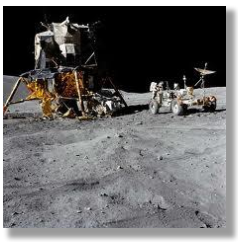
Safety of Commercial Suborbital Human Spaceflight

by
T. Sgobba
IAASS Executive Director
ISSF Board Member

Quite different beginning!

State-of-art at beginning of aviation

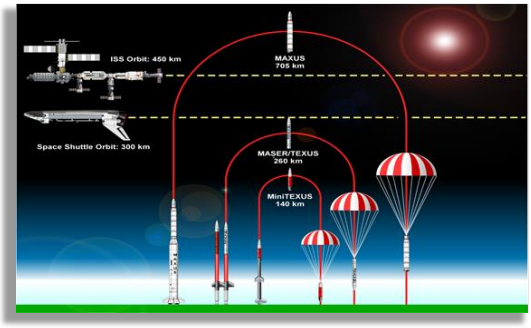


State-of-art at beginning of commercial human spaceflight

Suborbital spaceflight

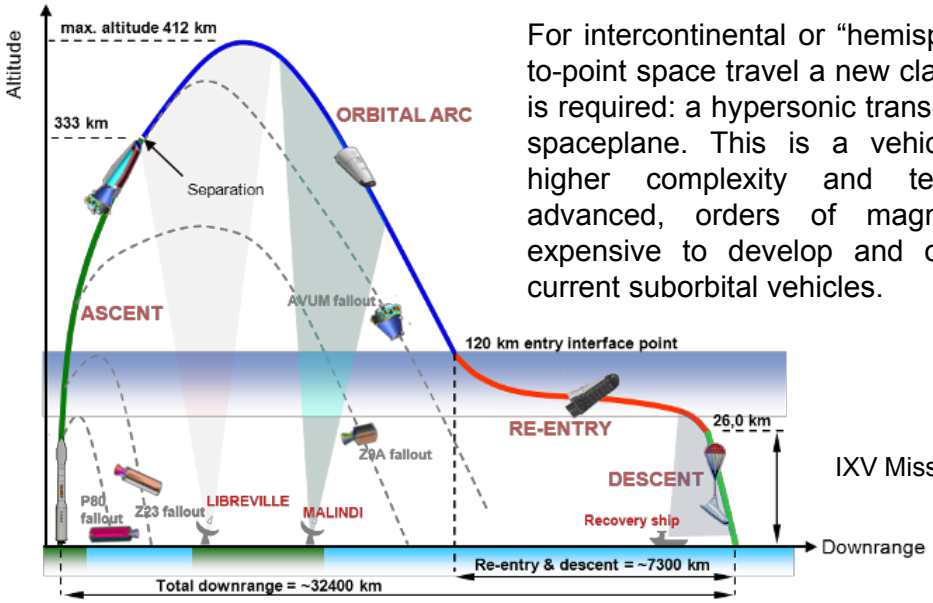
A suborbital flight is a flight beyond 100 kilometers above sea level but in which the vehicle does not attain the speed to escape Earth's gravity field (40,320 kph).

When a sub-orbital space vehicle of current design reaches its maximum altitude at the vertex of the parabola the horizontal speed is almost zero. It may be possible to adapt the current sub-orbital design to cover few hundred kilometers,



ESA unmanned suborbital rockets -credits: © ESA/G. Dechiara

Trans-atmospheric spaceflight



For intercontinental or “hemispheric” point-to-point space travel a new class of vehicle is required: a hypersonic trans-atmospheric spaceplane. This is a vehicle of much higher complexity and technologically advanced, orders of magnitude more expensive to develop and operate than current suborbital vehicles.

IXV Mission Profile

First rocket propelled airplane 70 years ago!

ME-163

First suborbital human spaceflights

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

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

Current developments still follow such configurations, plus two consisting into an airplane with either a rocket engine or jet engine plus rocket engine.

Comparing historical safety records

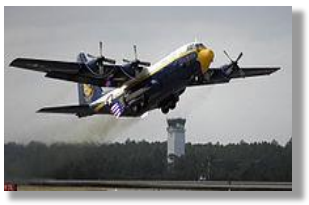
- **Capsule configuration** - The available (statistically significant) safety record for capsule configuration is that of Russian Soyuz (orbital vehicle). As of beginning of 2013 there have been 115 manned Soyuz launches with 4 failures in total: 2 during launch with no casualty (thanks to the activation of the abort systems), and 2 at re-entry with 3 casualties in total.

- **Air-launched configuration** – On a total of 199 flights X-15 flights there were 1 engine failure and 1 engine explosion with damages at landing (no casualty), and 1 crash with 1 casualty.

Suborbital spaceflight safety target 1/10000

It is a rocket or an airplane?

A space vehicle needs rocket propulsion to travel in vacuum. But a vehicle like a car or an airplane which uses rocket propulsion to accelerate on ground or in air is not a space vehicle! Since WWII there have been several types of (military) planes that have made use of rockets during take-off (RATO).



A person on a space vehicle orbiting Earth will experience microgravity (weightlessness), but you can experience it **on an aircraft performing a parabola**. Space agencies usually use aircraft parabolic flights to test equipment and train astronauts.

Most commercial human suborbital systems currently in development are essentially high-performance aircraft that use rocket propulsion to accelerate in air (rocket burn-out around altitude of 60 km) while in a parabolic flight.

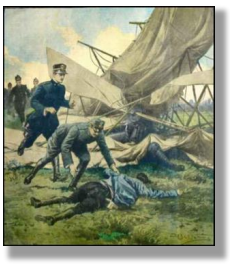
Atmospheric Pressure Variation

Altitude (meter)	Delta Pressure % (Altitude/Sea-Level)
0 (sea-level)	100%
2,500	74%
5,000	53%
12,500	18%
25,000	2,5%
50,000	0,8%
75,000	0,02%
100,000	≈ 0

International Space Safety Foundation

How it Started: Fly-Fix-Fly

Prior to the 1940s, flight safety consisted of basically trial-and-error. The term fly-fix-fly was associated with the approach of building a prototype aircraft, fly it and repair/modify if broke and fly it again For complex and critical systems such approach is simply impossible.



From 1952 to 1966 the USAF lost 7715 aircraft, in which 8547 persons were killed. Most accidents were blamed on pilots, but many engineers argued that safety had to be designed into aircraft just as any other functional or physical feature related to performance. Seminar were conducted by the Flight Safety Foundation, headed by Jerome Lederer that brought together engineering, operations, and management personnel. At one of those seminars, in 1954, the term "*system safety*" was first used in a paper by the aviation safety pioneer C.O. Miller.

How it Started: MIL-STD-882

When the Atlas and Titan ICBMs were being initially developed in the 1950s there was no safety program. Within 18 months after the fleet of 71 Atlas F missiles became operational, four blew up in their silos during operational testing. The worst accident occurred in Searcy, Arkansans on August 9 1965, when a fire in a Titan II silo killed 53.

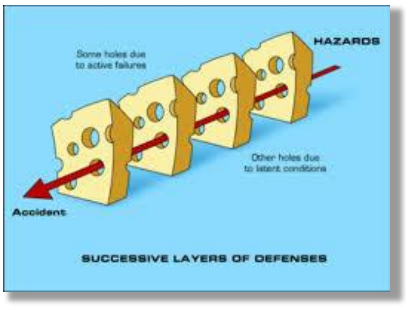
The U.S. Air Force then developed system safety assessment and management concepts. Such efforts eventually resulted into the establishment of a major standard, MIL-STD-882, and ***System Safety Engineering*** as a discipline.

International Space Safety Foundation

How it Started: O&SHA

Considering that on one hand we cannot afford the “luxury” of a nuclear disaster to learn the lesson, and that on the other hand the conditions leading to a ‘potential accident’ are relatively easy to identify, thus that preventive actions could be readily taken particularly in the early stages of a project, a technique was devised called ‘hazard analysis’.

Basically hazard analysis is a technique that postulates the scenario of a potential accident and takes the necessary corrective measures to remove or ‘control’ the causes such to lower the risk (consequence severity + probability) to an acceptable level. ‘Controls’ consist essentially in the application of redundancies, barriers, safety-factors, best-practices, and operational procedures.



How it Started: O&SHA

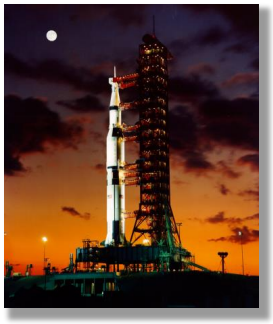
The fact that a reliable design is not enough to ensure safety, was dramatically shown by another Titan II accident, which lead to the establishment of O&SHA (Operation and Support Hazard Analysis) requirements in MIL-STD-882. On September 18, 1980, a maintenance technician dropped a tool, which fell about 25 meters before hitting and piercing the rocket's fuel tank, causing a leak. Next day during the clean up the missile exploded, blowing the nuclear warhead about 30 meters from the launch complex's entry gate (but did not explode!)

International Space Safety Foundation

How it Started: Man-rating

Use of term *man-rating* began at NASA in the early manned spaceflights days (**Mercury and Gemini Programs**) and pertained to modifications, improvements, added redundancy, and crew escape features applied to existing military ballistic missiles (Redstone, Atlas, Titan II) to make them suitable to launch manned capsules.

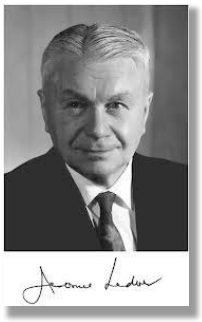
It was for the Apollo Program that the man-rating features were expanded and introduced for the first time in a new development: the Saturn rocket.



CESMA 2016

How it Started: Man-rating (cont'd)

After the 1967 Apollo 1 fire that killed three astronauts, NASA commissioned the General Electric Company to develop policies and procedures that became models for human spaceflight safety activities. Jerome Lederer (father of aviation safety) was hired to head safety at NASA. He set up an extensive system safety program much of it patterned after the USAF and US DoD programs.

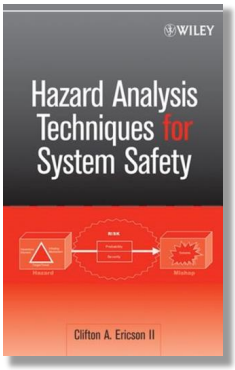


International Space Safety Foundation

How it Started: the Space Shuttle

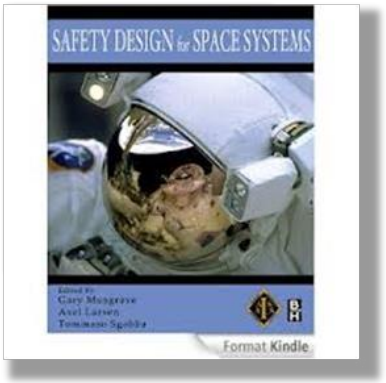
By the time the Space Shuttle was designed the old man-rating concept was embodied together with specific safety analyses and logic procedures taken and adapted from MIL-STD-882 in what we can call ***Space System Safety Engineering***. The approach was also applied with some simplifications to Space Shuttle payloads.

Improvements were later introduced following the "Challenger" disaster in 1986 and the "Columbia" in 2003. [Although those accidents were mainly traceable to a deficient organizational safety culture and lack of independent check-and-balance].



The Example of ISS and Commercial Cargo Vehicles

It is through the massive use of hazard analyses driving the implementation of best (safety)-practices in systems design that safety has been designed into the International Space Station, including newly added commercial vehicles like SpaceX Dragon, and Orbital Cygnus.

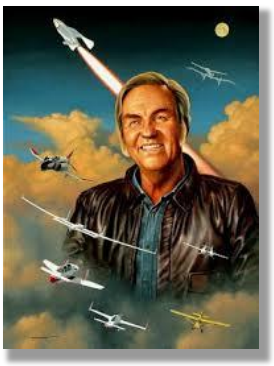


International Space Safety Foundation

Applying Hazard Analysis to Suborbital Vehicles

Suborbital vehicles designers often maintain that no safety requirement can be levied on industry until sufficient operational experience is accumulated, (several years, perhaps decades from now).

Such cultural misconception is rooted essentially in the aviation experience of designers of new suborbital vehicles. Aviation is an “evolutionary” industry, where standards are the results of proven successful use, and where detailed prescriptive requirements based on ‘lessons learned’ from past accidents are the rule. Hazard analyses are not generally used to drive the design.



Sub-orbital Vehicles Top Hazards

By combining the columns of the table, all current vehicles configurations are addressed. For example the top risks of an air launched winged suborbital vehicle like SpaceShipTwo are collectively those of columns (b) + (c) + (d)

Design / Risk	Capsule (a)	Air Launched (b)	Rocket propulsion (c)	Winged System (d)
Carrier malfunction		X		
Explosion			X	
Launcher malfunction	X			
Inadvertent release or firing		X		
Loss of pressurization	X			X
Loss of control at reentry				X
Parachute system failure	X			
Crash landing				X
Escape system failure	X			
Falling fragments (catastrophic failure)				X
Leaving segregated airspace	X			X
Atmospheric pollution			X	

International Space Safety Foundation

Does Industry Need a Space Safety Institute?

The age of commercial human spaceflight is being ushered under unique conditions, namely without a US government regulatory framework for ensuring the safety of those on board. On the other hand traditional (bureaucratic) regulatory bodies may have difficulty in issuing standards and performing oversight of a high-tech fast evolving industry even if they have the mandate to do so. Safety is a strategic goal for the future of commercial human spaceflight. It is a challenge and a great opportunity.

Questions:

- What should industry do collectively, and companies individually?
- How to transfer 50 years of government programs safety know-how?
- Who will educate (on safety) future generations of engineers and managers?
- Is there a role for academic space safety research?
- What can we learn from other safety-critical high-tech industries?

What did we learn in 50 years of human spaceflight?

We learned how to safety-certify a completely new space system for which there was no previous (or only partial previous) experience.

Key elements:

- **Safety requirements and technical standards**
- **Safety analyses** (Hazard Analysis, PRA, FTA, etc.)
- **Independent surveillance**
  - safety reviews
  - manufacturing reviews
  - readiness reviews
  - QA, etc.
- **Safety verification program** (tests, analyses, inspections, demonstrations)

Safety-by-Design

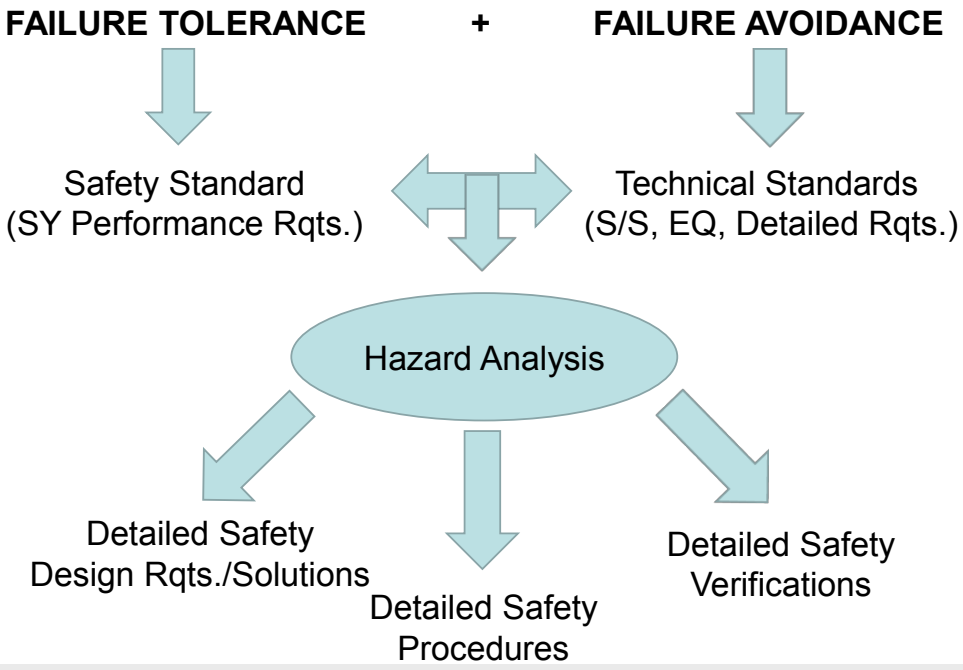
Hardware and software can be designed at the best of our knowledge, but our knowledge is not perfect. We can apply the most rigorous quality control during manufacturing, yet perfect construction does not exists and some defective items will be built and escape inspection.

A safe system is one that through additional margins, redundancies, barriers, and capabilities will "avoid" or "tolerate" (to a certain extent) hardware failures, software faults, and human errors, by lowering the probability of occurrence and/or mitigating harmful consequences.

Safety-by-Design is the use of best practices for achieving :

FAILURE TOLERANCE + FAILURE AVOIDANCE

Safety-by-Design



Certification Performed by Non-regulatory Entity

For example, NASA Crew Commercial Program (CCP) roles include:

- Transportation services (to/from ISS) customer
- **System safety certification authority for transportation phases** (ESMD-CCTSCR-12.10, CCT-STD-1140, -1150)
- ISS integrator + responsible for US provided elements
  - Issuing of detailed safety requirements (SSP 50021)
  - Performance of safety reviews (SSP 30599)
  - Interface requirements (including additional SR) (SSP 50808)

For agency procured US elements of ISS, NASA performs surveillance of design & development activities through "**oversight**". For the CCP NASA performs an "**insight**" role similarly to what is done for the ISS systems provided by International Partners.

Certification Performed by Non-regulatory Entity (cont'd)

NASA Technical Standards are separated into 3 types:

–**Type 1** documents are those that contain requirements the commercial project must meet as written - **Mandatory**

–**Type 2** documents are those that contain requirements the commercial project can either choose to adopt, or propose an alternate – **Meets or Exceeds**

–**Type 3** documents are those that contain requirements where the commercial project does not need to either formally adopt the document or recommend an alternate – **Reference**

NASA Technical Authority	Type 1	Type 2	Type 3
Health & Medical	0	3	1
Engineering	0	35	7
Safety & Mission Assurance	0	36	10

International Space Safety Foundation

Space Safety Institute

Even when NASA is not involved in a human commercial spaceflight program, there is still the need for an organization to play a similar role in:

- **Establishing standards for safety of human on board**
- **Independently verifying compliance**
- **Monitoring/auditing the verification program**
- **Safety education and training**

An industry-driven (and funded) organization, a Space Safety Institute, is better suited and cost-effective than a government regulatory organization

Government regulatory organizations can still play a key-role by establishing:

a) high level transportation system safety **goals** (human on board)

b) **process** for performing third party system certification

c) **criteria** for approval of third-party certification organization

d) regulations for operations and public safety (as already the case)

The Safety-Case Regime

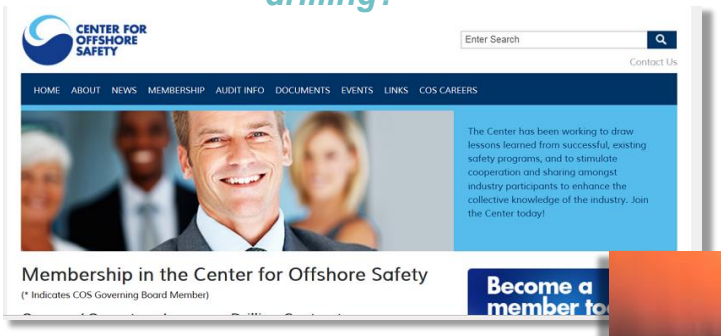
The proposed regime is called “safety-case regime”. It recognizes that the regulatory authority should have the role and responsibility to **define the “safety goals and objectives”,** while the developer would be in charge of proposing valid detailed technical solutions, due to its in-depth knowledge of the system design and operations.

In such regime an independent **safety certification team is needed having skill comparable (or higher) than the design team,** in order to evaluate the soundness of the detailed design solutions chosen to mitigate the risks. For government bureaucracies to attract and maintain a variety of advanced skills in a fast-evolving high tech industry it is difficult, inefficient, and expensive. Instead **certification teams composed by independent experts, drawn from industry, government agencies, and academy would be easier to assemble and retain for a (limited) needed duration**.

Finally the establishment and maintenance of technical standards for rapidly evolving technologies, based on previous experience, is better done by industry than by government organizations, or by a mixed organization.

Examples from other industries: Oil & Gas

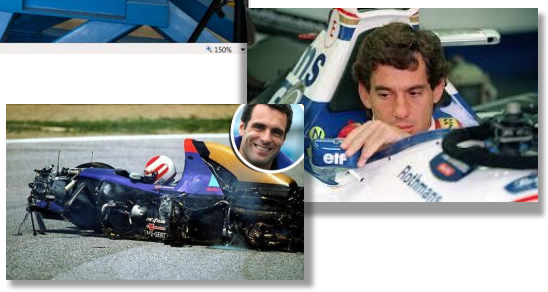
“Could they forbid off-shore drilling?”



The **Center for Offshore Safety** was established following recommendations of the Presidential Committee on the “Deepwater Horizon” platform disaster in the Gulf of Mexico in 2010

Examples from other industries: Formula-1 Car Racing

"Could we lose television rights?"



The **FIA (International Automobile Federation) Safety Institute** was established after the triple accidents at the Formula 1 Imola (I) Grand Prix in 1994

Examples from other industries: Nuclear Power Operations

"Are we risking to be outlawed?"

The **Institute of Nuclear Power Operations**, was established in 1979 by the U.S. nuclear power industry in response to recommendations by the Kemeny Commission Report, following the investigation of the following the investigation of the Three Mile Island accident.


The Nuclear Accident

Radiation Continues To Leak From Crippled Plant

HARRISBURG, Pa (AP) — Radiation leaks from the Three Mile Island nuclear power plant continued today, authorities said, as a debate grew over what was described as one of the most serious such incidents in this country's history.

"The vapor that is now going into the atmosphere is from a sump pump and is only mildly radioactive within accepted limits," said Dan Curry, a spokesman for the Metropolitan Edison Co., owner of the plant. The pump is designed to remove water after it has cooled the reactor. But Curry said the utility is not just a little thing." Curry said, "In terms of publicity it will probably surpass the Brown Ferry incident."

Until now, a March 1975 fire in the control room of the Browns Ferry nuclear plant in Alabama has generally been considered this nation's most dangerous incident involving a nuclear reactor.

Low level radiation was detected in the air as far as 16 miles away after an apparent valve failure Wednesday morning resulted in excessive pressure being built up in the water used to cool the reactor core at Three Mile Island.

"Some of the water vapor, through the venting system, went into the atmosphere," Curry said.

Curry said the latest radiation measurements outside the plant were at two to three millirems. Individuals are exposed to up to 30 millirems in a single X-ray examination.

Walter Cronkite, president of Metropolitan Edison, said on ABC-TV's *Good Morning America* show this morning that the plant shut down safely and that the level of radiation released "would not endanger or injure any people."

Cronkite said the company did not know what equipment had been disabled or what precisely caused the accident.

An aerial view of the Three Mile Island nuclear power plant.

AP Photo

Conclusions

It is recommended, in conclusion, to apply to the commercial spaceflight industry the same recommendation issued by the US Presidential Commission that investigated the 'Deepwater Horizon' oil-spillage disaster of April 2010 in the Gulf of Mexico:

"Commercial spaceflight 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 space sustainability"