annunciation/ safing, abort/escape, fire detection, etc.)
- Safety Analysis/Certification Process

Safety requirements and criteria are used to inform the designer about the acceptable level of risk control that the system must achieve

1.4 SAFETY MANAGEMENT SYSTEM

The *Safety Management System (SMS)* is the systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.

1.4.1 Organizational requirements

The top management of a system developer and/or operator must demonstrate leadership and commitment to the development, implementation, maintenance and continual improvement of the Safety Management System. The top executive must retain ultimate responsibility for the performance of the safety activities and must have ultimate control over the financial and human resources required for the safety activities. The top executive must designate sufficient safety management personnel

The top executive must retain ultimate responsibility for the performance of the safety activities and must have ultimate control over the financial and human resources

who, on his/her behalf, are responsible for coordinating implementation, maintenance, and integration of the Safety Management System and regularly report to the top executive on the performance of the SMS and on any need for improvement.

The responsibilities, accountabilities and authorities of staff having a role that affects safety (including management and other staff involved in safety-related tasks) must be defined at all levels within organizations involved in system development and operation, documented, assigned and communicated. The staff with delegated responsibilities for safety related tasks shall have the authority, competence and appropriate resources to perform their tasks without being adversely affected by the activities of other business functions. Delegation of responsibility for safety-related tasks shall be documented and communicated to the relevant staff, accepted and understood.

1.4.2 Identifying, documenting, and validating system hazards

The system developer/operator must develop and maintain a process to iteratively identify system hazards as integral part of the system design, development, and operational processes, starting with the conceptual design phase. Must analyze the systems functions, in the worst environment conditions and with reference to the operational scenario, to assess their safety criticality. The functional system analysis and other detailed analysis must be used to identify hazards, and in developing and implementing risk controls.

The key concept applied in space programs is that the safety authority sets safety policies, while the program establishes relevant safety requirements and criteria and develops the most appropriate design solutions and verifications. In other words, the safety authority defines where the limit lies between “safe” and “unsafe”, but it is the developer, having the best knowledge of system design and operations, who defines the design safety features and operational procedures.

Because of the generic nature of safety requirements, the design solutions need to be validated by the developer through an analytical process using techniques like hazard analysis, Fault-Three Analysis, etc. and checked trough an independent peer-review.

Safety Data

The resulting detailed safety design and verification requirements (i.e. hazards controls and relevant analyses, tests, inspections, demonstrations, will be documented and tracked in a safety data package (sometimes called safety-case) that usually includes:

a) summary description of the system, and operational environment;
b) identified hazards in the system and their severity;
c) safety requirements and criteria applicable to a specific hazard;
d) possible causes of each hazard;
e) description of how hazard causes are controlled (i.e. eliminated or mitigated);
f) description of relevant verification plans, procedures and methods for each control.

Risk Management and Acceptance

Intrinsic in the concept of a standard is that compliance must be assessed and enforced, otherwise the requirements become simply a set of guidelines. Monitoring and enforcement can be done by any party to which such authority belongs or is assigned. Such organization must have the following three key prerequisites: authority, competence, and independence (from the specific project or program).

The safety review process consists in the independent verification that a system has been designed in compliance with applicable safety requirements, that hazard controls have been duly implemented during manufacturing, integration and operations preparation, and that hazard controls verification were carried out successfully. Requirements on type, content and submission schedule of safety data to be review, are established by the safety authority.

During the safety reviews process, safety data are examined by the safety review panel, sometimes called safety review board, which is a multidisciplinary team of independent representatives from different technical and functional areas providing a spectrum of knowledge on system safety. The safety panel is typically composed of experts in various fields of engineering and science such as structures, software, mechanisms, materials, electrical and power subsystems, toxicology, biology, medicine, and of representatives from organizations such as flight and ground operations, integration, and astronaut office. Members of the safety review panel have individual responsibilities to provide the consolidated assessment of their specialist organizations, and collective responsibility

Intrinsic in the concept of a standard is that compliance must be assessed and enforced, otherwise the requirements become simply a set of guidelines

to support discussion and coordination of all review findings and recommendations. Panel members advise panel chair (or co-chairs), who holds delegated decisional responsibility. Upon successful completion of a safety reviews cycle, the chair(s) will issue a formal statement of safety system compliance.

Safety reviews are carried out incrementally in phase with design and development activities. For such reason, they are called phased safety reviews. Safety reviews are often identified sequentially with 0, and Roman numerals I, II, III. Safety reviews are carried out either immediately before or after project reviews, depending on considerations of potential impact on design if some hazard controls are changed, rejected, or modified.

Phase 0 Safety Review is held during the conceptual phase of design. Phase I follows at the time of project Preliminary Design Review (PDR). Then Phase II at the time of project Critical Design Review (CDR), and finally phase III at completion of successful verification of hazard controls implementation.

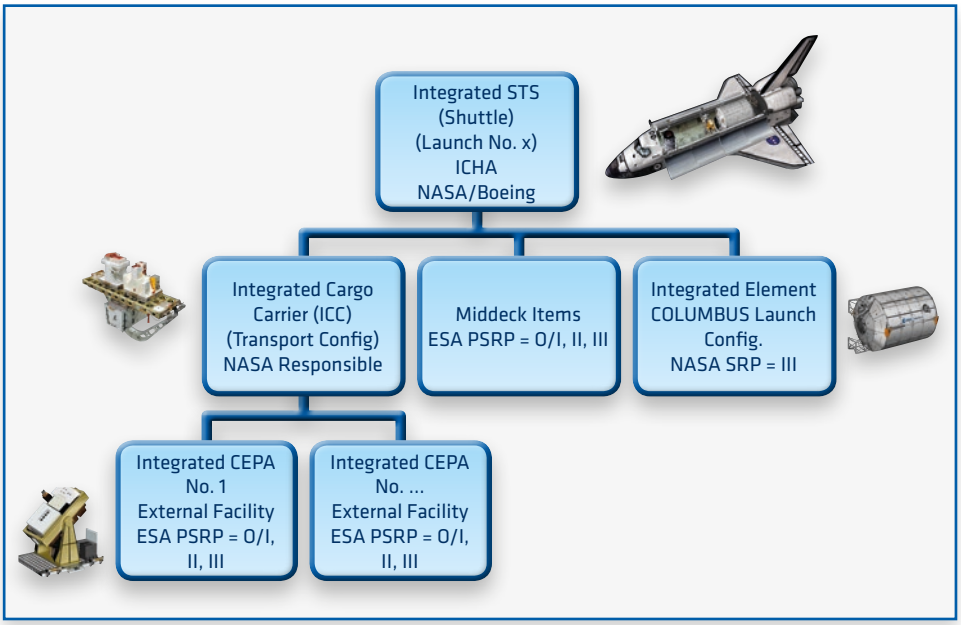
Safety data are the input to safety reviews. They consist of hazard reports and supporting data, becoming more and more detailed as project design and development activities progress.

At Phase 0, safety data are limited to the identification of hazards and applicable safety requirements. At Phase I, due to design evolution since the conceptual phase, new hazard reports may be presented for review while others may be cancelled. The Phase I hazard reports will document all hazard causes while design and operational hazard controls are presented in a preliminary form. At phase II safety review, all details on design hazards controls and approved operational hazard controls are presented for review, together with hazard controls verification plans and procedures. Finally, at phase III safety review, the results of safety verification activities are presented.

Safety reviews are carried out not only in phase with system design and development, but also at several levels of integration with other systems, depending on complexity. Take for example the international Space Station habitable units called modules. Each module reached orbit separately on-board Shuttle or Russian rockets to be integrated on-orbit. Each module accommodates various kind of scientific instruments, research facilities, and system equipment, which are developed by different organizations and according with different timelines. Each ISS module had its own cycle of system safety reviews, followed by integrated safety reviews at various levels of integration of instruments, research facilities and equipment. Finally, an integrated safety review cycle follows at level of overall space station on-orbit configuration. Similarly, for the transportation of each module by Shuttle, an integrated safety review cycle was carried for Shuttle in transport configuration with the integrated module in transport configuration, and other payloads in the cargo bay, as shown in the figure here below.

Because new instruments and equipment are continuously sent to ISS and other are returned or disposed, every time the configuration of the space station changes, in particular in conjunction with departure and arrival of transport vehicles, a new cycle of integrated safety reviews is carried out.

In the following chapter we will see how safety standards emerged at NASA in response to specific needs of the Shuttle Programs and International Space Station Program. We will see how goal-oriented safety requirements and criteria have emerged and evolved from early concepts of human rating, and how they are documented. We will see also the relationship between safety standards and technical standards and how they are used in combination.



Shuttle Integrated Safety Review Process - European Payloads Transported in Cargo Bay and Middeck Lockers.

Chapter 2
EVOLUTION OF SYSTEM SAFETY AT NASA

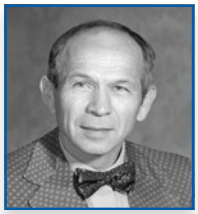
2.1 HUMAN RATING

The early NASA approach to human spaceflight safety (called man-rating at the time) consisted on adapting military rockets for crewed missions. The driving considerations were:

- Safety during launch
- Satisfactory operation within human-factors tolerances
- Adequate performance margins for mission reliability

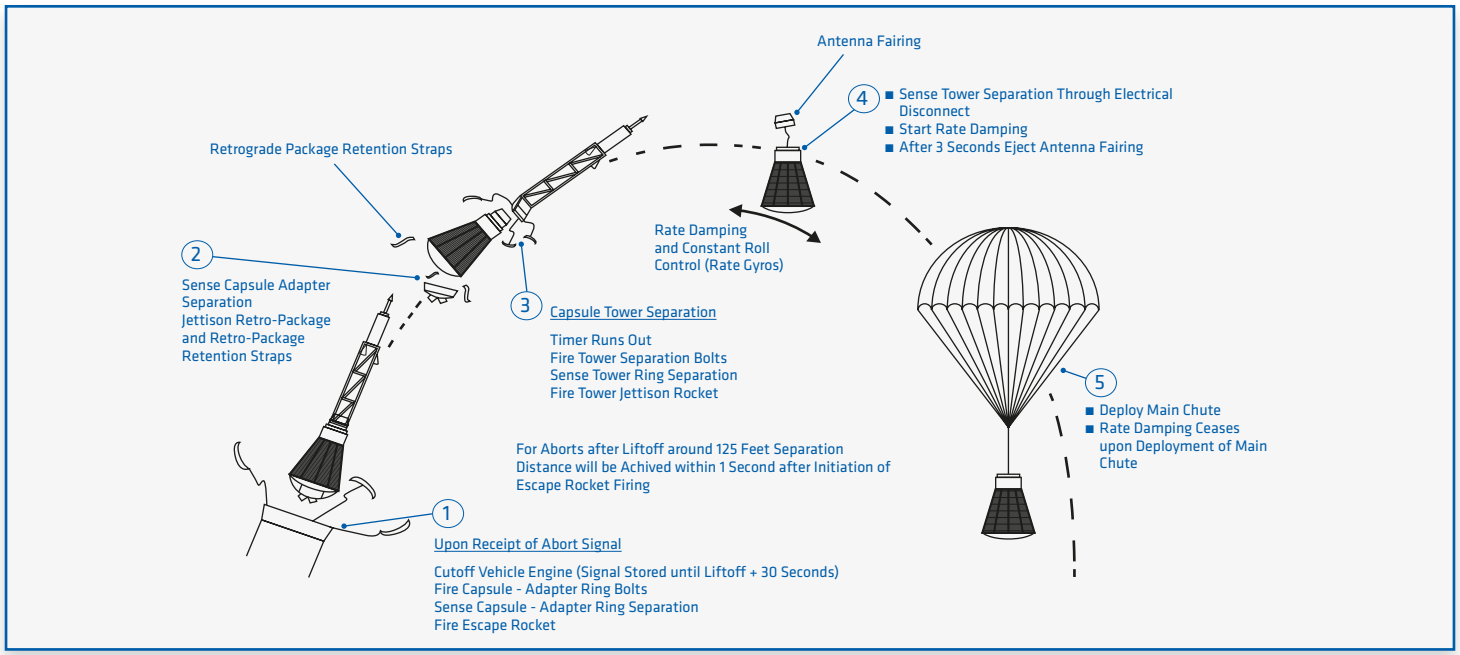
The key idea was to lower the risk of loss of crew (LOC) caused by launch vehicle malfunctions by providing abort capability, so-called emergency or launch escape system, from the time of astronaut boarding through capsule separation. In addition, performing extensive ground and flight tests at components, subsystems and system level to identify changes and modifications to improve system reliability.

The key idea was to lower the risk of loss of crew (LOC) caused by launch vehicle malfunctions by providing abort capability



Dr. Maxime A. Faget
Launch escape system inventor.

Space systems human rating concepts have evolved from the narrow scope of adapting existing rockets for human spaceflight use, to the current encompassing human-centered approach of designing the system to ensure human protection, to account for human limitations, capabilities and performance, and to accommodate human needs.



Mercury-Atlas Launch Escape System (NASA).

First suborbital human spaceflight almost 60 years ago

In 1961, Alan Sheppard on a suborbital flight reached **187 km** of altitude on board the first Mercury. A capsule on top a man-rated Redstone 3 rocket.

In 1963, NASA test pilot Joseph Walker reached an altitude of **108 km** in an X-15 aircraft, and returned to the runaway from which he took off (attached to a B-52 mother ship).

2.1.1 Launch abort system

In 1958, Maxime Faget developed at NASA the concept of safely aborting flight using a dedicated rocket to remove the capsule from the launch vehicle. The most challenging failure scenario, which ultimately determines the design of a launch abort system, is the explosion of the rocket right on the launch pad. Generally, in such situation, ejection seats cannot guarantee to reach almost instantaneously a safe distance from exploding rocket fireball and shrapnels. The configuration Faget conceived used a tower on the top of the crew capsule to house solid propellant rockets. Sensors would detect potentially catastrophic launch vehicle malfunctions, terminate the flight by shutdown of propulsion, and quickly separate the capsule to a safe distance from the rocket.

NASA Mercury was the first human spaceflight program of the United States, running from 1958 through 1963. Mercury was the first to use a launch escape system (LES) on two different military rockets modified for human spaceflight: Redstone for the early suborbital flights, and Atlas D for orbital flights.

In 1963, Russians, which had previously used ejection seats on Vostok, developed a similar 'tractor' tower escape system for Soyuz. Curiously, at the same time NASA went the other way by developing ejection seats for Gemini-Titan II that included a special feature called rocket catapult (ROCAT) to propel the seats to a safe distance (Ray, Burns 1967). The following NASA Apollo program to land man on the Moon went back to a launch escape system based on Faget tractor configuration.

An important choice in designing an abort system is between automatic and manual control. For Mercury, an automatic abort sensing and separation system was selected since some emergency conditions could develop too rapidly to permit manual activation of the abort command. The automatic system would relieve the astronaut, whose performance under flight loads was not well established at the time, from the requirement to monitor and sense all emergency situations. However manual activation from ground, and by crew on-pad (from umbilical drop until ignition), was also possible.

In April 1961, during an unmanned Mercury flight test, the rocket guidance system failed. The range safety officer activated the capsule launch escape system from ground by manual radio command to terminate the flight to avoid risk on ground, and to test the system. Years later, in 1983, Russian activated a Soyuz LES by manual radio command from ground while the rocket was still on the launch pad. A fire had engulfed the base of the rocket burning the LES command cables used by crew and ground. The capsule was successfully separated before the Soyuz rocket exploded.

The NASA Gemini program used manual abort command, which proved its value on Gemini VI mission when the engines ignited, but after about 1.5 seconds of operation, they abruptly shut down. Mission rules dictated immediate activation of the ejection seats. However, Schirra, the commander, did not feel any movement and knew that the launcher hadn't lifted, so he decided to not abort, thus saving the mission.

Nowadays. Chinese Shenzhou, and NASA Orion both use a tractor rocket powered configuration for LES, which is jettisoned during flight, instead SpaceX Dragon commercial crew transportation vehicle uses a liquid fueled 'pusher' launch abort system integrated into the capsule. Boeing uses a similar pusher abort system on its commercial CST-100 capsule.

2.1.2 Early programs

In early space programs, system safety was essentially considered to coincide with system reliability, plus abort capability. Some hazards mitigations were introduced sporadically on an opportunistic basis. For example, the toxic Hydine (60 percent UDMH, 40 percent diethylene triamine) used on military Redstone, was replaced by alcohol, because it was unsafe for the astronaut in the event of a prelaunch emergency egress.

The low reliability of military rockets was acceptable for their original mission but totally inadequate for crewed spaceflight. Although low, military rockets

reliability was proven, being the result of on-going maturation through actual operations. Before Mercury manned missions, Redstone rockets had been already launched 37 times and Atlas rockets 100 times. Furthermore, many components were originally designed to mission parameters exceeding those required for manned missions. Therefore, programs were reluctant to introduce design changes, unless mandated by mission needs, due to concern of inadvertently degrading the rocket reliability instead of improving it. Redundancies where mainly used on the new abort system in order to overcome the potential problems of false abort signal (mission loss) or undetected actual abort conditions (loss of crew). For the rest, the pillar of the reliability program was a massive campaign of subsystems and components environmental tests to validate existing design and changes, with margins added to operational environment. A stricter quality assurance program was putted in place to prevent human errors during manufacturing, integration and operations going undetected.

Starting with the Apollo program the term "man-rating" took a different meaning. No longer referring to the adaptation of existing unmanned rockets, but to indicate that a system (rocket and capsule) had been developed for crewed missions. Until Apollo 1 ground fire accident, the two tenets of the man-rating approach remained, the use of abort system and reliability program.

The Apollo reliability program was based on different considerations with reference to previous NASA programs. No longer about improving reliability, but on designing reliability into a new system. The approach adopted by NASA was a smart synthesis of two competing approaches, statistical techniques and engineering judgement respectively. which had been at the center of a heated debate. The statistical approach rested on the concept of building system reliability through an iterative process that started with top-down apportionment of system reliability quantitative target to subsystems and components, followed by determination of failure rates at components level by statistically significant number of tests, and finally bottom-up verification using mathematical models to assess the achieved reliability at subsystem and system level. Instead, the engineering judgement approach emphasized, in the words of Von Braun, "an almost religious vigilance and attention to detail on the part of every member of the development team". Meticulous search for errors in design, "testing to failure" to expose hidden flaws, effective corrective actions system, and strict quality control. The synthesis of the two approaches consisted in the use of a combination of quantitative and qualitative reliability analyses (e.g. failure modes and effects analysis, criticality analysis), use of failure avoidance techniques (simplicity, derating, large safety factors, use of approved parts, etc.), implementation of redundancies, and finally performance of extensive design reviews and qualification and acceptance testing at all levels (Sperber, 1973).

Being understood that methods to quantitatively assess the reliability of the design where not precise enough, due to the limited amount of data, numerical values were considered as guidance to judge the adequacy of the design and not as true measure of system reliability. Quantitative analyses were relegated to initial trade-off studies during the conceptual design phases of hardware development.

Removal of single point failures (SPF), as far as feasible, through the implementation of redundancies and inhibits was the main reliability requirement driving the Apollo program design activities. The redundancy philosophy of Saturn V rocket consisted essentially into "engine-out capability" for the first stage, plus redundancies for the guidance system (triple modular redundancy), flight termination system, and abort system sensors (NASA, 1968). More extensive use of redundancies was made on the Apollo spacecraft modules.

Awareness that safety could not be achieved solely by combination of abort system and reliability program dramatically emerged with the Apollo 1 fire that killed three astronauts during ground testing at Kennedy Space in January 1967. Within few months, an Apollo system safety program was mandated by NASA Headquarters requiring to perform formal hazard analyses of system, and ground and flight operations. The activities started with the compilation of a list of "potential accidents" from the time the astronauts entered the launch pad until splashdown and recovery of the capsule. The "potential accidents" were prioritized based on program experience, mission phases criticality, and

Within few months, an Apollo system safety program was mandated by NASA Headquarters requiring to perform formal hazard analyses of system, and ground and flight operations

expectations of likelihood of occurrence. Besides hazards analyses, several safety studies were undertaken on flammability testing, selection of materials, prevention of damages to electrical wiring, fire suppression etc. Even the paper chosen for on board procedures, handbooks, and manuals was of a special one difficult to burn.

The Apollo accident happened around the time when techniques for human error prevention and control had become commonplace in aviation and had started to be applied extensively to consumer goods too. After 1965, consumer goods manufacturer's liability was no longer limited to the case of a product that was "unsafe for its intended use," but included the case of a product "unsafe for an unintended but foreseeable misuse".

Safety analyses conducted after the Apollo accident included consideration of the human element limitations and capabilities. The handbook Boeing prepared for NASA on the execution of safety analyses stated as follows:

"A study of man-machine relationships complements system safety by providing additional emphasize on human error analysis and error reduction. These are critical considerations in determining potential system modes that can result in hazardous conditions. Identification and analysis of the overall hazardous consequences of a given failure event require an understanding of human capabilities and limitations as well as the interfaces between subsystems, systems, and environments. Man-machine relationship to be effective must be integrated with system safety to provide a logical and consistent continuum throughout the lifespan of an aerospace system" (NASA, 1969).

Main safety requirements and risk mitigation best practices later used on Skylab and Shuttle programs were traceable to the Apollo post-fire safety program. Skylab, for example, was the first U.S. program to transition to a two gases atmosphere instead of pure oxygen, which was studied in the aftermath of Apollo 1 fire but not implemented due to major design impact.

The Hubble Telescope was one of the most notorious Shuttle payloads.

2.1.3 Shuttle payloads and ISS

The NASA Shuttle program, officially known as National Space Transportation System (NSTS), was announced by President Nixon on January 5, 1972. The Shuttle was considered at the time the reusable launch system of the future, promising to revolutionize launch availability and costs.

All kind of users were expected, from government agencies to commercial customers and other NASA programs.

As Shuttle development was progressing, NASA started to work on payload accommodation, interfaces, and safety requirements. A wide variety of payloads were expected including many that had never been flown before in space. The Shuttle cargo bay was sized to accommodate entire satellites like Hubble telescope, Galileo and Ulysses, plus rocket upper stages, or habitable modules like SpaceLab and SpaceHab. Smaller payloads, research facilities and experiments would be accommodated in lockers in the pressurized crew compartment or in dedicated canisters called Get Away Special (GAS) externally in the cargo bay. For such reason, the safety requirements had to be encompassing but generic and performance oriented.

Shuttle payloads preparatory activities started with work on safety and interface requirements, payload integration process, and implementation guidelines. The work included preparation of so-called interpretation letters (because of their letter format) meant to be advisory. With safety requirements being mainly generic and goal oriented, there was the need to help Shuttle customers understand purpose and rationale of some requirements, and to advise them on possible design solutions that could be acceptable, but without imposing them. Verification requirements (i.e. analyses and/or tests, inspections, and

Potential catastrophic hazards required two-fault-tolerance, while critical hazard required single-fault-tolerance

demonstrations) were also defined as well as guidance for the preparation of payloads verification plans.

For customers' benefit, the Shuttle program created also documents describing available payloads accommodations for electrical power, cooling, or safety inhibits like switches and valves that could be made available (upon negotiation) on the Orbiter side to help meet some safety requirements levied on payloads. Whole series of technical standards, support standards, and handbooks were developed to help customer design and verify their systems and to plan operations. Those standards covered structures, mechanical systems, batteries, pyros, wiring, safe distances for firing payloads propulsion system, etc.

In establishing payloads safety requirements, the Shuttle program decided to take some "comfort margin" or in other words to be more conservative than was the case for the Shuttle systems. This was not meant to be a penalty but the price to be paid for allowing design freedom to payloads developers. For example, for Shuttle systems, rigorous requirements were applied on procurement, selection and testing of EEE components, on software development, on quality control, and on configuration management, but payload developers could use whatever EEE components they considered suitable, their own software development methods, etc. In the case of small enterprises or universities, it was even expected that they could lack familiarity with basics of quality control and configuration management. Overall, it was a matter of trading reliability for cost. Payloads failures were deemed acceptable as long as they did not affect safety.

The classification of 'hazard severity' was used to drive the amount of fault tolerance required for Shuttle payloads. Potential catastrophic hazards required two-fault-tolerance, while critical hazard required single-fault-tolerance. A critical hazard was defined as potentially resulting in injury to the crew or impairment to the vehicle or the mission. A catastrophic hazard could lead instead to loss of life, a life threatening or permanently disabling injury, or an occupational illness. Loss of major flight elements or ground facilities can also be classified as catastrophic. Critical consequences were defined as those causing temporary disabling injury or occupational illness, use of contingency or emergency procedures, or damage to equipment.

The required fault-tolerance level depended on safety criticality of payloads function, and on severity of hazards. In general, payloads do not have 'must-work-function', (i.e. active functions vital for keeping the crew alive) but often include 'must-not-work functions', which are functions that if operated inadvertently or untimely (e.g. access to a live high-power laser) can kill or injury the crew, or cause damages. Payloads may include some inherent hazards such as high voltages, high temperature, toxic compounds, etc.

An important concept was to assume that payload software was zero-fault-tolerant thus counting it as providing only one level of hazard control. All additional controls had to be hardwired, unless payload developer opted to apply the same strict software development and independent verification and validation processes required for Shuttle systems software. In other words, the possibility to achieve two-fault tolerance (i.e. triple controls) by computer only was basically

The following fault-tolerance levels were levied on Shuttle payloads

- Safety critical system had to be two-failure tolerant. This criterion applied to "must work" systems.
- Inadvertent operation of safety critical system functions had to be controlled by a minimum of three inhibits. One of these inhibits had to preclude any operation by an RF command. The ground return for the circuit of the safety critical function had to possess the capability to be interrupted by one of the three inhibits. As well, at least two of the three inhibits had to be monitored.
- No combination of two failures or operator error could result in catastrophic consequence.
- No single failure or operator error could have critical consequence.

NOTE: In this report the terms 'fault-tolerance' and 'failure-tolerance' are used interchangeably. One refers to an event (failure), the other to a status (fault),

discouraged. (The Shuttle system relied extensively on computer control of many 'must-work-functions'. For example, the flight control system had four redundant computers plus one back-up to be fail-operational/fail-safe).

The 'margin of comfort' approach for payloads safety consisted essentially in requiring up to two-fault-tolerance and larger safety factors for hazard controls, and applying some conservativism when classifying the severity of a hazard. For example, structural failures and pressurized systems failures where always classified as 'catastrophic'. Some conservativism was applied when classifying the toxicity of chemical compounds too.

Following the Shuttle Challenger disaster, NASA decided to deemphasize the commercial use of the Shuttle Program and leave commercial customers to fly on expendable rockets.

Commercial customers had been a central consideration when establishing the Shuttle payloads safety requirements. Now the Shuttle was expected just to serve other NASA programs. Payload safety requirements may have been different if this had been known from the very beginning. However, the wisdom of using generic goal-oriented safety requirements was confirmed when an unexpected Shuttle customer appeared, the Russians, and later when development of the space station started.

In 1994, NASA agreed with Russians to use the Shuttle to deliver a Russian docking module to the Space Station Mir. So the Russian docking module became a Shuttle payload and had to comply with the relevant safety requirements. What NASA learned by reviewing the Russian design was that the Russians had a robust and safety-minded design, which had been thoroughly tested. It was not difficult to show that it met Shuttle payloads safety requirements because they were not prescriptive. But there was more come!

In 1984 the U.S. began developing Freedom, a permanent manned space station, and called upon the G7 Group of countries to join in the program.

Mission	Description	Safety Approaches/Goals Mission Duration	Main Human Rating Techniques
Mercury	Suborbital proof of concept and single crewperson orbital operations	No Single Failure results in Loss of Mission. No Single Failure during an abort results in Loss of Crew. Short duration mission: hours to days	Launch escape system. Single electronics unit with crew based diverse manual backup systems. Ground support from centralized control center to guide operations and support anomaly resolution.
Gemini	LEO, proof of concept change of orbit/rendezvous and docking in preparation for lunar landing missions	Probability of Mission Success: 0.95 Probability of Safe Crew Return: 0.995 Medium duration missions: days to 2 weeks	Launch escape via ejection seats. Single electronics unit with crew based diverse manual backup systems. Redundancy (incl. functional) for all systems effecting crew safety. Ground support from centralized control center to guide operations and support anomaly resolution.
Apollo	Moon rendezvous, landing and return	Probability of Mission Success: 0.95 Probability of Safe Crew Return: 0.999 Medium duration missions: 1-2 weeks	Launch escape system. Single electronics unit with crew based diverse manual backup systems. Three fuel cells and power buses Ground support from centralized control center to guide operations and support anomaly resolution.
Skylab	LEO Station	Long mission duration: years	Dual redundant computers. On-rbit maintenance. EVA. Ground support from centralized control center to guide operations and support anomaly resolution.
Shuttle	Space access, launch and return (sat. deployment/ LEO experiments platform), aircraft-type return and landing. Reusable vehicle	System: Fail-Safe including Aborts. Avionics: Fail-Operational, Fail-Safe, two Fault-Tolerant. Medium duration missions: 1-2 weeks	1st stage launch escape not possible, only first flights provided ejection seats. Capability to return to launch site and to land at trans-Atlantic abort landing sites. Triple and quad redundancy. On-orbit maintenance. EVA. Ground support from centralized control center to guide operations and support anomaly resolution.
ISS	LEO Station (experiments platform). On-orbit assembly proof of concept	Two Fault-Tolerant, Fail-Operational, Fail-Safe. Designs for Minimum Risk (where Fault-Tolerance not possible). Long duration missions: decades	Safe-haven, crew escape vehicles. Redundancies. On-orbit maintenance. EVA. Ground support from centralized control center to guide operations and support anomaly resolution.

Comparison of historical safety approaches, goals and techniques (adapted from Miller, J., 2008).

In 1993, the Clinton Administration decided to broach the subject of cooperation to construct the International Space Station (ISS) between US and Russia, together with the international partners of the previous Freedom station program, Japan, Europe, Canada, and Italy. In 1998, the on-orbit construction of ISS began.

When NASA started discussing with partners the safety requirements for the future ISS systems, certain similarities with the early considerations about Shuttle payloads emerged. A large number of ISS elements would be developed at remote locations, not under direct control of NASA, and by following to a large extent local technical standards. In addition, all modules and payloads except those from Russia would be transported to the International Space Station by Shuttle and had therefore to comply with Shuttle payload safety requirements. It was the best interest of everybody that safety requirements of ISS would not conflict but complement those of Shuttle payloads. The solution was to adopt Shuttle payloads safety requirements for ISS systems and payloads with some tailoring.

For all previous U.S. space programs, including Shuttle, safety requirements were embedded in systems specifications. For the International Space Station, for the first time, safety requirements were established as a separate, dedicated standard.

2.1.4 Current NASA Human-rating program

In 2005, NASA issued the policy directive NPR 8705.2C on "Human-Rating Requirements for Space Systems", which establishes technical and certification requirements for any space system developed and/or operated by or for NASA, that support human activity in space and that interacts with crewed human-rated space systems such as vehicles, space suits, planetary bases, planetary rovers, and surface vehicles (NASA NPR 8705.2C).

The NPR 8705.2C directive is the synthesis of lessons learned over more than 50 years of human spaceflight

The NPR 8705.2C directive is the synthesis of lessons learned over decades of human spaceflight. The key tenets are:

a) protect human life;

b) integrate human as "master" system, taking into account limitations, capabilities, performance vulnerability, and needs; and

c) perform human-rating process throughout system lifetime, under authority, direction, and control of Agency's Administrator.

The human-rating directive makes applicable NASA's human system standards for crew health and human factors, which are directed at minimizing health and performance risks for flight crews. The standards set requirements for fitness for duty, human physical and cognitive capabilities and limitations, space flight permissible exposure limits, medical care, as well as human factors, and habitability. The standards consider human physiologic parameters as a system and therefore treats them as an integral part of the overall vehicle design process. The standard sets requirements for human-system integration where the context is about how the crew interacts with other systems, including the habitat and the environment.

Other standards that support and complement the technical human-rating requirements in the directive are not identified beforehand but left to the so-called Technical Authorities for safety, engineering and medical respectively to identify as program applicable baseline of safety, engineering, and medical standards.

The NASA human rating directive is structured in three parts:

1) certification process

2) certification requirements

3) technical requirements.

The human rating certification process starts with the approval of program maximum acceptable level of risk for crew, and long-term safety goals by NASA's Administrator. Continues with verification at program major development and operational milestones of progress in implementing the human rating requirements, and concludes with approval by the Administrator of the human rating certificate for the mission.

The appropriate implementation of risk reduction measures such as failure tolerance is responsibility of the program manager but during design he must follow a number of mandated human-rating processes and activities, such as:

1) allocation of safety goals and thresholds to mission phases and elements

2) definition of redundancy/back-up strategies, and level of failure tolerance

3) identification of crew survival strategies, and effective utilization of crew during emergencies

4) integration of safety analyses and system design

5) human-system integration, including evaluation of system design impact on crew workload, and human-in-the loop usability evaluation

6) design to prevent and mitigate human errors, and human error analysis of nominal and emergency operational procedures

Human-rating directive (top-level) technical requirements include traditional and new requirements. Traditional requirements such as automatic/manual launch escape system, failure/fault/human error tolerance or design for minimum risk, and provision for safe and habitable environment (protection from radiation, space debris, hot surfaces, high voltages, etc.) New requirements are mainly aimed at allowing human control of automatic systems. The human must have means to override system software, or to take manual control of space vehicle flight path and attitude unless not feasible (e.g. during atmospheric ascent phase).

2.2 SAFETY PANELS & SAFETY AUTHORITY

2.2.1 Safety Review Panel origin and evolution

Until Apollo 1 fire accident in 1967, there was no safety program at NASA and no safety organization. After the accident, hazards analyses were systematically performed, and safety divisions established starting with the one at Johnson Space Center.

Safety divisions fulfilled their function during system development through so-called 'concurrent engineering', consisting in the participation of representatives to various project reviews, but without safety playing an independent role in the decisional process. In other words, the safety organization had no independent voice and had to compete during project review meetings with engineering and operations representatives to have its own concerns addressed.

In January 1981, few months before the first Shuttle launch, NASA established the Senior Safety Board "…as a mechanism to periodic review of system and element level hazard resolution activities and for providing management visibility of open and accepted risk hazards". The board concentrated its efforts on reviewing Space Shuttle integration, cargo integration, and element-level open hazards, and review and approve of hazards closure rationale (Duarte, 2007). The board reported to the Johnson Space Center (JSC) Director of Safety, Reliability and Quality Assurance, and membership and chair were all from the safety organizations.

In 1986, after the Challenger disaster, the Aeronautics and Space Engineering Board that evaluated the Shuttle risk assessment and management processes stated in their report that: "The multilayered system of boards and panels in every aspect of the NSTS may lead individuals to defer to the anonymity of the process and not focus closely enough on their individual responsibilities in the decision chain. The sheer number of NSTS related boards and panels seems to produce a mindset of "collective responsibility" (National Academy of Sciences, 1988).They recommended that "NASA should periodically remind all NASA personnel that boards and panels are advisory in nature. He should specify the individuals in NASA, by name and position, who are responsible for making final decisions while considering the advice of each panel and board. NASA management should also see to it that each individual involved in the NSTS Program is completely aware of his/her responsibilities".

The Shuttle Challenger disaster investigation report branded the safety program as the 'silent program' to underline how little influence the safety organization had on the program.

In December 1988, NASA replaced the Senior Safety Board with the NSTS System Safety Review Panel (SSRP) "…as a mechanism of enhancing the Space Transportation System Safety Management and Engineering through informational interchanges, development of concepts to improve the STS Safety Program review of safety documentation, review of STS integration and cargo integration, review of STS element-level hazard identification and resolution activities, and recommendations to level II management for Hazards reports disposition".

The Silent Safety Program

The Commission was surprised to realize after many hours of testimony that NASA's safety staff was never mentioned…
No one thought to invite a safety representative to the January 27, 1986, teleconference between Marshall and Thiokol.
Similarly, there was no representative of safety on the Mission Management Team that made key decisions during the countdown on January 28, 1986…
An extensive and redundant safety program existed during and after the lunar program to discover any potential safety problems.
Between that period and 1986, however, the program became ineffective.
This loss of effectiveness seriously degraded the checks and balances essential for maintaining flight safety.

Report of the Presidential Commission investigating the Space Shuttle Challenger disaster (Rogers Commission).

In February 2000, the scope of SSRP was extended to include CIL (Critical Items List) dispositions, and identification and implementation of innovative risk management methods, but in the meantime, the panel reporting line had changed from independent to program.

According to Nancy Leveson, "In time, the Space Shuttle Program asked to have some people support this effort [SSRP] on an advisory basis. This evolved to having program people serve on the function. Eventually, program people began to take leadership roles. By 2000, the office of responsibility had completely shifted from SR&QA to the Space Shuttle Program."

After the Shuttle Columbia accident of 2003, the SSRP operation was found deficient and needing change. In particular:

a) Safety panel to become more proactive and focused, but without losing independence

b) Program manager to get insight into risks (i.e. involvement in risk acceptance)

c) Active involvement of engineering in the safety review process

In April 2005, the SSRP was replaced by the Safety Engineering Review Panel (SERP), constituted by a panel at each NASA center involved in the Shuttle Program (JSC, MSFC, KSC), plus an integration SERP for the review of integrated hazard reports, all reporting to the Shuttle program manager via a panel manager from the safety organization, The SERPs had review and approval authority for hazard reports and critical item lists. In addition, they were involved in the assessment of all project changes and anomalies with possible impact on safety.

The safety review panels of current NASA Space Launch System (SLS) program and Orion Multi-Purpose Crew Vehicle (MPCV) program, are a further evolution of Shuttle SERP.

The panels members are independent from the program and represent various branches of NASA engineering and functional organizations. They include also independent representative of prime contractor safety and engineering organizations but with some limitations on voting rights. SERP co-chairs are the safety and engineering technical authorities. The co-chairs have delegated responsibility for review and interim approval of safety analyses while final approval remains with the relevant program manager. Changes to the design which impact cost and schedule constraints are elevated to the program manager for final decision.

In 1977, in the early stages of the Shuttle program as work on payload safety and technical requirements progressed, consideration was given to the payload safety organization. This was to be a novel kind of organization. The Shuttle Program decided to establish the PSRP (Payload Safety Review Panel). The approach was completely different from Shuttle systems project reviews, and gave to the safety organization a leading and authoritative role, clear lines of responsibility, and ample technical support.

The safety review panel would be chaired by a safety staff and composed by representatives of different technical groups and organizations (engineering, operations, astronaut office, etc.)

The safety review panel would be chaired by a safety staff and composed by representatives of different technical groups and organizations (engineering, operations, astronaut office, etc.). The chair had sole authority for signature of hazard reports, and had direct access to Shuttle Program Manager. A pillar of the overall approach was that the payload organization (i.e. the customer) bore responsibility for the design and verification of the payload they provided. The safety review panel had instead the responsibility to ascertain that customers understood the safety requirements and carried out correctly the hazard analysis by identifying hazards, hazard causes, and relevant controls and verifications.

The customer had also to prove to the panel that agreed hazard controls had been incorporated first in the design and then in the builds. In the process, the payload organization had to obtain concurrence from NASA specialist groups on specific items such as construction materials usage, as meeting requirements for flammability, off-gassing and stress corrosion, toxicological assessment of hazardous chemicals, etc.

At the end of the safety review process, the chair would issue a letter certifying that safety reviews had been successfully completed for that payload to fly on a specific Shuttle mission.

In case of re-flight on a subsequent mission, any change had to be discussed with the panel. Any anomaly encountered in the previous mission had also to be discussed with the panel for safety relevance, and implemented corrective actions concurred.

The 'natural' separation between Shuttle program and payloads projects gave as rare benefit the development of the first goal/performance oriented safety standard, NSTS 1700.7b (NASA, 1989), and organizational independence, strong management support, and multi-disciplinary support to the safety review panel.

The PSRP operated flawlessly from the beginning of Shuttle operations, and was reconfirmed after Challenger and Columbia accidents.

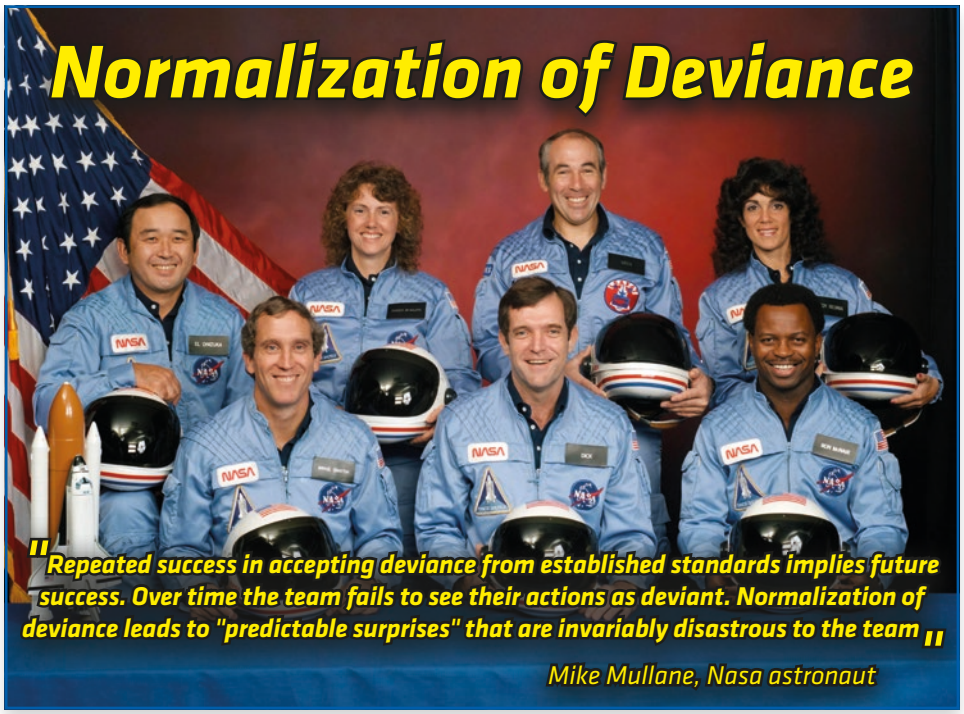
Some years later with the start of the International Space Station program, the safety review process and panel organization was modelled for the system and for payloads after the Shuttle payloads PSRP. The ISS payload safety reviews became a responsibility of the Shuttle payloads PSRP that was renamed accordingly as NSTS/ISS PSRP. A separate ISS SRP (Safety Review Panel) was created for ISS systems safety review. After Shuttle retirement and ISS assembly completion, the two panels were merged in a single one covering modification of ISS, operations, new cargo and crew transport commercial vehicles, and payloads.

In the words of Bob Wren, engineering representative in NSTS/ISS and ISS SRP:

> *"We set it up, copied the exact same approach that we did for the PSRP, for the Shuttle payloads. It turned out that that was a good move. That was a smart move. I guess, and it worked fine. So that way we could come in and have reviews, phase reviews, and I guess I didn't talk about that, but we'd have a series in both payload process and in this SRP process where we keyed the reviews to where the customer was in their development cycle… So we set up that same approach for the Station modules and it worked great".*

In 2002, a new chapter was inaugurated with the decentralization of safety review panels. A "franchised" NSTS/ISS Payload Safety Review Panel was established at the European Space Agency in The Netherlands, to operate with same rules and practices, and under oversight of NASA. A similar agreement was soon made with the Japanese Space Agency JAXA, while equivalent arrangements were putted in place with Russians.

After the Columbia accident, there were uncertainties at NASA about the organizational placement of the safety review panels, but eventually it was decided to maintain the chair reporting line to program managers (ISS and Shuttle).



2.2.2 Safety governance

The issue of "normalization of deviance"

An anomaly is "an unexpected event, hardware or software damage, a departure from established procedures or performance, or a deviation of system, subsystem, or hardware or software performance outside certified or approved design and performance specification limits".

A nonconformance is "a condition of any article, material, process, or service in which one or more characteristics do not conform to requirements specified in the contract, drawings, specifications, or other approved documents. Includes failures, defects, anomalies, and malfunctions". A nonconformance at the level of detailed design which can be solved without impact on system level requirements is a 'quality nonconformance'. If a safety relevant requirement is affected it is a 'safety nonconformance'.

An 'anomaly' is a possible nonconformance waiting confirmation. An engineer, a technician, a flight controller sees something that in his view is unexpected and reports an anomaly. Experts examine it and decide if it is truly something abnormal or the report initiator has mistakenly interpreted as anomalous something that is normal behavior of the system. Upon anomaly confirmation, a nonconformance resolution process is initiated, which will either determine how to fix the problem, or accept the violation as-is. Sometimes, the original requirement is found to be wrong and another process called 'engineering change request' is engaged to change it.

During operations, before engaging the offline nonconformance resolution process, other steps may be necessary. There are three different environments through which the anomaly resolution process may, in principle, progress: 1) real-time; 2) near real-time; and 3) offline environment. Usually, these three environments are not mutually exclusive, nor are truly progressive. When an anomaly is observed, immediate and/or urgent actions may be required to ensure the safety of the crew, and then the anomaly can be further investigated

offline. Other cases may not require real-time troubleshooting or safety actions at all and can be immediately addressed offline. The environment in which the anomaly is being handled determines who is responsible for its investigation and resolution.

The term 'normal anomaly', or 'normal deviance', was coined after the Challenger disaster to denounce a failure of the organization that tended to consider some recurrent anomalies as 'normal' although they were affecting high level safety requirements (Hall, 2003). This was the case of hot gases erosion of both redundant O-rings of the solid rocket motor field joints that caused the Challenger disaster. Leakage and multiple damages that in theory had a remote probability to take place were judged innocuous and accepted 'as-is' just because they were reoccurring without consequences. Usually, it is very expensive and time-consuming to root out the cause of a problem, and the motivation will surely lack if the problem is not deemed to represent an actual "flight safety" risks. There is also a cultural divide to take into account between operations team and safety teams, because the former looks to anomalies in the nominal context in which they generally happen, while the latter is trained to project their occurrence under worst case conditions.

A 'normal anomaly' is something perceived as between a non-confirmed anomaly and a confirmed one. It should not be there but can be seen as no problem because previously there was no consequence. Somehow the 'granularity' of the requirement is considered too be coarse. The fact that the anomaly keeps reoccurring without consequences is used as prove of its 'normality'.

Also, the cause of the Columbia accident, a loose piece of insulation foam from the main tank, was eventually traced back to the failure of the organization to recognize the seriousness of a recurrent anomaly that was considered 'normal'.

With the advantage of hindsight, we can clearly see the mistake but before the accident things were not at all so clear, and judgement open to biases. There was a requirement in the Shuttle specification stating that no material or parts had to be released during flight, the concern being damage due to collision. Starting from the first Shuttle flight there were chunks of insulating foam released from the main tank, but nothing serious happened. The conclusion was that such lightweight foam could not be a problem. Should we modify the requirement? No, too much paperwork. It is formally an anomaly but has no consequence, somehow the requirement is too strict. It is a 'normal anomaly'.

The Columbia Accident Investigation Board raised the following key questions:

- Why did NASA continue flying the Shuttle with a known problem that violated design requirements?
- The longer the Shuttle Program allowed debris to continue striking the Orbiters, the more opportunity existed to detect the serious threat it posed. But this is not what happened.
- Why were Debris Assessment Team engineers so unsuccessful at communicating their concerns up the NASA shuttle hierarchy?
- Why did NASA managers who espoused safety principles and risk aversion so quickly dismiss signs of risk and so readily accept facile arguments that the shuttle was safe to continue flying?

Columbia Accident Investigation Board (CAIB) Report

The Board concludes that NASA's current organization does not provide effective checks and balances, does not have an indipendent safety program and has not demonstrated the characteristics of a learning organization

Example of cognitive biases

Self-serving bias	Tendency for people to evaluate ambiguous information in a way beneficial to their interests
Gamble's fallacy	Putting a tremendous amount of weight on previous events, believing that they'll somehow influence future outcomes
Status quo bias	Unwarranted assumption that a change will be inferior or make things worse
Confirmation bias	Tending to agree with people who agree with us
Bandwagon effect	Going with the flow of the crowd
In-group bias	Overestimating the abilities and value of our immediate group (program team) at the expense of people {independent experts) we don't really know.

The technical authority process is built on the organizational and financial separation of the programmatic and institutional authorities

- How did unquestioned and unexamined aspects of the NASA culture contribute to the loss of the Columbia, are other organizations managing high risk technologies with checks/balances/safety reviews similar to NASA's susceptible to the same blind spots and influences, and what can be done about it?

- With the striking similarity to the errors and systemic problems that contributed to the loss of the Challenger in 1986, how could the lessons of Challenger have been forgotten so quickly?

The answer is that as long as deviations, having potential serious impacts on cost and schedule if not approved, are evaluated and decided upon by experts and managers belonging to the same program without the authoritative concurrence of an independent team, a certain amount of 'cognitive bias' should be expected to influence the decision-making process. In other words, people tend to believe what they have interest to believe!

Engineers and managers at NASA track thousands of program anomalies, and it is understandable that some anomalies may be perceived as normal, as acceptable low risk. What is not acceptable is that risk acceptance is done by the program without the concurrence of an independent technical authority.

In the words of the Columbia Accident Investigation Board:

"Organizations that successfully operate high-risk technologies have a major characteristic in common: they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule and mission-accomplishment goals."

Technical Authority

Government space agencies in US and Europe, have always struggled with the necessity of establishing a system of checks and balances to limit the authority of program managers in taking final decisions on safety matters. Safety review panels have enjoyed sometimes effective independence as long as the program manager had no programmatic interest about the impact of their decisions, otherwise panels gradually lost their independence.

Following accidents, the position of head of safety has been periodically moved up in the hierarchy and given direct access to the head of agency, but the power of the program manager as final decision maker remained basically unaltered until the Columbia accident.

After the publication of the Columbia accident report, NASA established an independent technical engineering authority responsible for technical requirements and all waivers to them and for independent oversight of programs and projects. *"Key principles in this framework include having clearly defined roles and responsibilities and having an effective system of checks and balances to provide a firm foundation for the balance of power between organizational elements"*. The technical authority process is built on the organizational and financial separation of the programmatic and institutional authorities.

The technical authority originates with the NASA Administrator and is then delegated to the Chief Engineer for technical standards, to Chief Safety and Mission Assurance (S&MA) for safety standards, and then to center directors (NASA, 2016). There is also a medical technical authority. Subsequent delegations down from the center director are formally made to selected individuals at specific organizational levels. The activity of individuals holding technical authority are funded independent of a program or project (NASA, 2014).

Technical authority individuals are involved in day-to-day program/project activities, including serving as members of control boards, change boards, and internal review boards. According to the technical authority process, decisions related to technical and operational matters involving safety residual risk require formal concurrence by the relevant technical authority (engineering, safety and medical) based on the technical merits of the case. Residual safety risks require first acceptance by the responsible program manager, then the consent of the technical authority, and finally the acceptance of the responsible safety organization. Should a technical authority disagree with a program action he/she can submit the matter to the next higher level of management. However, the program manager has the freedom, if in the interest of the project, to proceed at risk in parallel with the pursuit of a resolution through the technical authority hierarchy. Resolution is jointly attempted at successively higher levels of program and technical authority until the dissent is resolved, with possibility to raise the issue up to the NASA administrator.

Chapter 3

COMMERCIAL PRODUCTS STANDARDS DEVELOPMENT AND CONFORMITY ASSESSMENT – AN OVERVIEW

3.1 ORIGIN OF STANDARDS

One of the early examples of standardization was making rifle parts interchangeable between guns. This was a revolutionary idea from Thomas Jefferson and Eli Whitney, who was a mechanical engineer in the late 18th century. Whitney is sometimes called "The Father of Standardization," since he was the first to manufacture products on a large scale with the idea of complete interchangeability of parts. Years later, during the Civil War, the U.S. government recognized the military and economic advantages to having a standardized track gauge. The government worked with the railroads to promote use of the most common railroad gauge in the U.S. at the time which measured 4 feet, 8 ½ inches, a track size that originated in England. This gauge was mandated for use in the Transcontinental Railroad in 1864 and by 1886 had become the U.S. standard.

In 1904, a fire broke out in the basement of the John E. Hurst & Company Building in Baltimore. After taking hold of the entire structure, it leaped from building to building until it engulfed an 80-block area of the city. To help combat the flames, reinforcements from New York, Philadelphia and Washington, DC immediately responded—but to no avail. Their fire hoses could not connect to the fire hydrants in Baltimore because they did not fit. Forced to watch helplessly as the flames spread, the fire destroyed approximately 2,500 buildings and burned for more than 30 hours.

Great Baltimore Fire 1904.

It was evident that a new national standard had to be developed to prevent a similar occurrence in the future.

Up until that time, each municipality had its own unique set of standards for fire-fighting equipment. As a result, research was conducted of over 600 fire hose couplings from around the country and one year later a national standard was created to ensure uniform fire safety equipment. Soon afterwards, two boiler explosions in Massachusetts shoe factories, (Brockton, 1905 and Lynn, 1906) motivated the Governor to include in his inaugural address a demand for prompt action for improved public safety. One outcome of this mandate was the creation of a new Massachusetts law, "An Act Relating to the Operation and Inspection of Steam Boilers" (1909). This motivated another state, Ohio,

To help combat the flames, reinforcements from New York, Philadelphia and Washington, DC immediately responded—but to no avail. Their fire hoses could not connect to the fire hydrants

to draft their own laws in 1911. At the same time, as both states were developing laws, ASME was looking to the future in a way that would change the boiler industry and its future evolution, industry-wide standardization. From ASME's actions, the first edition of the Boiler and Pressure Vessel Code (BPVC) was issued in 1914 and published in 1915.

In the course of the 20th century standardization practices spread throughout industry worldwide from machine tools and sewing machines to bicycles, automobiles and eventually aviation. There were several incentives for standardization across the industry: It enabled parts suppliers to produce large quantities for multiple customers, such that suppliers could gain economies of scale and lower their costs. Suppliers passed these savings on as lower prices to automobile manufacturers. In addition, standardization meant that if one supplier went out of business, shortfalls of parts could be made up by other suppliers without a delay for reconfiguring their machinery to new specifications. Standards also allowed manufacturers to impose minimum quality criteria on their suppliers. In general, standardization benefited both suppliers and manufacturers throughout the industry.

Mass production of cars by many companies was a formidable early driver for the establishment of consensus standards. Coordinating standards development among different automotive firms became the responsibility of the Society of Automotive Engineers (SAE). SAE was a professional society whose membership spanned the industry, including both manufacturers and suppliers; was independent of any one firm or set of interests; and had the technical competence for the required work. Its success in reducing the variety of parts and in promoting interchangeability and quality was such that the National Automobile Chamber of Commerce, an industry trade association, estimated in 1916 that SAE standards yielded cost reductions of 30 percent in ball bearings and electrical equipment and 20 percent in steel.

A standard consists of a set of characteristics that describes the features of a product, process, or service, and against which it can be measured or assessed

3.2 DEFINITIONS

There is no single, simple definition of *standard* that captures the broad range of meanings and uses of the term. There are, however, general characteristics of many or most standards that will serve as a working definition within this report. A standard consists of a set of characteristics that describes the features of a product, process, or service, and against which it can be measured or assessed. The description can take the form of detailed design/construction rules or performance criteria.

A standard must be well designed, based in sound technology, appropriate to the task at hand, and accepted as valid and useful by the population of users. A standard that meets these criteria, however, still fails to have the effect its developers intended if products, processes or services designed to conform to it do not, in practice, conform. Conformity assessment is the comprehensive term for measures taken by manufacturers, their customers, regulatory authorities, and independent third parties to assess conformity to standards.

In the past, it was considered that wide agreement on a standard could be reached only as a result of long and successful application of a technical practice, which was then promoted to the level of standard. Nowadays, standards are often needed to be established upfront in many new technological fields to support their integration and diffusion. This is for example the case of the upcoming transition from analogue ground-based technologies (radar, radio) for air traffic management to digital space-based data communication.

Standardization helps to build focus, cohesion and critical mass in the emerging stages of technologies, and to codify and diffuse the state of the art. Consensus standardization processes driven by industry stakeholders enable competition between and within technologies and contribute therefore to innovation and growth (Blind, 2013).

Conformity assessment is the comprehensive term for measures taken by manufacturers, their customers, regulatory authorities, and independent third parties to assess conformity to standards

3.3 FUNCTIONS OF STANDARDS

Based on the purpose of a standard we can identify seven categories: fostering commercial communication; diffusing technology; raising productive efficiency; enhancing market competition; ensuring physical and functional compatibility; improving process management; and enhancing public welfare.

Because of the purpose of this report we will focus on two categories: process management and public welfare

3.3.1 Process Management

Manufacturers not only design products to conform to standards, sometimes they also organize the manufacturing process itself in accordance with standards. For example, the U.S. Occupational Safety and Health Administration (OSHA) regulates many manufacturing processes to protect worker safety. Independent inspection and audit of production play a key part in the enforcement of process standards such as those set by OSHA. Company may also apply process management to quality assurance, in accordance with voluntary standards like ISO 9001 or with the more stringent aerospace quality assurance standard AS9100 developed by IAQG, a consortium of major aerospace companies, and published by SAE. Accredited independent auditors perform conformity assessment against such voluntary standards.

3.3.2 Public Welfare

Standards are an important means of promoting societal goals, such as protection of health, safety, and the

Category of standards	For example...
1. COMMERCIAL COMMUNICATION Standards convey information about a product to the buyer in a consistent, understandable manner.	(a) **construction materials** – standard dimensions, strengths, and durabilities make it easier for the builder to select materials for specific purposes (b) **film speed** – standard ratings (ISO 100, 200, 400, etc.) simplify matching film to photographic needs
2. TECHNOLOGY DIFFUSION A technological advance incorporated into a standard is more readily adapted and used by others.	(a) **personal computer architecture** – use of PCs expanded rapidly once IBM-compatibility standard came into being (b) **advanced materials (e.g., composites, ceramics)** – standards that describe processing and test methods allow duplication and improvement upon state of the art
3. PRODUCTION EFFICIENCY Standardization of parts, processes and products enables economies of scale in production.	(a) **automobile assembly line** – efficient mass production pioneered with the Ford Model T (b) **fast food chains (e.g., McDonald's)** – food, restaurant style, equipment, and procedures standardized for efficiency
4. ENHANCED COMPETITION When some or all of the features of different manufacturers' products conform to one standard, comparison is easier and competition sharper.	(a) **direct-dial long-distance telephone service** – competing carriers offer a standardized basic service; competition centers on price and extra services (b) **gasoline** – octane ratings allow consumer to compare similar products on the basis of price
5. COMPATIBILITY Standards defining interfaces enable products to work or communicate with each other.	(a) **Internet** – standard format for sending and receiving data enables communication among computers worldwide (b) **stereo system components** – various types of components can be connected with standard cables and jacks
6. PROCESS MANAGEMENT Manufacturers not only design products to conform to standards, they also organize the manufacturing process itself in accordance with standards.	(a) **numerically controlled machine tools** – standard computer languages allow rapid reconfiguration of production line (b) **quality assurance** – ISO 9000 series of standards guides firms in setting up and maintaining a quality assurance management system
7. PUBLIC WELFARE Standards are an important mechanism for promoting societal goals, such as protection of health, safety, and the environment.	(a) **health codes** – restaurants conform to sanitary standards that are backed up by inspections (b) **automobile air bags, seat restraints, and bumpers** – government mandated crash protection

environment. Government agencies at the national, regional, state, and local levels administer thousands of regulatory standards or technical regulations. These govern the characteristics of the products and services that manufacturers produce and the materials and processes that they use in producing them. Some regulatory standards are developed by government agencies, but many are developed within the private sector and adopted by government. Government is both a major producer and a major user of standards. This report takes as given the fact that public needs may sometimes outweigh other concerns. There are, for example, health and safety concerns that justify imposition of regulatory standards despite the costs they impose on manufacturers and consumers. Government is also a major purchaser of goods and services, frequently by means of procurement standards and specifications. As a result, government agencies have a public interest in obtaining the best value for money through appropriate standards and efficient conformity assessment procedures.

De facto Standard	A standard arising from uncoordinated processes in the competitive marketplace. When a particular set of product or process specifications gains market share such that it acquires authority or influence, the set of specifications is then considered a de facto standard. *Example: IBM-compatible personal computer architecture.*
Voluntary Consensus Standard	A standard arising from a formal, coordinated process in which key participants in a market seek consensus. Use of the resulting standard isvoluntary. Key participants may include not only designers and producers, but also consumers, corporate and government purchasing officials, and regulatory authorities. *Example: photographic film speed – ISO 100, 200, 400, etc., set by International Organization for Standardization (ISO).*
Mandatory Standard	A standard set ny government. A procurement standard specifies requirements that must be met by suppliers to government. A regulatory standard may set safety, health, environmental, or related criteria. Voluntary standards developed for private use often become mandatory when referenced within government regulation or procurement. *Example: automobile crash protection – air bag and/or passive seat restraint mandated by National Highway and Traffic Safety Administration.*

3.4 TYPE OF STANDARDS BY DEVELOPMENT

Principal types of standard by development process are: de facto standard, voluntary consensus standard, and mandatory standard.

De facto standards may arise without formal sponsorship, simply through widespread, common usage.

When groups write standards through a formal process of discussion, drafting, and review. to meet customer, industry, and public needs, and the resulting standards are published for voluntary use throughout industry, such standards are termed ***voluntary consensus standards***. No single organization, public or private, controls the U.S. standards development system. The efforts of many U.S. voluntary consensus standards organizations, however, are coordinated by the private, nonprofit American National Standards Institute (ANSI). This organization sets guidelines for groups to follow in managing the consensus-seeking process in a fair and open manner. ANSI reviews and accredits many U.S. standards-setting organizations for compliance with these guidelines. It also approves many of the standards these organizations produce, designating them as American National Standards.

Mandatory standards are standards set by government with which compliance is required, either by regulation or in order to sell products or services to government agencies. Even in the case of standards written by government, the process of development is not without private input or participation. For example, laws governing administrative processes, such as the Administrative Procedures Act, require public review and comment on proposed regulations. The *Federal Register* regularly publishes requests for comments on standards drafted by federal agencies. The boundary between voluntary and mandatory standards is not always distinct. Government standards writers frequently refer to privately developed, voluntary standards within the text of regulations and procurement specifications. Mandatory standards may cite voluntary standards in whole or in part, with or without additional criteria beyond those set in the referenced standard.

3.4.1 Development of Consensus Standards

Consensus standards developing organizations

Standards developing organizations (SDOs) belong to one of three main categories: *professional societies, industry associations, and standards-developing membership organizations.* In addition,

consortia are playing an increasingly important standards development role, particularly in industries characterized by rapid advance of technology. In US, SDO's are private organizations. Outside US many countries have a central, primary national standards-developing body. This is usually a government-chartered private organization or a quasi-public agency, rather than a direct agency of the government. Examples include Germany's Deutches Institute fur Normung (DIN), the British Standards Institute (BSI), and France's Association Francaise de Normalisation (AFNOR). To promote trade inside the European Union (EU), the EU endorses the work of the three European standards (harmonization) bodies: The Comité Européen de Normalisation (CEN, founded in 1961), the Comité Européen de Normalisation Électrotechnique (CENELEC, founded in 1973), and the European Telecommunications Standards Institute (ETSI, founded in 1988).

Voluntary Consensus Standard Process

The typical method for developing voluntary consensus standards is to coordinate participation of volunteer technical experts in standards-writing committees. Committee membership is generally selected to represent a diversity of interests and viewpoints. draft technical standards are proposed, discussed, revised, and voted on. Consensus is the key goal. Although negative votes do not prevent a standard's adoption, they must generally be considered and responded to in writing. After review, comment, and approval by the SDOs oversight board and membership at large, the organization publishes the standard. Firms also pay salary and travel expenses for employees who serve as individuals in the work of professional societies and standards-developing membership organizations such as SAE International, the American Society for Testing and Materials (ASTM), and the Institute of Electrical and Electronics Engineers (IEEE). Unless the standard is subsequently mandated as part of a government regulation or procurement specification, its acceptance by potential users is voluntary. Standards adopted as mandatory by government, moreover, are usually more effective if they reflect consensus among affected parties. A consensus among interested parties during the design of a standard clearly increases its prospects for broad acceptability. The second feature of the voluntary consensus standard process is the administrative *due process*. These groups have formal policies governing such facets of standards development as technical committee membership; setting the scope of proposed standards; drafting and revising standards; voting within committees; review of draft standards by higher authority within the SDO; and balloting and

Consensus Standards Developing Organizations

Professional Societies

Professional societies are individual membership organizations that support the practice and advancement of a particular profession. Several such societies, particularly in the engineering disciplines, develop technical standards. The goal of these SDOs is generally to find the best technical solution to meet an identified need. Participants in standards committees serve as individual professionals, not as representatives of the firm they work for. (e.g. IEEE-Institute of Electrical and Electronics Engineers, ASME-American Society of Mechanical Engineers)

Industry Associations

Industry associations, also known as trade associations, are organizations of manufacturers, suppliers, customers, service providers, and other firms active in a given industry sector. Their mission is to further the interests of their industry sector, including the development of technical standards. Many industry associations develop standards or sponsor their development through a subsidiary or associated SDO. Funding is primarily through members' dues. Members of technical committees typically serve as representatives of their firm. Each firm carries equal weight in committee voting, regardless of the number of experts it sends to participate in the committee's standards development work. Industry association SDOs are likely to be more openly responsive to commercial market concerns in their technical decision making than other types of SDOs.

Membership Organizations

Unlike industry associations and professional societies, standards-developing membership organizations have standards development as their central activity and mission. They do not limit their membership to an industry or profession, and they tend to have the most diverse membership among all SDOs. Their procedures tend to have the strictest due process requirements. Publishing and selling standards documentation accounts for the majority of their revenues. Membership fees are generally relatively low, facilitating participation by individuals not sponsored by an employer. (e.g. ASTM - American Society for Testing and Materials).

Consortia

Standards consortia are a response to the rate of technological advance outpacing consensus standards development in some industry sectors. Participation in standards-setting is generally limited to consortium members. Requirements for openness, consensus, and due process are less strict than in other standards-developing organizations, primarily to speed the development process. In fact, standards produced by consortia represent a hybrid stage between de facto industry standards and full consensus standards (e.g. IAQG – International Aerospace Quality Group). The original objective of the IAQG members (leading aircraft and engines manufacturers) was to upgrade the ISO 9001 consensus voluntary standard with harmonized quality assurance requirements they used to levy on suppliers, and to establish a consortium-controlled accreditation system for third party conformity assessment.

approval by the membership at large. Formal procedures, such as open participation and review, also serve as protection against allegations of collusive behavior for participants from competing firms.

3.5 CONFORMITY ASSESSMENT

Standards would be unable to fulfill any of their functions without some degree of confidence that manufacturers' claims for their products of conformity to standards are correct and justified. Such assurance can come from the firm's internal procedures for meeting standards; from review by an independent, private source outside the firm; from a government-mandated regulatory program; or from a combination of such elements. Conformity assessment is the comprehensive term for procedures by which products and processes are evaluated and determined to conform to particular standards. As distinct from standards *development*, conformity assessment may be thought of as a central aspect of the use of standards.

Conformity assessment comprises three areas. The first area, ***manufacturer's declaration of conformity***, is assessment by the manufacturer based on internal testing and quality assurance mechanisms.

Second is ***testing*** of products, parts, and materials performed by independent laboratories as a service to the manufacturer. Independent testing may be of value to the manufacturer as an outside confirmation of in-house test results; it may be required by a customer as a condition of sale; or it may be mandated by a regulatory agency.

The third area is ***certification***, formal verification by an unbiased third party (review of design, testing, etc.) that a product conforms to specific standards. Familiar examples of certification, among many others, are the Underwriters Laboratories for commercial product safety certification (the UL mark).

3.6 SAFETY STANDARDS DEVELOPMENT AND CONFORMITY CERTIFICATION

3.6.1 Prescriptive vs. performance safety standards

In the early hours of 15 April 1912, the RMS Titanic struck an iceberg on her maiden voyage from Southampton, England, to New York, and sank. A total of 1,517 people died in the disaster because there were not enough lifeboats available. During the Titanic construction Alexander Carlisle, one of the managing directors of the shipyard that built it had suggested using a new type of larger davit, which could handle more boats thus giving Titanic the potential for carrying 48 lifeboats providing more than enough seats for everybody on board. But in a cost cutting exercise, the customer (White Star Line) decided that only 20 lifeboats would be carried aboard thus providing capacity for only about 50% of the passengers (on the maiden voyage). This may seem a carefree way to treat passengers and crew on-board, but as a matter of fact the Board of Trade regulations of the time stated that all British vessels over 10,000 tons had to carry 16 lifeboats. The regulation had become obsolete within a short period of time when at the beginning of the 20th century ship tonnage raised up to Titanic's 46,000 tons. Furthermore, the RMS Titanic was believed to be unsinkable by design, therefore why worry about lifeboats?

Prescriptive Standard. Prescriptive standard is a standard that specifies design requirements, such as materials to be used, how a requirement is to be achieved, or how an item is to be fabricated or constructed, such that the item can be considered safe. The Titanic accident illustrates what a prescriptive

A total of 1,517 people died in the RMS Titanic disaster because the number of lifeboats requirement was obsolete.

requirement is (i.e. an explicitly required design solution for an implicit safety goal), and how it can sometimes dramatically fail by obsolescence.

The underlying motivation for prescriptive requirements is to prevent circumvention by avoiding any subjective interpretation in the implementation as well as in compliance verification. Violation of requirements can be unequivocally determined by simple inspections.

The vast majority of standards in use in aviation and other "evolutionary" industries are the result of lessons learned from incidents and accidents, and steady technological advancement. They are detailed per type and prescriptive. In contrast, there are industries in which building on future experience is simply not possible, because the system is completely new, highly safety-critical and/or extremely expensive.

Performance Standard. A performance standard specifies the outcome required (e.g. safety level) but leaves the concrete measures to achieve that outcome (e.g. hazards risk mitigation and control measures) up to the discretion of the designer.

How performance standards are designed and how they are implemented and enforced matters greatly

Performance standards include requirements that are *qualitative* and/or *quantitative* with reference to the ultimate goal (e.g. level of safety). *Quantitative* performance requirements can be distinguished between those for which compliance can be demonstrated by *prediction* (e.g. launch failure), and those for which compliance can be demonstrated by *measurement* (e.g. air contaminants in the habitable environment).

By focusing on outcomes, performance standards give to developers flexibility, and make it possible for them to find the lowest-cost means to achieve compliance. Performance standards can generally accommodate technological change and the emergence of new hazards in ways that prescriptive standards cannot. Performance standards can be imprecise when the requirements are too loosely specified or can be questionable when performance has to be assessed by quantitative predictions. Sometimes uncertainty is injected into a performance standard just because of the need to be generic.

How performance standards are designed and how they are implemented and enforced matters greatly.

While it is useful for conceptual purposes to distinguish performance standards from prescriptive standards, in practice the two approaches can be better thought of as end points along a spectrum of requirements running from what might be considered "pure" performance standards to "pure" design standards, depending on advantages and limits. A good performance standard may leave ample freedom to the designer by setting goals at system level, while somehow constraining the designer's freedom for some high-risk technologies (e.g. batteries, pressure vessels, EMC) where existing prescriptive requirements are known to work well. However, by including a clause in the standard about

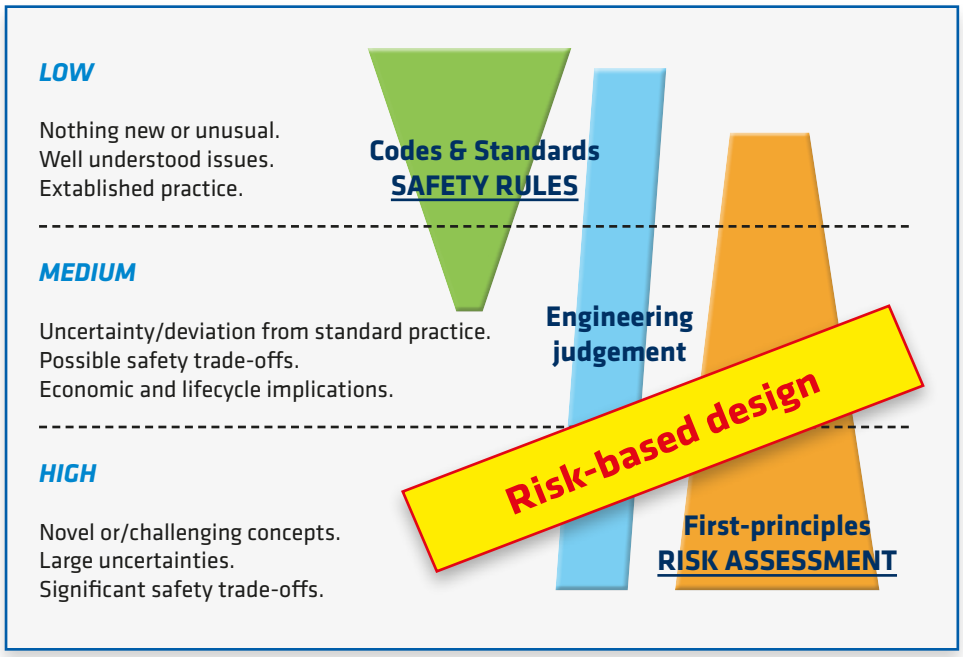
Pros and Cons of Prescriptive Requirements

Advantages of prescriptive standards, also called design standards or rules-based standards

- Easier for developers and operators to implement
- Easy to check compliance with for the safety authority
- Schedule efficient: just read and transpose into design
- No need (for industry) to think "is this good enough"

Disadvantages of prescriptive standards, also called design standards or rules-based standards

- Mandated solutions may be effective in some cases but not in other cases
- Mandated solutions may prove to be more costly than other equally effective solutions
- By specifying how to act, prescriptive standards can inhibit innovation or become obsolete
- Are reactive (reviewed and changed post mishap)
- May lead to over/under-engineering
- Nurture a compliance mindset rather than a safety mindset



Level of Innovation and Risk-Based Design (Papanikolaou et al. 2009).

"Equivalent Safety", ultimate freedom for the designer is restored.

The correct implementation of performance standards requires training/familiarity of the project team such to avoid misinterpretations of the requirements (too loose, too tight). Sometimes, guidelines on requirements interpretation and accepted means of compliance can help the design team. "Safety Equivalency" demonstration may require sophisticated analysis like PRA (Probabilistic Risk Assessment).

The key concept in implementing a performance safety standard is that it cannot be used directly for the design but it is an input to a risk-based design process. Performance requirements are tailored through hazard analysis and modulated depending on consequence severity such to aim for low probability of occurrence for high-consequence events, while allowing higher probability of occurrence for low-consequence events.

3.6.2 Third-party Safety Certification

Conformity assessments of prescriptive standard versus performance standard vary greatly. While objective evidence of compliance with prescriptive requirements is straightforward through inspections and tests, assessing compliance with performance requirements necessitates an independent multi-disciplinary review team with design and operations skills and competences equal or even better than those of the project team. Furthermore, the review team chair must have the authority to mandate actions, to "own" the standard's uncertainties (provide interpretations), to approve equivalencies, and to recommend approval/disapproval of deviations.

Measures to evaluate and ensure conformity are of as much or more significance than the standards themselves

In the context of many commercial and regulatory uses of standards, in particular those related to public welfare, measures to evaluate and ensure conformity are of as much or more significance than the standards themselves.

Manufacturers of potentially dangerous products generally maintain internal assurance procedures and also seek third party conformity assessment. Third-party assessment is the sector of the conformity assessment system that has grown most in recent years. In most commercial interactions, there is no need for the added expense and complexity of third-party conformity assessment. There is, however, one circumstance in which relying on the manufacturer's declaration and the purchaser's own assessment is inadequate, when the safety, health, or environmental impact of a product are sometimes too important to be left to the manufacturer's own assessment and too expensive or technically difficult for the customer to perform. This is true, for example, of products whose failure could lead to injury, illness, property damage, or loss of life. In these cases, it is unacceptable to discover the product's nonconformity after a failure has occurred. Much of the U.S. conformity assessment system exists specifically to address this type of safety, health, and environmental concern. In regulated product sectors, such as aircraft, automobiles, agricultural chemicals, heavy machinery, and drugs, a regulatory authority requires competent, prior assurance of conformity to relevant standards before a product can be accepted and used. Many regulations require third-party assessment to verify product safety. Drug safety certification required by the Food and Drug Administration is an example of a federal program of this type.

Often in the field of safety, standards development and certification of conformity are performed by the same organization as "public service" or under delegation from the Government. A well-known certification mark found on many products is the "UL" label. This mark is owned and managed by Underwriters Laboratories, a nonprofit institution that develops safety standards and tests and certifies many consumer and other

Independent (safety design) Peer Review

According to The UK Nuclear Industry Guide To Peer Review of Safety Cases, August 2016, *"A key benefit of Independent Peer Review is that it allows a competent team, free from project/production pressures, the time to read the safety submission and to think clearly and logically about the hazards and risks inherent in an activity and from this make a judgement on whether the safety submission has demonstrated that these hazards and risks are adequately controlled. Being independent from those responsible for the production of the safety submission allows the Peer Review process to bypass any 'group think' mentality and any prejudgements on safety that may exist within production teams."*

"The Peer Reviewer must have a comparable degree of technical competence and experience to the author of the safety submission. Peer Reviewers should therefore have appropriate academic, professional or vocational qualifications in the relevant subject matter. Peer Reviewers must also have an understanding of the principles and concepts in safety and safety management and of the safety regulatory framework, standards, guidelines and codes of practice pertaining to the subject of the submission".

"It is particularly important to be aware of the dangers of Peer Reviewers losing their independence and becoming part of the project team's decision-making process. Peer Reviewers should not advise projects on what decisions to make or what safety argument would be acceptable and must not provide verbatim text to be written into a safety submission. Nevertheless, in the interests of efficiency, if a Peer Reviewer is aware of a better way of doing things or something important has been missed, then they should point this out in clear and unambiguous terms whilst being careful not to compromise their independence when giving such advice to a Project".

products. Other examples are illustrated here below.

In the case of certification against a performance safety standard, unique skills and a well-thought organizational set-up are required. The results of the safety analysis, the description of the risk mitigation measures, and the verification of implementation of such measures are documented in a report that it is submitted to an independent peer review (also called safety review panel) as the design progresses. Such report is sometimes called *Safety Case or Safety Data Package, Safety Submission*, etc.

Classification Societies

In the second half of the 18th century, marine insurers based at Lloyd's coffee house in London, developed a system for the independent inspection of ships presented to them for insurance coverage. In 1760, a committee was formed for this express purpose, the earliest existing result of their initiative being Lloyd's Register Book for the years 1764-65-66. The condition of each ship was classified on an annual basis. Hull condition would be A, E, I, O or U, according to the excellence of its construction and its perceived continuing soundness (or otherwise).

In 1834, the Lloyd's Register of British and Foreign Shipping' was reconstituted as a self-standing 'classification society'. Following the example, a number of Classification Societies were established worldwide in 19th century: Bureau Veritas, Registro Italiano Navale, American Bureau of Shipping, Det Norske Veritas, Germanischer Lloyd and Nippon Kaiji Kyokai), followed in 20th century by Russian Maritime Register of Shipping, China Classification Society, Korean Register and Indian Register of Shipping.

In 1948, the United Nations International Maritime Organization (IMO) was established to deal with maritime safety, traffic and environmental issues within an international framework. In 1968, the major classification societies established the International Association of Classification Societies (IACS) to provide coordinated technical support and guidance to the International Maritime Organization (IMO) and to national maritime organizations.

Legally, Classification Societies act as a "Recognized Organizations" carrying out statutory surveys and certification as delegated by national maritime administrations (flag administrations). In particular:

- Developing technical standards for design and construction of ships
- Approving designs against those standards

The world oldest *"safety institute"* the Lloyd's Register of ships is nearly three centuries old. Bizarrely, it all began rather modestly in a London coffee house.

- Conducting technical surveillance during construction
- Performing in-service inspection and periodic survey during operation
- Reviewing and approving in-service modifications
- Performing safety research and development programs

The standards published by Classification Societies, together with the requirements set down in the various International Conventions of the International Maritime Organisation (IMO) and the marine legislation of the flag states, form a comprehensive and coherent set of standards for design, construction and maintenance in operation of ships. Classification Societies maintain a leading role in all matters related to technical standards and certification activities, while national and international governmental organizations concentrate primarily on operational and environmental matters.

Classification Societies are specialized but they operate in an industry that has evolved over centuries and therefore does not require unique competences. They are independent because they are not controlled by, and do not have interests in, ship-owners, shipbuilders or engaged commercially in the manufacture, equipping, repair or operation of ships. They are completely separated from industry because of historical reasons, and being favored by the market size of ships certification business. Their authority is essentially delegated from the government.

Center for Offshore Safety

On April 20, 2010 the Deepwater Horizon oil rig located in the Gulf of Mexico exploded and subsequently sank killing 11 people, injuring 17, and causing the largest marine spill and environmental catastrophe in history. The report of the U.S. Presidential Commission that investigated the disaster made, among others, the recommendation that "the gas and oil industry must move towards developing a notion of safety as a collective responsibility. Industry should establish a "Safety Institute…this would be an-industry created, self-policing entity aimed at developing, adopting, and enforcing standards of excellence to ensure continuous improvement in safety and operational integrity offshore" (National Commission, 2011). In early 2011, following the recommendation, industry created the Center for Offshore Safety (COS), with the stated mission to "promote the highest level of safety" for offshore operations through "leadership and effective management systems". The Center for Offshore Safety helps operators to develop safety programs based on best-practices that are rigorously assessed by well-trained third-party auditors. The COS is a branch of a trade organization, thus attracting some criticism about its independence (theconversation.com, 2014).

The gas and oil industry must move towards developing a notion of safety as a collective responsibility

FIA Institute for Motor Sport Safety and Sustainability

In the first three decades of the Formula 1 World Championship, inaugurated in 1950, a racing driver's life expectancy could often be measured in fewer than two seasons. It was accepted that total risk was something that went with the job (Tremayne, 2000).

A racing driver's life expectancy could often be measured in fewer than two seasons

The Deepwater Horizon oil rig exploded and sank killing 11 people, and causing the largest environmental catastrophe in history.

How on earth did they change the riskiest sport into one of the safest?


DEATH OF A LEGEND

SENNA SAFETY PLEA TOO LATE

MOTOR SPORT

By GEOFFREY HARRIS

35 "14

FERRARI legend and triple world champion Niki Lauda begged Ayrton Senna to take a stronger line on driver safety hours before Senna was killed yesterday.

Lauda, who cheated death after a fiery crash in Germany in 1976, said he spoke to Senna at Imola race track during an early phone call.

"I told him that as the No.1 driver and a world

They pulled apart all of their processes and equipment and changed what was happening on and around the [Formula 1] track. Jackie [Stewart] makes a pretty bold claim that, based on the numbers, is hard to argue with, "there is no doubt that Formula One has the best risk management of any sport and any industry in the world". Far from being the preserve of overthinking pessimists, I believe that risk management is actually the place where you'll find the bravest and hardiest of souls. People who care less about being popular and more about saving lives, businesses, and sometimes, entire communities. It is not for the fainthearted. You need to be tenacious. Backsliding can easily happen, so you need to be vigilant, too. But the rewards are potentially enormous.

(The Triumph of Risk Management, Craig Thornton, Adjunct Faculty Television, Radio & Film, Syracuse University)

The turning point was the Imola Grand Prix of 1994 with live coverage of Roland Ratzenberger and Ayrton Senna deaths that forced the car racing industry to look seriously at safety or risk the loss of television rights. In the days after the Imola crashes the FIA (Fédération Internationale de l'Automobile) established the Safety Advisory Expert Group, later renamed FIA Safety Institute, to identify innovative technologies to improve car and racetrack safety, and to mandate certification testing. Nowadays Formula 1 car racing is a safe multi-billion dollar business of sponsorships and global television rights. Entertainment for families that can be enjoyed without risking shocking sights. The institute was reorganized as integral part of FIA in 2016.

Institute of Nuclear Power Operations

In March 1979, a series of mechanical and human errors at the Three Mile Island nuclear generating power plant in Pennsylvania, caused an accident that profoundly affected industry.

A combination of stuck valves, misread instruments, lack of information and poor decisions led to a partial meltdown of the reactor core and the release of radioactive gases into the atmosphere. The accident although minor in its health consequences, had widespread and profound effects on the American nuclear power industry. It resulted in temporary closing of seven reactors and moratorium on the licensing of new reactors that significantly slowed industry for several years (history.com).

The Kemeny Commission, which president Jimmy Carter formed to investigate the accident recommended that "The (nuclear power) industry should establish a program that specifies appropriate safety standards including those for management, quality assurance, and operating procedures and practices, and that conducts independent evaluations" and that "There must be a systematic gathering, review and analysis of operating experience at all nuclear power plants, coupled with an industrywide international communications network to facilitate the speedy flow of this information to affected parties" (Kemeny, 1979). In response to the recommendations, industry established in December 1979, the Institute of Nuclear Power Operations (INPO) as a not-for-profit organization with the mission to promote the highest levels of safety and reliability in the operation of commercial nuclear power plants. The INPO establishes performance objectives, criteria and guidelines for the nuclear power industry, conducts regular detailed evaluations of nuclear power plants, and provides assistance to help nuclear power plants continually improve their performance.

The nuclear power industry should establish a program that specifies appropriate safety standards including those for management, quality assurance, and operating procedures and practices, and that conducts independent evaluations

Chapter 4
STANDARDS CURRENTLY USED IN COMMERCIAL SPACE PROGRAMS

4.1 INTRODUCTION

Often technical standards are seen as something different and separated from safety standards just because they are under the authority of different organizations, Engineering, instead of Safety & Mission Assurance (S&MA). As a matter of fact, many requirements levied by technical standards for human-rated systems development are aimed at minimizing the safety risk. Wayne Hale, former NASA Shuttle Program Manager, made the point as follows:

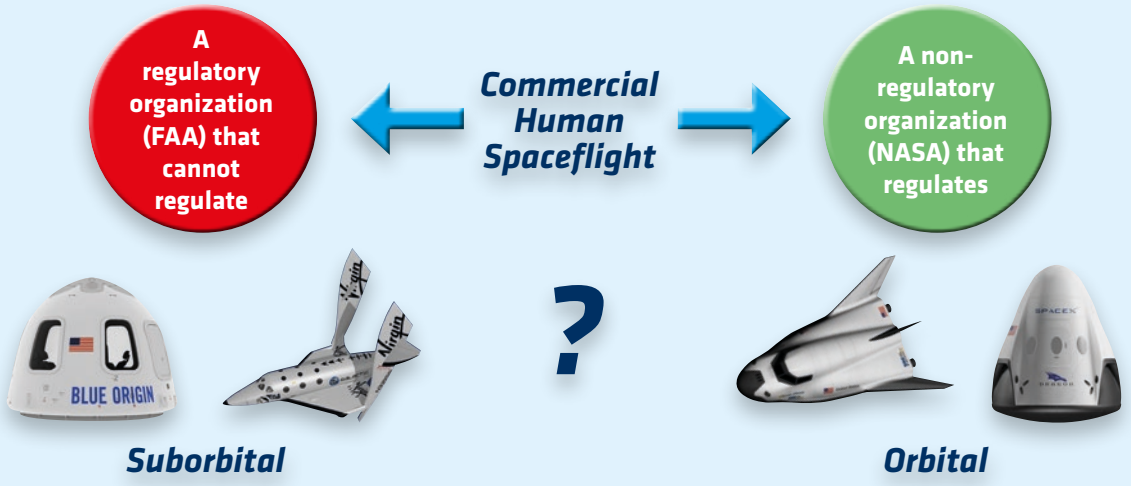
Wayne Hale
NASA Shuttle Program Manager (ret.)

"Armchair authorities like to discuss the "big ticket" items in the Human Ratings Requirements: redundancy requirements for fault tolerance, or minimum factor of safety for structures as examples. Real rocket builders know while those are important, the real key to safety and success is very much more affected by the quality of parts and myriad individual steps in workmanship of the end product. These are measured against thousands of individual checks against the appropriate standard. So, you must realize the vast majority of standards and requirements do not show up in the NPR 8705.2C Human Ratings Requirements document, they must be searched out in a hundred subordinate documents."

(Hale, W. 2010)

4.2 UNITED STATES

The commercial spaceflight industry is developing in U.S. under some specific constraints on the establishment of government regulations and international activities: namely legal moratorium until 2023 on safety regulations for humans



Orbital vehicles have suborbital flight capabilities, and in some cases both versions have been designed (e.g. Dream Chaser of SNC). However, while requirements for safety certification of orbital flights are available from NASA, FAA is forbidden to levy similar requirements for suborbital vehicles.

on board, and export control rules. The moratorium was spearheaded by proponents of suborbital spaceflight fearing imposition of extensive (and expensive) aviation-like certification test programs. The export control rules limit instead the dissemination of technical information outside the country because of space technologies dual-use.

Because of the moratorium on safety regulations for humans on board, current U.S. legislation requires only that a commercial space operator obtains a FAA license for public safety of launch and re-entry operations. But there is one remarkable exception: operators providing commercial transportation services to the International Space Station under the terms of NASA's Commercial Crew Program (CCP) are required to obtain a NASA safety certificate for the safety of humans on board, as foreseen by the original agreements signed by governments participating to the ISS program (NASA OIG, 2016). In U.S. a de-facto double regulatory regime exists (no-regulation/full-regulation) for safety onboard space vehicles depending if the customer is a private entity or NASA ISS Program.

Differently from all other NASA programs, companies involved in the CCP program own and operate their spacecraft and infrastructure and are free to design the system they think is best, and to use the manufacturing and business operating techniques they choose. However, the NASA program has to implement the safety policy outlined in a dedicated document (ESMDCCTSCR-12.10) (NASA, 2010), and companies must meet or exceed a pre-determined set of NASA technical and safety requirements. In the initial phase of the CCP program, NASA made an inventory of such standards and recommended them either as reference baseline (meet or exceed) or as good practices, stating that "In the course of over forty years of human space flight, NASA has developed a working knowledge and body of standards that seek to guide both the design and the evaluation of safe designs for space systems".

Safety policy and technical standards used by NASA Crew Commercial Program represent an excellent reference from which U.S. commercial human spaceflight industry can develop policies and standards to be used on non-NASA suborbital and orbital commercial spaceflight programs. Furthermore, industry can use the NASA CCP certification program as model for developing their own independent third-party certification process.

4.3 EUROPE

Standards meant for voluntary use also on commercial space systems were started in Europe in the early 1990's under an initiative called ECSS (European Cooperation for Space Standards).

In 1987, Europe started an ambitious human spaceflight program including Hermes spaceplane, Ariane 5 human-rated launcher, and Columbus Man-Tended Free-Flyer. At that time the European Space Agency (ESA) had a safety standard, PSS-01-40, based on Shuttle/Spacelab experience. Because of the close involvement in those new programs of other European space agencies, in particular the French Space Agency CNES, and because of industry interest to establish common standards

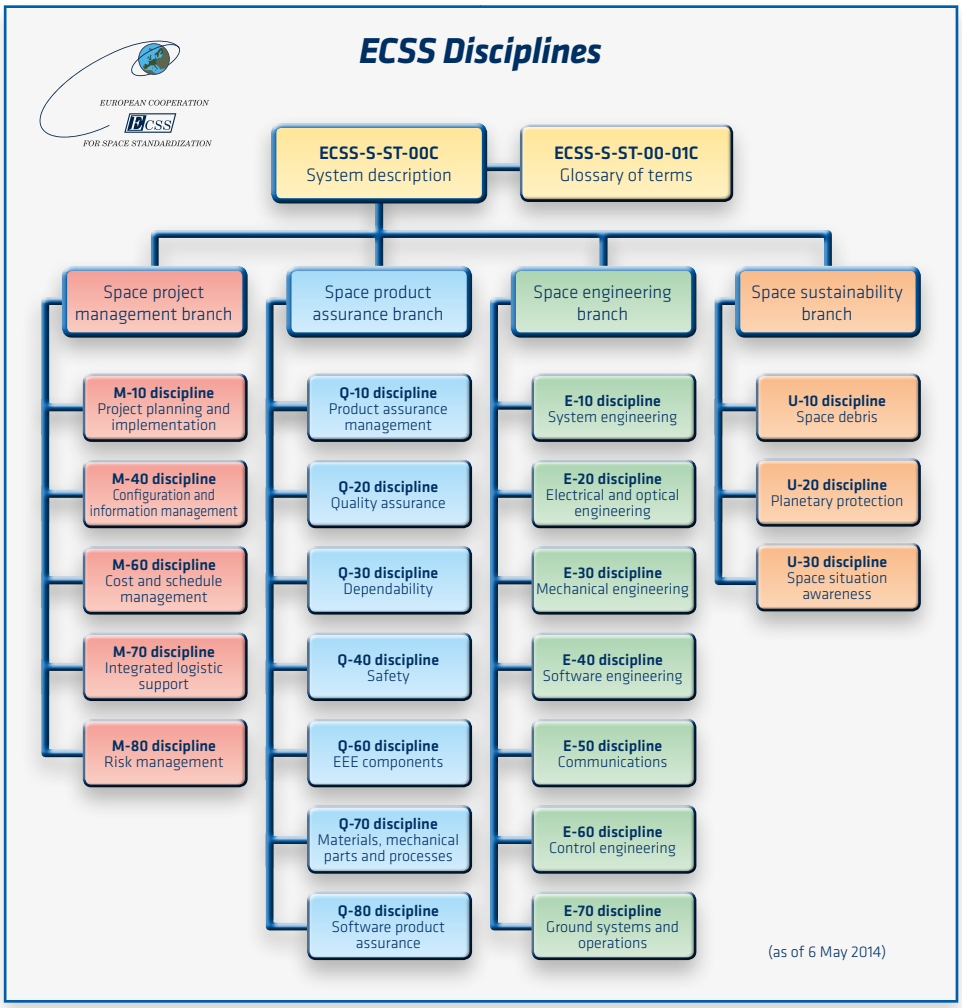
NASA Commercial Safety Certification Document

The safety policy document ESMD-CCTSCR-12.10 "Commercial Crew Transportation System Certification Requirements for NASA Low Earth Orbit Missions" includes four parts:

- ***Certification:*** outlining scope and elements of the certification process: validation of the technical and performance requirements/standards; verification of compliance with requirements/standards; consideration of operational experience; and acceptance of residual technical risk due to hazards, waivers, non-compliances, etc.
- ***Documentation:*** compilation of plans and documents required for submittal at project milestones to collectively prove that the system meets technical requirements and is safe.
- ***Safety Requirements:*** system capabilities in three primary categories of system safety, crew/human control of the system, and crew survival/aborts.
- ***Standards:*** in the fields of engineering, safety, and medical/health, subdivided in those that must either be met as written, or equivalent alternate proposed to NASA Technical Authority for approval, or representing recommended best practices.

for their commercial satellite business, a joint standardization initiative was launched to create a single system of European space standards. The aim was to improve industrial efficiency and competitiveness, by making available a single set of technical, safety/QA, and management standards to satisfy government and commercial contractual needs without differentiation. In the autumn of 1993, European agencies and industry partners signed the ECSS terms of reference which defined the framework and the basic rules of the ECSS system, and concurrently the space agencies committed to gradually discard and replace their own standards with ECSS standards in all future programs. In accordance to the ECSS terms, the European space industry assumed from the outset an equal rank in the direction and development of ECSS standards, and held an equal share of voting rights on their approval.

Several standards in the ECSS system were an adaptation of previous agencies standards, but many new standards were developed in the course of the years. The ECSS technical standards were extensively used for designing European elements, facilities and payloads of the International Space Station, including in particular Columbus module and ATV cargo transportation vehicle.



The previous ESA PSS-01-40 safety standard was the basis for the ECSS-ST-Q-40 "Safety". This standard is essentially a statement of safety policy. It includes four main parts:

- Safety Program: planning, organization, roles and responsibilities, risk management, safety review process, approval authority, training/awareness, documentation
- Safety Engineering: policy and principles, risk reduction and control, failure tolerance, design for minimum risk, safety-critical functions, operations safety
- Safety Analysis Requirements and Techniques: hazard analysis, safety risk assessment, supporting analyses
- Safety Reporting and Verification: hazard reporting, verifications planning and methods, hazard close-out

The ECSS-ST-Q-40 standard identifies three roles: supplier, customer, and safety authority.
The supplier is the system developer.
The safety authority is the relevant government organization having ultimate safety responsibility.
The customer could be an agency, an industrial customer, a space operator, or a recognized third party.

Chapter 5
ESTABLISHING THE SPACE SAFETY INSTITUTE

5.1 WHICH REGULATORY FRAMEWORK AFTER 2023?

On December 23, 2004, President Bush signed the Commercial Space Launch Amendments Act of 2004 (CSLAA). The CSLAA made the Department of Transportation and the Federal Aviation Administration (DOT/FAA) responsible for regulating commercial human space flight. The law established a moratorium (also called 'learning period') for safety regulations of flight participants (crew and passengers) of 8 years, later extended until 2023. The CSLAA just requires operators to provide prospective customers with written information about the risks of spaceflight and a statement that the U.S. government has not certified the vehicle as safe for carrying crew and passengers. For the following 15 years the discussion about commercial human spaceflight safety standards has revolved mainly around suborbital tourism vehicles and has been anchored to the old-fashioned concept that the safety requirements for a new system can be established only when enough operational experience is accumulated. A lose-lose situation because the lack of safety rules leaves the customer potentially unprotected while defeating the fundamental right of industry to operate within a stable set of norms, being safety an attribute that cannot be otherwise defined in absolute and objective terms. The other question, how to deal with NASA procurement of commercial crew transportation services to the International Space Station (ISS), was settled by 2010 because the ISS Inter-Governmental Agreement (IGA) prescribes a role for NASA as safety certification authority for those vehicles in accordance with agreed safety requirements and processes.

The dream of flying to the boundary of space didn't get much farther than Amsterdam for XCOR, where a Lynx model was part of a marketing campaign. (credit: Air&Space Smithsonian/Branko Collin)

Within a decade, human spaceflight operation in Low Earth Orbit (LEO) may become predominantly commercial

While the initial enthusiasm for suborbital spaceflight seems to be fading away following continuous delays, accidents and bankruptcies, the sector of potential space commercial services is widening and gaining momentum. Within a decade, human spaceflight operation in Low Earth Orbit (LEO) may become predominantly commercial. There could be also important elements of private participation to government Moon and Mars exploration missions, which because of high costs could also include international partners (see ESA/Airbus DS cooperation with NASA/LMCO on Orion spacecraft development). The suborbital industry may evolve away from space tourism into a similar mixed-users environment (see recent agreements to buy/operate Virgin Galactic SS2 in Italy and UK), and become more safety-conscious in the perspective of developing future point-to-point transportation vehicles.

Therefore, there is a strong need to establish harmonized safety requirements and a system of recognition of safety certifications to better fit commercial space programs into those emerging programs and markets.

We have seen in the previous chapters the long and sometimes painful process by which safety rules and organizations have matured at NASA. We have seen also the different schemes in use in other industries to perform safety standardization and conformity assessment of commercial products. We will now discuss the possible regulatory frameworks that could be applied to commercial human spaceflight systems when the CSLAA moratorium expires in 2023.

There are four possibilities:

1. **Government regulations**
2. **Consensus standards and third-party certification**
3. **Unregulated self-policing**
4. **Regulated self-policing**

Government regulations. This framework is essentially the same currently used in civil aviation. FAA would issue safety regulations and conduct relevant "spaceworthiness" certifications the same way it does for airworthiness certifications. Unfortunately, such framework is workable with relatively limited human resources and skills of a regulatory body only if prescriptive standards (i.e. rules-based design) are available, which is not the case for space program. We have seen in previous chapters that prescriptive standards are inadequate for highly innovative and fast evolving system developments. Since the eighties, defense and space programs have been the forerunner of the modern use of performance safety standards (i.e. risk-based design). The key advantage of performance standards is that they are to a large extent generic and "configuration neutral", in the sense that the same standard can be applied to the development of a variety of space systems (suborbital, orbital, interplanetary, etc.) and for any level of system complexity, from simple cargo item to a Moon base. However, verification of compliance with a performance safety standard is a crucial and complex task that requires interdisciplinary competences and multidisciplinary review teams with proficiency levels equal or better than design teams. For the current Commercial Crew Program (CCP) those competencies and teams are provided by NASA, but this happens under rather unique circumstances. There is no obvious and simple substitute for NASA's technical capabilities for certifying non-NASA commercial human systems, unless NASA is tasked to perform such role in support of FAA, which is out of NASA's institutional scope.

Prescriptive standards are inadequate for highly innovative and fast evolving system developments

Consensus standards and third-party certification. This is essentially the scheme used for the ISO 9001 Quality Management System certifications. According to such scheme a consensus standard developing organization (ISO, ASTM, SAE, etc.) would set-up a committee (of individuals) to draft a standard on commercial human-rated space systems, which would then be balloted/approved in accordance with the SDO's rules. Then commercial third-parties could offer conformity assessment services and issue conformity certificates. Such approach has many drawbacks. In particular, due to the lack of overarching policies, goals and regulatory oversight, and considering that there are already commercial space systems (suborbital) in the final stages of development, one can expect that the safety standard could fail to reflect "best-practices" (i.e. those used/proven in government programs) and express instead the "lowest common denominator". In other words, a safety standard would be produced that almost any developer/operator could readily achieve. An additional concern is that the SDO's committee could be heavily influenced by those companies whose ability to serve as a reliable standard-setter is doubtful being principal lobbyist and public policy advocate fighting minimum safety regulations. Another concern is the relatively easy admission to serve as expert member on those committees, even when lacking design and/or operation experience, and minimum familiarity with modern risk-based design techniques. Finally, the integrity of commercially-based third party certification, could also be a questionable. Their selection could be driven by cost considerations and "friendly" attitude. Currently there is no industrial sector dealing with safety-critical systems (aviation, nuclear power plants, maritime constructions, etc.) in which such approach is used.

Unregulated self-policing. This is essentially the scheme used by the IAQG (International Aerospace Quality Group) for the Quality Management System certification in accordance with AS9100, the quality standard used also in space programs. The IAQG membership is for companies and institutions and not for individuals. The IAQG is separate and independent from trade organizations. The IAQG provides strategic planning and direction for the standardization activities performed via a SDO (SAE). In addition, the IAQG is directly involved in the accreditation and performance evaluation of the organizations (third-parties) performing conformity assessment and certification. The IAQG model is characterized by the participation of all major aerospace stakeholders worldwide, sometimes fierce competitors in the market (e.g. Boeing and Airbus), and by their active commitment to cooperate to continuously improve the quality performance of the supply chains. The only drawback of applying such scheme to system safety, is the exclusion of any regulatory top function in the direction.

Regulated self-policing. This is essentially the scheme according to which the Institute of Nuclear Power Operations and the Center for Offshore Safety

Allocation of Tasks, Roles and Responsibilities

	COMPANY	SAFETY INSTITUTE	REGULATORY BODY	INT. ORG
POLICIES	-	*advise*	*develop*	*coordinate*
STANDARDS	*implement*	*develop*	*validate*	-
CERTIFICATION	*data*	*perform*	*oversight*	-
PROCESSES	*establish/execute*	*establish/execute*	*establish/execute*	-
AUDITS	-	*Company*	*Safety Institute*	-

COMPETENCE

INDEPENDENCE

AUTHORITY

The regulatory body has the authority to define the overall safety goals and certification program policies. The regulatory body also defines criteria for approving the safety institute as 'recognized organization', and decides on delegated tasks and responsibilities. Development of standards in line with mandated policies, and performance of (safety) certification reviews are the key responsibility of the space safety institute. Implementation of standards, safety-case data submission to the SSI, and safety management system processes are the responsibility of the developer/operator.
Refer to Annex D for further considerations about essential features of a self-policing organization (source: National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling)

where established and operate following the findings and recommendations of the U.S. presidential commissions of 1979 and 2010 respectively. Companies cooperate through the institute/center towards the safety common goal by issuing standards and verifying compliance, under government broad direction and control. This is also the scheme proposed in this document for the establishment of the Space Safety Institute. It combines the advantage of empowering the stakeholders (in the case of space, industry, FAA, and NASA as customer) to direct and fund the resources needed to achieve rapid response flexibility in standardization and conformity assessment activities, with affordable access to shared skilled resources, under the assurance of pursuing public interest provided by the regulatory body involvement.

5.2 BUILDING THE SPACE SAFETY INSTITUTE

For commercial human spaceflight to flourish and expand, industry must build on the experience accumulated until now in government space programs and cooperate between them, with institutional customers, and with regulatory bodies to advance safety as common strategic goal. For such purpose, the International Association for the Advancement of Space Safety (IAASS) and the International Space Safety Foundation (ISSF) are promoting the establishment of a Space Safety Institute (SSI). The SSI main mission would be to establish and manage a safety certification process for commercial human rated systems which is lean, effective, and does not stifle innovation. A process that allows maximum design freedom and quick and efficient reaction to technological advancement. For such purpose the Space Safety Institute would be organized around two concepts: “regulated self-policing” and “safety-case”. The “safety-case” approach leaves the definition of (safety) design solutions and operational procedures to the developer/operator, while placing the responsibility for validation of system’s compliance into the hands of an independent team of experts. Instead the “regulated self-policing” regime gives to the stakeholders’ community the responsibility to define the safety (performance) standards and organizational processes that must be followed to ensure that government issued safety policies and goals are met.

The Space Safety Institute would be somehow a “middle-man” between the regulatory body and the commercial

The Space Safety Institute would be organized around two concepts: "regulated self-policing" and "safety-case"

space companies for the benefit of both parties. The SSI would provide standardization and safety certification services as a "recognized organization" approved by and operating under oversight of the regulatory entity. The Space Safety Institute would include:

1) **Standardization secretariat:** for detailed annual planning of standardization activities, issuing of operating procedures, and monitoring progress of working groups activities, publications of standards.

2) **Safety review panel:** for reviewing certification data packages, approval of hazard controls/verifications, and providing recommendations to safety authority on waivers/deviations to policy requirements

3) **Safety Management System auditing function:** for periodically auditing companies' safety organizations, design, operations and management processes, safety capabilities and performance.

The Space Safety Institute would also coordinate, support and promote research in the field of space safety engineering, support educational programs, and provide professional training opportunities to members.

Public safety, space traffic management, environment protection and international coordination would remain outside the scope of the Space Safety Institute, and entirely under the responsibility of the relevant regulatory authority.

5.2.1 Standardization activities

At NASA a large body of knowledge exists in the form of specifications, standards and handbooks, which has been accumulated in several decades of space programs. However, they cannot be directly used in commercial programs because on one hand the language used reflects customer-contractor relationship and the organization of specific government programs, while on the other hand, they were established internally to serve the agency's own ultimate objectives and policies.

An inventory of such technical standards was already performed by NASA as recommended practices for possible use by companies involved in the Crew Commercial Program. Those standards could be reviewed, adapted and re-issued as commercial standards with relatively minor effort. They would represent the starting reference for the development of a wider and coherent set of commercial space systems safety and technical standards. However, for safety, a single NASA standard does not exist. Safety requirements developed since the Shuttle program were either embedded in system specification or issued as program safety specification (e.g. SSP 50021, the International Space Station safety standard). The IAASS has performed a compilation of those safety requirements (see IAASS-SSI-1700) such to represent an envelope of the current best-practices.

Participation to SSI standardization activities would not be restricted to SSI Partners but would be open to any company, government organization, and non-government organization involved in space studies, developments, and operations, or procuring commercial space systems and services.

The tenets of the SSI standardization activities are competence, inclusiveness, use of proven best-practices as starting point, and commitment to continuous improvement of system safety engineering and management practices. Details on the SSI initiative are provided by a separate document in the form of draft Memorandum of Understanding (MoU).

5.2.2 Safety Review Panel

The SSI Safety Review Panel (SRP) will be responsible for conducting flight safety reviews. The SSI SRP will assist the developer/operator in assuring that safety critical systems, subsystems and operations are appropriately designed and verified. Specifically, the SSI Safety Review Panel will perform the following functions:

a) Assisting the developer/operator in interpreting safety requirements in a manner consistent with applicable requirements, and providing recommendations for implementation.

b) Conducting safety reviews as appropriate during various phases of system development and operation.

c) Evaluating changes to system that either affect a safety critical subsystem or create a potential hazard to interfacing systems, or crew.

d) Evaluating safety analyses and safety reports, and processes Non-Compliance Reports.

e) Ensuring the resolution of system safety issues.

At the successful conclusion of safety reviews cycle, the SSI Safety Review Panel Chair would submit a Certificate of Flight Readiness (CoFR) to the regulatory organization (FAA).

Safety Review Panel Chair

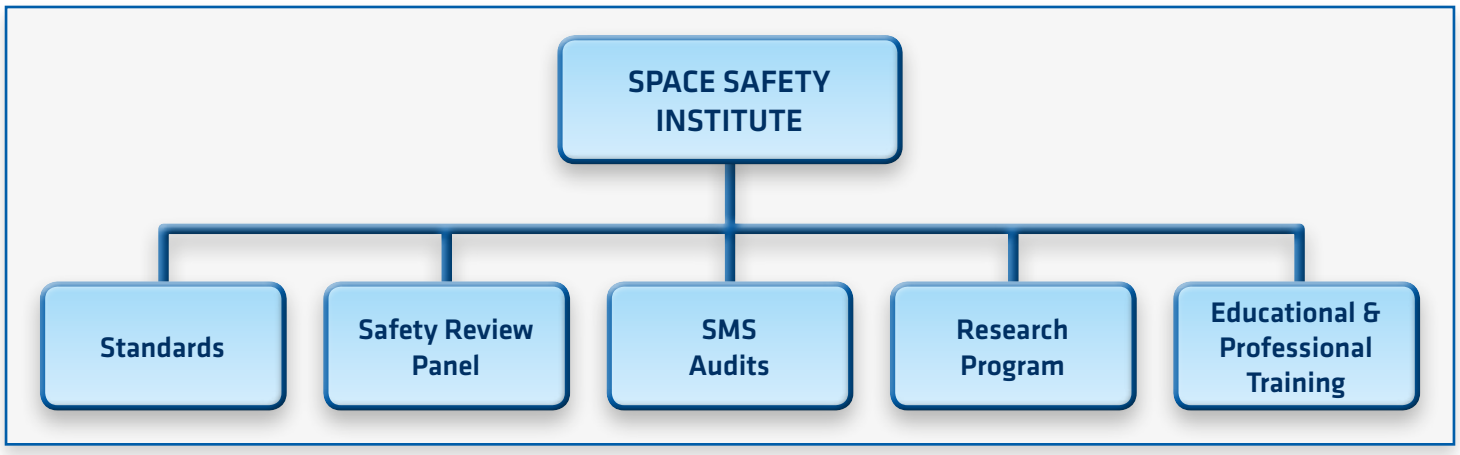
The SSI SRP Chair would be a staff of the SSI and would be appointed by the SSI Board. The SSI SRP Chair would define and implement the flight safety review processes for the system under certification, including assessing compliance with safety requirements and policies to assure safety of the vehicle, crew, and other interfacing systems. The SSI SRP chair would have the authority to approve individual phase safety review completion by signature of the relevant safety-case reports and to make panel decisions, considering recommendations from the other panel members of the safety review panel.

Safety Review Panel Executive Secretary

The SSI SRP Executive Secretary would be a staff of the SSI and would be appointed by the SSI Board. The Executive Secretary would ensure consistent implementation of safety process requirements as the principal administrative officer for the SSI SRP. The Executive Secretary would maintain the administrative records of the panel, coordinate the administrative check of incoming data, and ensure delivery of data to SRP Members. The Executive Secretary would coordinate and schedule formal flight safety reviews and technical interchange meeting. The Executive Secretary would draft and record action items for review and concurrence by the SSI SRP Chair and by the system developer/operator. An important task of the Executive Secretary would be the preparation of the annual plan of panel members resources required, and to issue the relevant work orders.

Safety Review Panel Members

The members of the safety review panel would be independent contractors of the Space Safety Institute, They would be proposed by SSI management or SSI Partners, and selected/appointed by the SSI Board, based on criteria such as competence, lack of conflict-of-interest, etc. The members of the Safety Review Panel would be engaged through work-orders for discrete durations of time. The members would be experts in the following disciplines (non-exhaustive list): safety & mission assurance, operations (crew operations, robotic operations, proximity operations, etc.), mechanical engineering (structures, pressure systems, mechanisms, materials, etc.), electrical/avionics (batteries, power distribution, GN&C), computer systems, propulsion, pyrotechnics, life support & habitability, toxicology, medical representative. The member would receive at the time of the first appointment a dedicated training by the SRP Executive Secretary on the safety review processes and requirements, and on panel members responsibilities and duties.

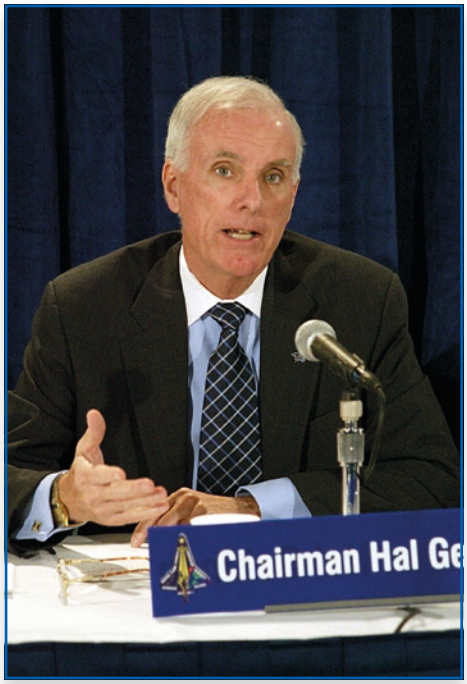


Chapter 6
SAFETY RESEARCH PROGRAM

6.1 NESC

The Space Safety Institute research program operation would be modeled to some extent after the NASA Engineering and Safety Center (NESC).

After the Shuttle Columbia accident, the investigation was entrusted to the CAIB (Columbia Accident Investigation Board) chaired by Admiral Harold Gehman. As the investigation progressed, the CAIB Chairman provided briefings and updates to NASA, the U.S. Congress, and the American public. On one such occasion in July 2003, speaking publicly following a Congressional briefing, Gehman stated: *"The safety organization sits right beside the (Shuttle) person making the decision, but behind the safety organization there is nothing there, no people, money, engineering, expertise, analysis … there is no 'there' there."*



Admiral Harold W. Gehman,

NASA responded within weeks to this statement announcing the formation of the NASA Engineering and Safety Center or NESC to provide programs an alternate perspective on difficult technical issues. The NESC fills this need by bringing together technical experts from across NASA, industry, other government agencies and academia and leveraging their expertise to solve problems.

The NESC is made of a core organization composed by Director, permanently assigned technical personnel, and management offices, and a network of on-call experts remotely located. The NESC operates in a "tiger-team" model when conducting studies and assessments, forming a dedicated team of subject matter experts to address a well-defined technical issue. The key functional groups inside NESC are the Principal Engineers Office, providing study leadership and management, particularly for longer term, multidisciplinary assessments, and the Technical Fellows Office. Technical Fellows are recognized technical leader in their specific discipline. Each TF maintains a Technical Discipline Team consisting of experienced subject matter experts from other NASA Centers, U.S. Government Agencies, academia, and industry.

Behind the safety organization there is nothing there, no people, money, engineering, expertise, analysis

The NESC NRB decides on accepting new studies or assessments according to the following priorities:

1) Technical support of projects in the flight phase
2) Technical support of projects in the design phase
3) Known problems not being addressed by any project
4) Work to avoid potential future problems
5) Work to improve a system

Max Launch Abort System test, July 8, 2009 at the NASA Wallops Flight Test Facility.

The NESC Review Board (NRB), composed by Technical Fellows and senior NESC managers as voting members, evaluates and approves each technical study and plan, monitors assessment progress, and reviews and approves the final report and recommendations to ensure technical rigor and accuracy.

Each final report is peer-review internally and externally to the NESC, and receives final scrutiny and approval from the NESC Review Board before publication. Since in some cases, assessment results must be delivered to the requester before the final report is complete, the NESC Review Board may also review and approve FORs separately from the report, with the expectation that they are final and will not change.

The NESC, in addition to assessments addressing near term mission needs, has undertaken several large-scale, risk-reduction projects for major NASA programs that, for one reason or another, the program could not undertake on its own. These projects include the Max Launch Abort System (MLAS). The NESC undertook the Max Launch Abort System project to develop and flight-test an alternative launch abort (escape) system design, as compared to NASA's traditional tower-based design used during Projects Mercury and Apollo.

6.2 THE SPACE SAFETY INSTITUTE RESEARCH CENTER

The Space Safety Institute Research Center (SSIRC) research program would have two main objectives:

1) supporting on going commercial projects risk assessments, as the need arises;

2) development of advanced risk controls.

The SSIRC would make available, upon request, extra expert support to the SSI Safety Review Panel and to commercial developers/operators for the evaluation of special safety issues or for the performance of independent assessment of complex cases, like unresolved anomalies or "equivalent safety" solutions.

Election into the SSI Technical Fellowship would follow a formal process. Prospective Technical Fellows would be nominated by SSI Members, and evaluated by the SSI management based on five criteria:

1) Technical knowledge and judgment
2) Creative problem solving and innovation
3) Technical leadership, advising and consulting
4) Capability as a teacher and mentor
5) Technical vision

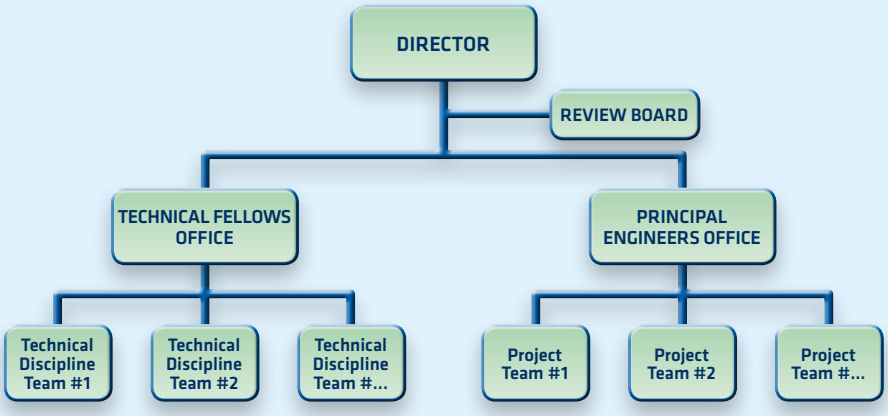
"Equivalent safety" is a key feature of performance-oriented safety requirements to allow maximum flexibility and freedom to designers. "Equivalent safety" refers to conditions that do not meet specific safety requirements in the exact manner specified. However, the system design, procedure, or configuration satisfies the intent of the requirement by achieving a comparable or higher degree of safety. Criteria are based on: (a) use of alternative methods/controls; (b) utilization of procedures, protective devices, pre-flight verification activities, and crew experience base; (c) reduced time of exposure; (d) likelihood/probability of additional failures after loss of first control/inhibit; reduction of hazard category, and/or other factors such as minimum of single FT with a robust design. "Equivalent safety" requires careful consideration and need to be investigated on a case-by-case basis. However, the lessons learned during such investigations represent an important knowledge data base to be maintained in support of the safety review panel.

The SSIRC would be made of a core organization composed by director, permanent technical personnel, and management offices, and a network of on-call experts remotely located. The SSIRC would operate in a "tiger-team" model when conducting studies and assessments, forming a dedicated team of subject matter experts to address a well-defined technical issue. The key functional groups inside the SSIRC would be the Principal Engineers Office, providing study leadership and management, particularly for longer term, multidisciplinary assessments, and the SSI Technical Fellows Office. SSI Technical Fellows would be recognized technical leader in their specific discipline. Each TF would maintain a Technical Discipline Team consisting of experienced subject matter experts from NASA, U.S. Government Agencies, academia, industry and professional associations.

The SSIRC would establish a Review Board (RB), composed by SSI Technical Fellows and senior SSIRC managers as voting members, to evaluate and approve each technical study and plan, monitors assessment progress, and reviews and approves the final report and recommendations to ensure technical rigor and accuracy. In case of an assessment performed on behalf of a company, a company nominated representative will be included as voting member of the Review Board for the relevant assessment plan and technical report. The publication and distribution of reports would be subjected, in principle, to the same clauses of confidentiality applied for the activities of the safety review panel.

The budget of the SSIRC would be managed in accordance to the principle that the activities performed by the permanent technical personnel would be charged as SSIRC costs, while those performed in support of a specific (commercial) project, either upon SRP request or as request by a company, would be charged to the company, as per dedicated contract.

Space Safety Institute Research Center Matrix Organization



Space Safety Institute Research Center Products

Assessment Engineering Reports
The detailed engineering and analyses generated from each assessment would be captured in comprehensive engineering reports and converted into SSI Technical Memorandums (TM) for permanent archive and access by all SSI Partners.

Technical Bulletins
Occasionally, significant and noteworthy data found during SSIRC assessments would be turned into one-page technical bulletins. The bulletins condense new knowledge or best practices into quick and easy reads, while also linking to additional reference material.

Lessons Learned
Safety lessons learned database would be used to capture important and broadly applicable lessons learned. In some cases, the lesson may be significant enough that it would be used as input to update an SSI standard.

Safety Review Panel Support Reports
Special reports prepared in support of the SSI Safety Review Panel, for their internal use. The reports would analyze new, complex or unique design solutions for acceptability with reference to an applicable generic safety requirement in the standard. The detailed engineering and analyses generated from each assessment would be captured in comprehensive engineering reports for internal use by the SRP.

Chapter 7
SAFETY EDUCATION AND PROFESSIONAL TRAINING

7.1 AN UNANSWERED NEED

Since its inception, the International Association for the Advancement of Space Safety (AASS) has identified *education* and *professional training* as key enhancer of space safety. Training is different from education. Several high technology organizations clearly make a key distinction between the concepts of education and training.

- We accept the concept that education is *"instruction and study focused on creative problem solving that does not provide predictable outcomes. Education encompasses a broader flow of information to the student and encourages exploration into unknown areas and creative problem solving"*. Graduate level education requires time to complete and often culminates with an original research endeavour. Such an educational program prepares individuals for careers and includes practice in critical and creative thinking that will in many ways last throughout a career.

Space system safety engineering methods and risk management techniques are not generally taught in depth in aerospace engineering schools

- We also accept that training can be defined as *"instruction and study focused on a structured skill set to acquire consistent performance. Training has predictable outcomes and when outcomes do not meet expectations, further training is required."* Training is much more short term and typically takes days to a week or two to complete.

Space system safety engineering methods and risk management techniques are not generally taught in depth in aerospace engineering schools. In the early times of space programs, after the Apollo 1 accident, engineers had to gain a broad understanding of multidisciplinary system safety aspects such to be able to perform integrated analyses, without the benefits of any specialized education background or professional training. Knowledge was developed through internal information exchanges, brain storming, discussions, and short seminars. Later those pioneer safety engineers started teaching newcomers in a sort of master-to-apprentice relationship, usually with much focus on administrative tasks, which represented the entry level into the safety job. As the system engineering community becomes increasingly aware that safety must be designed-in from the very beginning or risk escalating project costs, schedule delays, and a pile of safety non-compliances, the need for safety

IAASS has published four unique textbooks in the field of space safety

IAASS publishes a quarterly journal

education and training is being felt not only by the safety people but by the entire project team.

In 2009 the IAASS started the publication of university textbooks in the field of space safety, The first book, "Safety Design for Space Systems", was followed in 2011 by "Space Safety regulations and Standards, then in 2013 "Safety Design of Space Operations", and more recently "Space Safety and Human Performance" (2018).

The IAASS unique textbooks are widely considered to be essential reference for those that engage in formal study of space safety and represent a good foundation on which to build the SSI educational and professional training programs.

7.2 EDUCATIONAL AND TRAINING PROGRAMS

The effective education and training of professionals in the space safety field depends on the availability of relevant and up-to-date academic and training courses in all areas related to space safety. The aim of the SSI education and training programs is to create opportunities for and to manage the "circular" transfer of knowledge, from space agencies to industry and academia, and vice-versa. We can distinguish different levels of knowledge transfer: "know what," "know how" and "know why". The "know what" knowledge provides awareness of issues and problems and what action to take when one is presented with them. An astronaut on the international space station trained about what to do in case of air leakage and other emergency situations acquires a "know-what" level of knowledge. The next higher level of knowledge is "know-how". An engineer can be trained about how to perform a hazard analysis or how to estimate the level of risk. Such knowledge is required when the simple knowledge about the action to be taken, which is the essence of "know-what" knowledge is insufficient, and instead a process must be learned about how to establish the actions to be taken (as part of design, manufacturing or operations). For example, this could be the case of learning which rules to follow to design a spacecraft to prevent air leakage. Finally, the third level of knowledge, the highest, is the "know-why" knowledge. At this level, an individual has a deep understanding of causal relationships, interactive effects and the uncertainty levels associated with issues and problems. This will usually involve an understanding of underlying theory and/or a range of experience that includes many instances of anomalies, interaction effects, and exceptions to the norms and conventional wisdom of an area. The Space Safety Institute should provide professional training courses, focused on "know what" + "know how", and undergraduate and postgraduate university levels courses, focused on "know how" + "know why". Annex C provides an outline of the SSI educational and training programs.

Remote Learning Center (Courtesy: University of Southern California)

Annex A

COMMENTS ON THE HOUSE FLOOR UPON INTRODUCING A BILL TO ENHANCE THE SAFETY OF COMMERCIAL SPACE FLIGHT

By Rep. James Oberstar

Tuesday, February 8, 2005

Mr. OBERSTAR. Mr. Speaker, today I have introduced a bill to enhance the safety of commercial space flight by ensuring that the Federal Aviation Administration (FAA) has the authority it needs to protect the safety of passengers of the emerging commercial space industry.

Mr. Speaker, I support commercial space exploration and the commercial space industry, but not at the expense of totally ignoring safety. The Commercial Space Launch Amendments Act of 2004, P.L. 108-492, prohibits the Secretary of Transportation from issuing safety design and operating regulations or even minimal safety requirements for individual licenses for the next eight years unless there is a potentially catastrophic incident.

The current statutory language amounts to, in essence, the codification of what has come to be known in aviation safety parlance as the "Tombstone Mentality." For years, both I and many of my colleagues on the Aviation Subcommittee have criticized the FAA for waiting until after a disaster to take safety actions, and have urged more proactive safety oversight.

Supporters of the Commercial Space Launch Amendments Act argued that safety regulation would discourage experimentation and innovation. However, the Act went well beyond these objectives and essentially tied FAA's hands by totally banning any safety requirements, except in post-accident circumstances where lives have already been lost. Under the Act, the FAA would be prevented from requiring even the simplest, least expensive enhancements to protect safety of passengers on these space flights.

Mr. Speaker, my bill would amend the Commercial Space Launch Amendments Act to give the FAA the authority and flexibility to establish minimum safety regulations. My bill would not preclude innovation and, contrary to the claims of supporters of the Act, my bill would not require FAA to impose the same degree of regulation on the developing space travel industry that is imposed on the mature air transportation industry. Specifically, although my bill would require that FAA include, in each license it issues, minimum standards to protect the health and safety of crews and space flight participants, it would further require that, in imposing these standards, FAA must take into account the "inherently risky nature of human space flight." My bill would give the FAA the flexibility to create a regulatory structure governing the design or operation of a launch vehicle to protect the health and safety of crews and space flight participants as is necessary, without having to wait for a catastrophic failure to occur.

Mr. Speaker, safety regulation need not be incompatible with developing new technology. For example, although FAA has closely regulated aircraft manufacturing since the 1920's, this regulation has not prevented major technological progress, including the development of jet aircraft in the 1950's and all-composite general aviation aircraft in recent years. We can and should protect the safety of passengers on space flights in this new and emerging industry, without placing unreasonable limitations on industry development. I urge my colleagues to join me in working to pass this important legislation.

NOTE: The Bill did not pass. Hon James L. Oberstar became two years later Chairman of the House Transportation and Infrastructure Committee from 2007 to 2011.

Annex B

"SAFETY IS NOT PROPRIETARY" STATEMENT TO THE NATIONAL COMMISSION ON THE BP DEEPWATER OIL SPILL AND OFFSHORE DRILLING

By Rex Tillerson, Chairman and Chief Executive Officer Exxonmobil

November 9, 2010

America's oil and natural gas resources are the foundation of our nation's economy and our standard of living, and it is essential that we ensure the safe production of these resources.

This country — as well as the global energy industry — will benefit from a full understanding of the causes of the Deepwater Horizon incident. I am confident that the commission's findings will help advance our goal, which is to ensure that all our nation's energy facilities are operated at the highest standards of safety.

So, I am grateful for the chance to come before the commission today to share ExxonMobil's approach to safety, operational integrity and risk management. Many would say, especially now, that energy companies must make safety a "top priority" — but I believe that a commitment to safety must run much deeper than simply being a "priority."

A company's priorities can — and do — evolve over time depending on business conditions and other factors. A commitment to safety therefore should not be a priority, but a value — a value that shapes decision-making all the time, at every level.

Every company desires safe operations — but the challenge is to translate this desire into action. The answer is not found only in written rules, standards and procedures. While these are important and necessary, they alone are not enough.

The answer is ultimately found in a company's culture — the unwritten standards and norms that shape mindsets, attitudes and behaviors. Companies must develop a culture in which the value of safety is embedded in every level of the workforce, reinforced at every turn and upheld above all other considerations.

I've been asked today to explain how ExxonMobil approaches these critically

important areas of systems and culture when it comes to safe operations and risk management.

OIMS

The evolution of ExxonMobil's safety culture dates back to the 1989 Valdez spill. As I have said before, Valdez was a low point in our history. It was a traumatic event, with enormous consequences for all involved. But it also served as a catalyst and a turning point which prompted our management to completely reevaluate how ExxonMobil understands and manages risk.

That is not to say that, prior to Valdez, we did not take safety seriously. ExxonMobil had been in business for more than 100 years, and we had always taken steps to maintain safe operations as risks changed and energy technologies evolved.

We were proud of our safety record. We believed, as our safety credo at the time stated, that all accidents and injuries are preventable. Like many companies, we worked to meet or exceed all industry safety standards, trained our employees in safety procedures, and tracked certain metrics that measured our success. But we did not have a comprehensive, systematic view of this aspect of our business that we have today.

And so, in the early 1990s, ExxonMobil's management undertook what I consider to be a visionary approach. The goal was to wholly reorganize the company to make safety — of people, facilities and the environment — the center of everything we do. Safety would come first, period.

It was the beginning of a long journey for our company. And I should make it very clear: this is a journey that we have not completed. We know that we cannot rest or waver from the goal of driving accidents and incidents to zero. And we're not there.

But we have made significant progress. And, as we have learned, for this progress to be achieved, its impetus had to come from within the company. We could not have government impose a safety culture on us, or hire someone to do it for us. Experts and consultants do provide a valuable service, but for an organization to change its culture, change must come from the inside-out, not the outside-in. You cannot buy a culture of safety off the shelf — you have to craft it yourself.

So we began. We began by creating a framework that puts our safety commitment into action. Today, that framework is called the Operations Integrity Management System, or OIMS for short.

Because OIMS is multi-faceted, it can be hard to describe briefly. Here are the basics: OIMS is a rigorous 11-point set of elements designed to identify hazards and manage risks. Its framework covers all aspects of safety; management leadership and accountability; design, construction and maintenance of facilities; emergency preparedness; management of change; assessment of performance; and, of course, thorough inquiries into accidents and incidents.

OIMS guides the activities of each of ExxonMobil's more than 80,000 employees, as well as our third-party contractors, around the world. Over time, it has become embedded into everyday work processes at all levels.

Through OIMS, ExxonMobil monitors, benchmarks and measures all aspects of our safety performance. Its structure and standards are shared and communicated the world over. One of the greatest benefits of OIMS is that it has enabled ExxonMobil — a large organization that operates across diverse cultures and geographies — to be of one mind when it comes to safety and risk management. I can visit a refinery, a lab or an offshore platform anywhere in the world and immediately be on the same page as the local employees and contractors regarding safety practices and expectations.

And I want to stress that the contractors that we work with are embedded within our OIMS processes as well. We expect our contractors to be as knowledgeable and conversant with our OIMS processes as our own employees. Not every company has this expectation, but we have found that when everyone in the workplace speaks the same language of safety — employees and contractors alike — everyone can work collaboratively, safely and effectively.

You may have heard the phrase: "If you can't measure it, you can't manage it." And it's true. And that is why ExxonMobil measures and analyzes its safety performance — all the time, all the way down to every business level. We record not just our injuries, but we record our near misses and our close calls. Our goal is not just to analyze safety incidents after they happen, but to identify risks and risky behaviors before they lead to a safety incident. The more elements of risk to be managed in an activity, the more frequently we test, measure and analyze the safety approach in that activity.

More broadly, OIMS requires us to audit the health of the overall safety approach in all of our operating environments, on a regular basis. Importantly, these audits at ExxonMobil are performed not only by trained safety personnel, but by cross-functional, cross-regional teams drawn from all over our global organization. In this way, all employees are responsible for each other's safety. Also, the knowledge employees gain by participating in these audits is taken home to their jobs, and spread throughout the organization.

Leadership

Yet, OIMS by itself is only one part of the equation. Even the best safety systems are not fully effective unless they exist as part of a broader culture of safety within the people of the organization.

While ExxonMobil and other energy companies use a lot of equipment — everything from steel pipe to supercomputers — it is people who bring this equipment to life. And people's behavior is heavily influenced by their culture.

By instilling the value of safety in our employees from the first day of hire, ExxonMobil strives to create a working environment in which safe behaviors are internalized; they're reinforced; and they're rewarded.

The culture of safety starts with leadership — because leadership drives behavior and behavior drives culture. Leaders influence culture by setting expectations, building structure, teaching others and demonstrating stewardship.

And that is why the first element of OIMS is "management leadership and accountability." ExxonMobil managers are expected to lead the OIMS process by demonstrating a visible commitment to safety and operations integrity. In addition, safety leadership is a significant part of how a manager's overall performance is evaluated.

As chairman and chief executive, I know that a commitment to safety and operational integrity begins with me and the rest of ExxonMobil's management team. But management alone cannot — and should not — drive the entire culture. For a culture of safety to flourish, it must be embedded throughout the organization.

Therefore, safety leadership at ExxonMobil comes not just from supervisors and managers, but from employees and contractors, and through channels both formal and informal.

ExxonMobil's goal is not simply to have employees comply with safety procedures. A culture of compliance alone can lead to complacency. We seek to go beyond compliance, to create a culture in which employees are not only meeting the safety procedures, but they are challenging them so they can be improved wherever needed.

Achieving A Sustainable Culture of Safety

I do not want anyone to think — inside or outside our company — that pride in our safety systems means we can relax our commitment. The exact opposite is true. To get where we need to be on safety, continuous improvement is essential.

In an industry such as ours — which operates 24 hours a day, around the world — the need to manage risk never ends. Even the best safety framework should be viewed as a work in progress.

Developing a culture of safety therefore is not an event, but a journey. For ExxonMobil, that journey began more than 20 years ago, when we put our global safety framework in place.

Once that framework became embedded in our organization, we saw the culture start to change and the results became evident in improved performance. In turn, this allowed us to move from implementing the system to improving it.

That's when ExxonMobil's culture was really transformed. Over the years, I have seen people at all levels understand that our safety systems are put in place for them, that they are about protecting them and their coworkers and the public, and not about catching people doing the things wrong.

Part of that transformation is recognizing that every employee's job involves some degree of risk management — even those employees who work in office settings. That is why OIMS extends even to administrative locations.

When an organization reaches the point where everyone owns the system and believes in it, only then at that point, the culture of safety and operational integrity has been established that can be sustained — when it enters the hearts and minds of the people of the organization and becomes a very part of who we are.

We often use the phrase at ExxonMobil, "Nobody Gets Hurt" to describe our safety objective. Some observers of our company question this; they say it can't be done. Well, it can be done. We have operating units today that have gone years without a recordable injury.

Our challenge is to sustain that performance where it has been achieved, and to replicate and grow that record of performance across the organization. I have no doubt that every single employee shares this goal.

Risk/Change

Considering that many of ExxonMobil's energy projects can span decades, achieving the goal of a self-supporting, sustainable energy culture means we must be flexible and adaptable to changes in the operating environment.

As a result, management of change is a key component of our OIMS system. Our management of change processes are designed to ensure that with any change in our business or operations, we recognize the changed conditions, we actively identify the new or changed risks, and we apply our disciplined processes for managing the risks and their potential consequences.

Risks are addressed and the change is managed - typically through either technological solutions, or operating changes in response to the potential risk. But most importantly, it is clear who owns the management of change and the subsequent risk management, and every employee and contractor is important to that process.

These very deliberate, well-established processes, embedded in OIMS, have enabled ExxonMobil to pursue challenging new resources and new development projects with the confidence that we will do so safely and responsibly.

Such an approach is not only in the interests of employees and resource owners — but clearly it is also in the interests of our shareholders.

Best Practices

Which leads me to my next point: Upholding the highest standards of safety and operational integrity is not just "the right thing to do" — a phrase we sometimes associate with an act of selflessness; it is also in a company's self-interest, because it makes for more competent, more productive employees and organizations.

The rigor, discipline and degree of accountability required to improve safety performance are the same qualities that produce successful business results — operationally and fiscally.

Safety is not proprietary. And for this reason, ExxonMobil shares its best practices within our industry, and across other industries.

We seek to learn from others. After the 2003 Columbia space-shuttle explosion, ExxonMobil assembled a team of engineers, scientists and safety experts to study the technological and organizational factors that may have led to that disaster, and whether there were any lessons for ExxonMobil's operations.

It is by constantly learning and analyzing — by looking to best practices in other organizations, and by examining incidents and near-misses in our own organization — that we continually improve our own performance.

Deepwater

I know this commission has heard a lot about the importance of deepwater energy supplies, but it bears repeating. The technology that has enabled our industry to reach the oil and gas found in deepwater fields is one of the most significant energy-security developments of the last 20 years. Deepwater production, which did not exist prior to 1989, today makes up 15 percent of all non-OPEC production. By 2030, it will grow to nearly 20 percent. Along with Brazil and West Africa, the Gulf of Mexico is one of the most important deepwater provinces in the world.

In 2008, there was more oil and gas discovered in deep water than in onshore and shallow water combined. For the sake of our energy security, and the economic growth and jobs that depend on the production of these supplies, we simply cannot afford to turn our backs on this resource.

Neither can we miss the opportunity to improve safety in the Gulf of Mexico. The Macondo blowout cost 11 lives, and billions of dollars in economic and environmental damage. If we don't learn lessons from this disaster, it will have been a double tragedy.

As Chairman Reilly said at this commission's first meeting back in July, we must "come to grips with this disaster so we can never see its like again."

MWCS

I spoke earlier about risk management being a constant challenge. While ExxonMobil believes that incidents like the Deepwater Horizon spill should not happen if industry best practices are followed, the spill did expose that our nation, and the energy industry, could have been better prepared for the possibility, however remote, of a deepwater well blowout. That is why ExxonMobil is leading a multi-company effort, along with my colleague [Marvin Odum, Shell] today, to build a new rapid-response oil containment system in the Gulf of Mexico. This system — involving a $1 billion initial commitment from the four sponsor companies — is unprecedented in our industry. It will provide pre-engineered, constructed, and tested containment technology and equipment to be deployed within 24 hours of a deepwater spill in the Gulf.

In addition, ExxonMobil and other operators in the Gulf of Mexico, in conjunction with the Department of Interior, have instituted new requirements regarding inspection and certification of blowout preventers, well casing designs and cementing procedures.

I believe that these steps, in addition to the inspections performed on all deepwater rigs in the months following the Deepwater Horizon incident, will enable the Gulf region, and the entire country, to continue to develop our nation's energy resources with confidence.

Conclusion

In concluding I'd like to share this thought: ExxonMobil is sometimes viewed as a cautious company; we're sometimes criticized for being too cautious. And yet, meeting the world's growing demand for energy involves a high degree of risk; our employees operate some of the world's most complex technologies in some of the world's harshest environments.

How we continue to progress technologically while dealing with significant risk is that human progress does not mean avoiding risk; it means managing risk by identifying it, and taking steps to mitigate it. No company — including my own — can lay claim to a one hundred percent success rate in this endeavor. Yet that remains our clear goal.

In closing, there are three points that I hope the Commission will consider in its deliberations: First, a culture of safety has to be born within the organization. You cannot buy culture. You have to make it yourself.

Second, make no mistake: creating a strong, sustainable safety culture is a long process. If an organization is truly going to overhaul its approach to safety, it has to be committed from day one. But, you can't start until you start — and you're never going to finish.

Finally, I want to return to OIMS. I mentioned that there are eleven elements, all of which are fundamental to safe and responsible operations at ExxonMobil. But the first and last elements — the bookends of OIMS — are the most critical.

These are "Management Leadership and Accountability", and "Operations Integrity Assessment and Improvement". Without leadership by example and without thoughtful, honest and objective self-assessment, no system is sustainable.

Our nation, and our world, continues to face challenges. Meeting the world's growing demand for energy — safely, and with minimal impact on the environment — is one of our biggest. In examining the causes of the Deepwater Horizon incident, this commission is helping advance our progress toward this goal.

ExxonMobil strongly supports your inquiry, and remains committed to supporting the cause of safety within our company and beyond.

Annex C

EDUCATIONAL AND PROFESSIONAL TRAINING PROGRAMS

C.1 SAFETY EDUCATION PROGRAM

The SSI education program could consist of two main components:

- Postgraduate Certificate in Space and Aviation Safety, ten weeks in-class
- Undergraduate courses on dedicated topics, 21 hrs/course, distant learning

This study output would be a definitive outline of the 18 Credit (Half of Masters) international Postgraduate Certificate Program in Space and Aviation Safety, and of regionally available web-based undergraduate courses on space and aviation safety. It would provide information on possible instructors, and information with regard to the instructional program and all pre-program and post program activities. The SSI Academic Program is very roughly outlined below and is subjected to change and refinement as part of the study process based on key faculty availability, indicated need for educational courses in these disciplines as well as the result of other input from space agencies, aerospace agencies, research centres, or universities that might participate.

Web-based learning is often called online learning or e-learning because it includes online course content. Discussion forums via email, videoconferencing, and live lectures (video streaming) are all possible through the web. Web-based courses may also provide static pages such as printed course materials. One of the values of using the web to access course materials is that web pages may contain hyperlinks to other parts of the web, thus enabling access to a vast amount of web-based information. A "virtual" learning environment (VLE) or managed learning environment (MLE) is an all in one teaching and learning software package. A VLE typically combines functions such as discussion boards, chat rooms, online assessment, tracking of students' use of the web, and course administration. VLEs act as any other learning environment in that they

C.1.1 Postgraduate Certificate Courses

The 10-week postgraduate certificate will be split in:

- **"Human Spaceflight Module"** of 5 weeks duration
- **"Space and Air Legal and Regulatory Module"** of 1 week duration
- **"Space Operations Safety Module"** of 4 weeks

Human Spaceflight Module (5 weeks)	Space and Air Legal and Regulatory Module (1 week)	Space Operations Safety Module (4 weeks)
P1 **Space Environment and Human Performance** *(2 credits)*	*P5* **Space & Aviation Treaties, Regulations and Standards** *(1 credit)*	*P5* **Range Safety, Spaceport Ground Safety, Air-launch Safety** *(3 credits)*
P2 **Safety Design for Space Systems (including case studies)** *(3 credits)*	*P6* **Air Traffic Management & Space Traffic Management** *(1 credit)*	*P6* **On-orbit Safety** *(2 credits)*
P3 **Software Systems Safety** *(2 credits)*		*P7* **Re-entry Software Systems Safety** *(3 credits)*
P4 **System Safety Analysis Methods** *(3 credits)*		

C.1.2 Undergraduate/Postgraduates Courses (Web-based)	
U1	Elements of Industrial and Occupational Safety for Spaceports
U2	Orbital Debris Mitigation and Spacecraft Operations Safety
U3	Propellant and Explosive Systems Safety Design
U4	Materials Safety and Oxygen Systems Design
U5	Elements of Space Systems Design and Safety
U6	Extra Vehicular Systems and Activities Safety
U7	Aviation Airworthiness Certification
U8	Safety of Nuclear Spacecraft Systems
U9	Accidents Investigation
U10	Space Traffic Management
U11	Air Traffic Control
U12	Safety Management System and Safety Culture
U13	Cognitive Functions and Human Error
U14	Astronauts Selection and Training
U15	Human Reliability Analysis Methods
U16	Space Operations Safety
U17	Cosmic Hazards and Planetary Defence

distribute information to learners. VLEs can, for example, enable learners to collaborate on projects and share information. However, the focus of web-based courses must always be on the learner. Technology is not the issue, nor necessarily the answer.

Several approaches can be used to develop and deliver web-based learning. These can be viewed as a continuum. At one end is “pure” distance learning (in which course material, assessment, and support is all delivered online, with no face to face contact between students and teachers). At the other end is an organizational intranet, which replicates printed course materials online to support what is essentially a traditional face to face course. However, websites that are just repositories of knowledge, without links to learning, communication, and assessment activities, are not learner centred and cannot be considered true web-based learning courses.

The features of a typical web-based course are:

- Course information, notice board, timetable
- Curriculum map
- Teaching materials such as slides, handouts, articles
- Communication via email and discussion boards
- Formative and summative assessments
- Student management tools (records, statistics, student tracking)
- Links to useful internal and external websites (library, online databases, and journals)

C.2 SPACE SAFETY PROFESSIONAL TRAINING PROGRAM

The courses duration would generally vary from 12 hours to 30 hours, they would be mainly web-based, but few may be in-class.

1) System Safety Engineering
2) Commercial Human Spaceflight Safety
3) Launch Safety Analysis
4) Re-entry Safety Analysis
5) Space Debris
6) Explosive safety
7) Software System Safety
8) Safety Management System
10) Quality Assurance for Space Projects
11) Reliability for Space Projects
12) Configuration Management for Space Projects
13) Risk Management for Safety Engineer
14) Liabilities and Maximum Probable Loss (MPL) Calculation

Annex D

ESSENTIAL FEATURES OF A SELF-POLICING SAFETY ORGANIZATION FOR THE OIL AND GAS INDUSTRY

Excerpt (pages 241-242) from

Report to the President

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling

January 2011

Like the nuclear power industry in 1979, in the immediate aftermath of the Three Mile Island accident, the nation's oil and gas industry needs now to embrace the potential for an industry safety institute to supplement government oversight of industry operations. Akin to INPO, such a new safety institute can provide the nation with the assurances of safety necessary to allow the oil and gas industry access to the nation's energy resources on the outer continental shelf. To be sure, the significant differences between the two types of industries warrant significant differences in the precise structure and operation of their respective industry safety institutes. But, as elaborated below, the basic, successful principles upon which the INPO model is premised can serve as the touchstones for the oil and gas industry in establishing its own.

Credibility. To be credible, any industry-created safety institute would need to have complete command of technical expertise available through industry sources, and complete freedom from any suggestion that its operations are compromised by multiple other interests and agendas. As a consensus-based organization, the American Petroleum Institute (API) is culturally ill-suited to drive a safety revolution in the industry. For this reason, it is essential that the safety enterprise operate apart from the API. As described above and in Chapter 3, API's longstanding role as an industry lobbyist and policy advocate, with an established record of opposing reform and modernization of safety regulations, renders it inappropriate to serve a self-policing function. In the aftermath of the Deepwater Horizon tragedy, the Commission strongly believes that the oil and gas industry cannot persuade the American public that it is changing business-as-usual practices if it attempts to fend off more effective public oversight by chartering a self-policing function under the control of an advocacy organization.

Former EPA Administrator William Reilly (L) and former U.S. Sen. Bob Graham, co-chairs of the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. December, 2, 2010, in Washington, DC.

An industry-wide commitment to rigorous auditing and continuous improvement. The INPO experience makes clear that any successful oil and gas industry safety institute would require in the first instance strong board-level support from CEOs and boards of directors of member companies for a rigorous inspection and auditing function. Such audits would need to be aimed at assessing companies' safety cultures (from design, training, and operations through incident investigation and management of improvements) and encouraging learning about and implementation of enhanced practices.

As at INPO, the inspection and auditing function would need to be conducted by safety institute staff, complemented by experts seconded from industry companies, able to analyze the full range of technologies and practices, and designed to promote cross company learning and shared responsibility while protecting proprietary information There would also need to be a commitment to share findings about safety records and best practices within the industry, aggregate data, and analyze performance trends, shortcomings, and needs for further research and development. Accountability could be enhanced by a requirement that companies report their audit scores to their boards of directors and insurance companies.

The main goal is to drive continuous improvement in every company's standards and performance, measured against global benchmarks. The means, to that end, include the safety auditor's reviews; insurer evaluations of risk; and management recognition of and incentives for effective behavior. Senior leadership would be accountable to the company's board of directors, who in turn would be accountable to investors.

In a broader sense, the industry's safety institute could facilitate a smooth transition to a regulatory regime based on systems safety engineering and improved coordination among operators and contractors—the principles of the U.K.'s "safety case" that shifts responsibility for maintaining safe operations at all times to the operators themselves. It should drive continuous improvement in standards and practices by incorporating the highest standards achieved globally, including (but not exclusively) those set by the API. An initial set of standards and scope of operation. The industry needs to benchmark safety and environmental practice rules against recognized global best practices. The Safety and Environmental Management Program Recommended Practice 75 (API RP 75) developed in 1993 by the API and incorporated by reference in the Department of the Interior's new workplace safety rules, adopted in October 2010, is a reasonable starting point. 172 Updates to those safety rules are needed immediately, but a new industry safety institution could make a credible start by requiring members to adopt all safety standards promptly, and mandating that the companies, in turn, require that their contractors and service providers comply with the new safety rules.

NOTES & REFERENCES

1. **NOTE:** Sections: 1.1, 1.2, authored by Prof. Nancy Leveson (MIT Boston), and previously published as part of the IAASS book Space Safety and Human Performance, Elsevier (2017)
2. **NOTE:** Sections 1.3, 2.1, 2.2, 4.2, 4.3, authored by Tommaso Sgobba (IAASS), and previously published as part of the IAASS book Space Safety and Human Performance, Elsevier (2017)
3. **NOTE:** Chapter 3 is based on excerpts from Standards, Conformity Assessment, and Trade Into the 21st Century (1995), Policy Project Committee, Board on Science, Technology, and Economic Policy, National Research Council, The National Academies Press.
4. Barriero, J., J. Chachere, J. Frank, Ch. Bertels, A. Crocker (2010) Constraint and Flight Rule Management for Space Mission Operations, SAIRAS 2010, Sapporo, Japan.
5. Blind. K. (2013) The Impact of Standardization and Standards on Innovation, Nesta Working Paper 13/15.
6. Clifton, A. E. (2005) Hazard Analysis Techniques for System Safety, John Wiley & Sons, Inc.
7. Thornton, C., The Triumph of Risk management. *https://www.mangolive.com/blog-mango/triumph-of-risk-management*
8. Deep Water (2011) The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President.
9. Duarte, A. (2007) Engineering and Safety Partnership Enhances Safety of the Space Shuttle Program, 2nd IAASS Conference: Space Safety in a Global World; 14-16 May 2007; Chicago, IL; United States.
10. ESMD-CCTSCR-12.10 (2010) Commercial Crew Transportation System Certification Requirements for NASA Low Earth Orbit Missions.
11. Gehman, H., et. al. (2003) Report of Columbia Accident Investigation Board.
12. Hale, W. (2010) Wayne Hale's Blog: Human Rating a Spacecraft. *http://www.spaceref.com/news/viewsr.html?pid=33584*
13. Hall, J. L., (2003) Columbia and Challenger: organizational failure at NASA, Elsevier.
14. *http://theconversation.com*, (2014) Deepwater Horizon four years on and offshore safety remains questionable.
15. Kemeny, J. (1979) Chairman President's Commission on the Accident at Three Mile Island. Final Report.
16. Miller, J., J. Leggett, J. Kramer-White (2008) Design Development Test and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems. NASA/TM-2008- 215126/Vol II NESC-RP-06-108/05-173-E/Part 2.
17. Musgrave G., A. Larsen, T. Sgobba (2009) Safety Design for Space Systems Butterworth-Heinemann.
18. NASA NPR 8705.2C (2017) Human-Rating Requirements for Space Systems.
19. NASA NSTS 1700.7B (1989) Safety Policy and Requirements.
20. NASA/SP-2014-3705 (2014) NASA Space Flight Program and Project Management Handbook.
21. National Academy of Sciences, (1988), Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management. Committee on Shuttle Criticality Review and Hazard Analysis Audit, Space Applications Board, Commission on Engineering and Technical Systems, National Research Council, National, National Academy Press.
22. National Commission on BP Deepwater Horizon Oil Spill and Offshore Drilling, (2011)
23. Green, P., Why safety and Human Factors/ Ergonomics standards are so difficult to establish. University of Michigan Transportation Research Institute (UMTRI), Michigan, USA
24. Rogers, W., et. al. (1986). Report of the Presidential Commission on the Space Shuttle Challenger Accident.
25. Sperber, K. P. (1973) NASA TN D-7438 Apollo Experience Report Reliability and Quality Assurance.
26. Tremayne, D. (2000) The science of safety, the battle against unacceptable risk in motor racing. UK, Haynes Publishing.

SPACE SAFETY INSTITUTE STUDY TEAM

The Study Team will review this report to validate the concept of establishing a Space Safety Institute for commercial human spaceflight. The Study Team will also study and make recommendations about set-up and funding of the proposed Space Safety Institute, in particular the feasibility as Federally Funded Research and Development Center (FFRDC),

STUDY TEAM MEMBERS

Dr. George C. Nield

Dr. George C. Nield served as the Associate Administrator for Commercial Space Transportation at the Federal Aviation Administration (FAA) from 2008-2018. Under his leadership, the office had the mission to ensure public safety during commercial launch and reentry activities, as well as to encourage, facilitate, and promote commercial space transportation. Dr. Nield has over 35 years of aerospace experience with the Air Force, at NASA, and in private industry.

Edward J. Mango

Edward J. Mango served as the NASA program manager for the Commercial Crew Program (CCP) at NASA's Kennedy Space Center in Florida. The Commercial Crew Program is leading NASA's efforts to develop the next United States capability for crew transportation and rescue services to and from the International Space Station (ISS) and other low-Earth orbit destinations by the middle of the decade. The outcome of this capability is expected to stimulate and expand the U.S. space transportation industry.

Richard W. McKinney

Richard W. McKinney served as Deputy Under Secretary of the Air Force for Space and the Director, Executive Agent for Space Staff, Washington, D.C. He provided the principal support to the Under Secretary's role as the Headquarters U.S. Air Force focal point for space matters and in coordinating activities across the Air Force space enterprise. Additionally, he directed the headquarters staff responsible for space policy, issue integration and strategy.

Christopher T.W. Kunstadter

Chris Kunstadter is Senior Vice President and Global Underwriting Manager – Space at AXA XL, and manages AXA's space insurance portfolio. He is actively involved in all aspects of AXA's space business. Chris has worked closely with satellite operators and manufacturers, launch providers, and government agencies to enhance industry understanding of space risk management issues, and has served on numerous failure review boards for satellites and launch vehicle.

Dr. James W. Wade

Dr. James Wade is Vice President, Corporate Mission Assurance at Raytheon. He leads the end-to-end Mission Assurance, Quality, and continuous improvement efforts across the company. Raytheon Company is a technology and innovation leader specializing in defense security and civil markets throughout the world. Dr. James Wade joined Raytheon in 2010 from MIT Lincoln Laboratory where he was the head of its Safety and Mission Assurance Office.

IAASS-ISSF STUDY SUPPORT TEAM MEMBERS

Dr. Michael Kezirian

Dr. Michael Kezirian is President of the International Space Safety foundation (ISSF). Dr. Kezirian was an Associate Technical Fellow at the Boeing Company most recently supporting the development of the Boeing Starliner CST-100. Previously he was a design analyst for the Nitrogen Oxygen Recharge System (NORS) for the International Space Station (ISS). He was the Boeing Vehicle Safety Lead for the Shuttle Orbiter Endeavour.

Tommaso Sgobba

Tommaso Sgobba is Executive Director of the IAASS. Until 2013 Tommaso Sgobba was head of Independent Safety Office at the European Space Agency (ESA), responsible for human-rated systems safety certification, spacecraft re-entry, space debris, and planetary protection. Before joining ESA in 1989, he worked for 13 years in aviation as quality assurance manager.