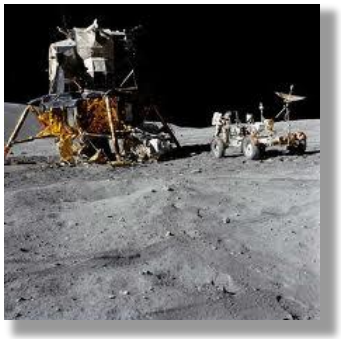
The Need for a Space Safety Institute

By
T. Sgobba & E. Mango

ICAO / UNOOSA AeroSPACE Symposium
Montreal

Quite different beginning!

State-of-art at beginning of aviation



State-of-art at beginning of commercial human spaceflight

What did we learn in 50 years of human spaceflight?

We learned how to safety-certify a completely new space system for which there is 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

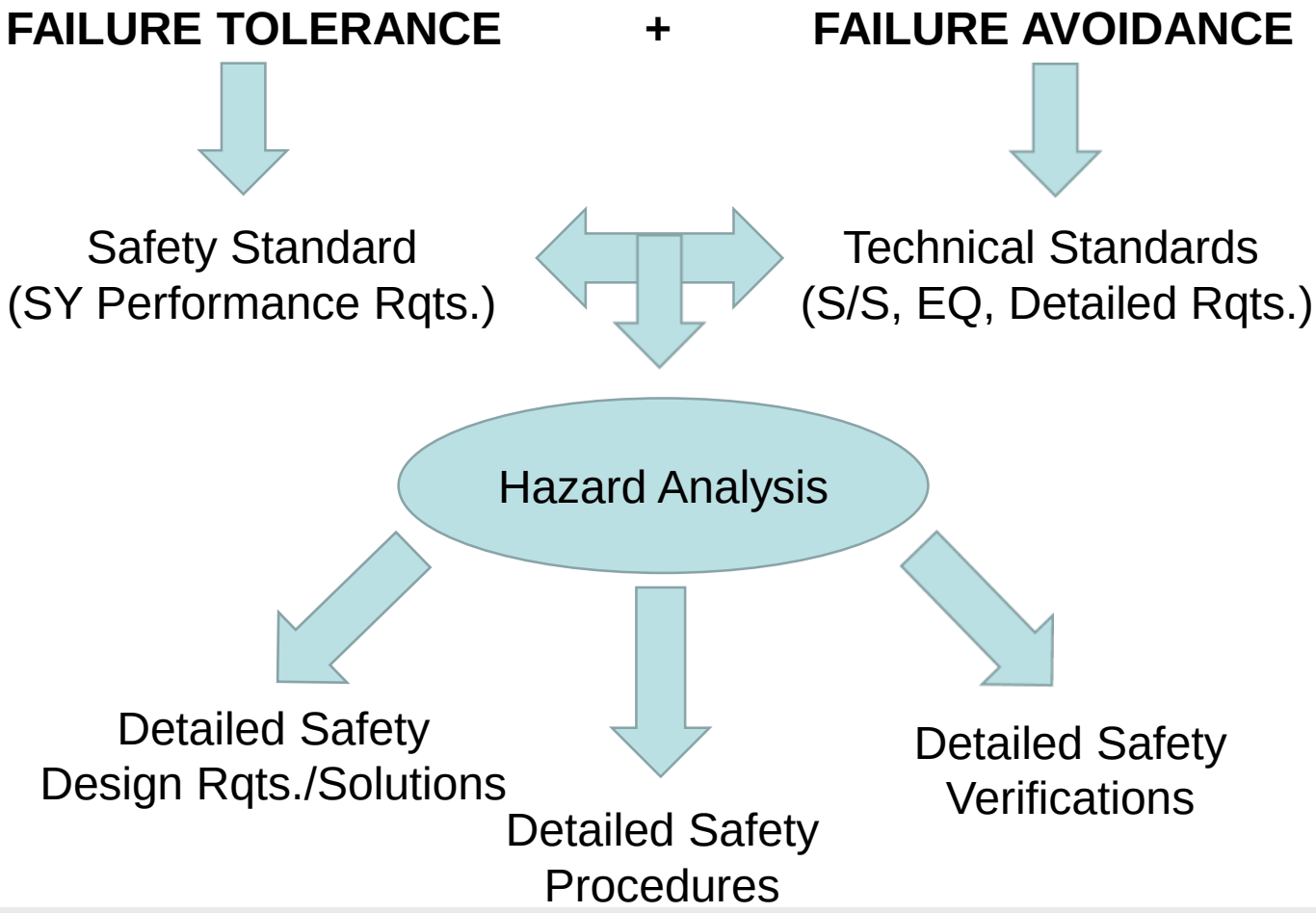
Hardware and software can be designed at the best of our knowledge, but our knowledge is not perfect. We can apply the most rigorous quality control during manufacturing, yet perfect construction does not exists and some defective items will be built and escape inspection.

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/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 project must meet as written - **Mandatory**

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

–**Type 3** documents are those that contain requirements where the 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

Oversight vs Insight

Oversight: It enables direct participation and direction by the customer throughout the design and development along with its trades and analyses used to drive the design configuration and verification program. In addition, Independent assessments, modeling and testing rounded out this resource intensive model of engagement in the design certification of the hardware and software.

This traditional surveillance approach appropriate if accountability and ownership of the design and operations are fully vested within the customer as certifying entity

Oversight vs Insight (cont'd)

Insight: A different approach is needed when the design ownership is with the project and not with the certifying entity. This process uses a risk-based approach to understanding the design and operations of the system and provides expertise to review and gain knowledge of the risk areas. Insight is a proactive approach to assess critical elements of the design development and operations phases by maintaining a continuous vigilance of the design and operational certification activities as the space system matures. Periodic exchanges of information with the design teams enable the insight team timely recognition of issues involving safety features and reliability concerns that warrant focus attention as the design and certification evolves. Insight teams review and provide advice but do not direct or approve.

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

NASA is not a regulatory entity (like FAA) but has been assigned responsibility by ISS IGA (Inter-Governmental Agreement) and MoUs to ensure the safety of its own crews and of those of International Partners during all phases of ISS missions, including transportation.

NASA performs its insight role in the Commercial Crew Program with the benefit of access to a variety of qualified personnel and means that are at least equal, and often exceed, skills, capabilities and experience available in the single industries involved in the program.

A 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

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 is difficult, inefficient, and expensive. Instead **certification teams composed by independent experts, drawn from industry would be easier to assemble and retain for the 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.

Conclusions

It is recommended, in conclusion, to apply to the commercial human 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:

"***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***" (US Presidential Commission on Deepwater Horizon Disaster)