Suborbital Commercial Vehicles– IAASS Safety Technical Committee

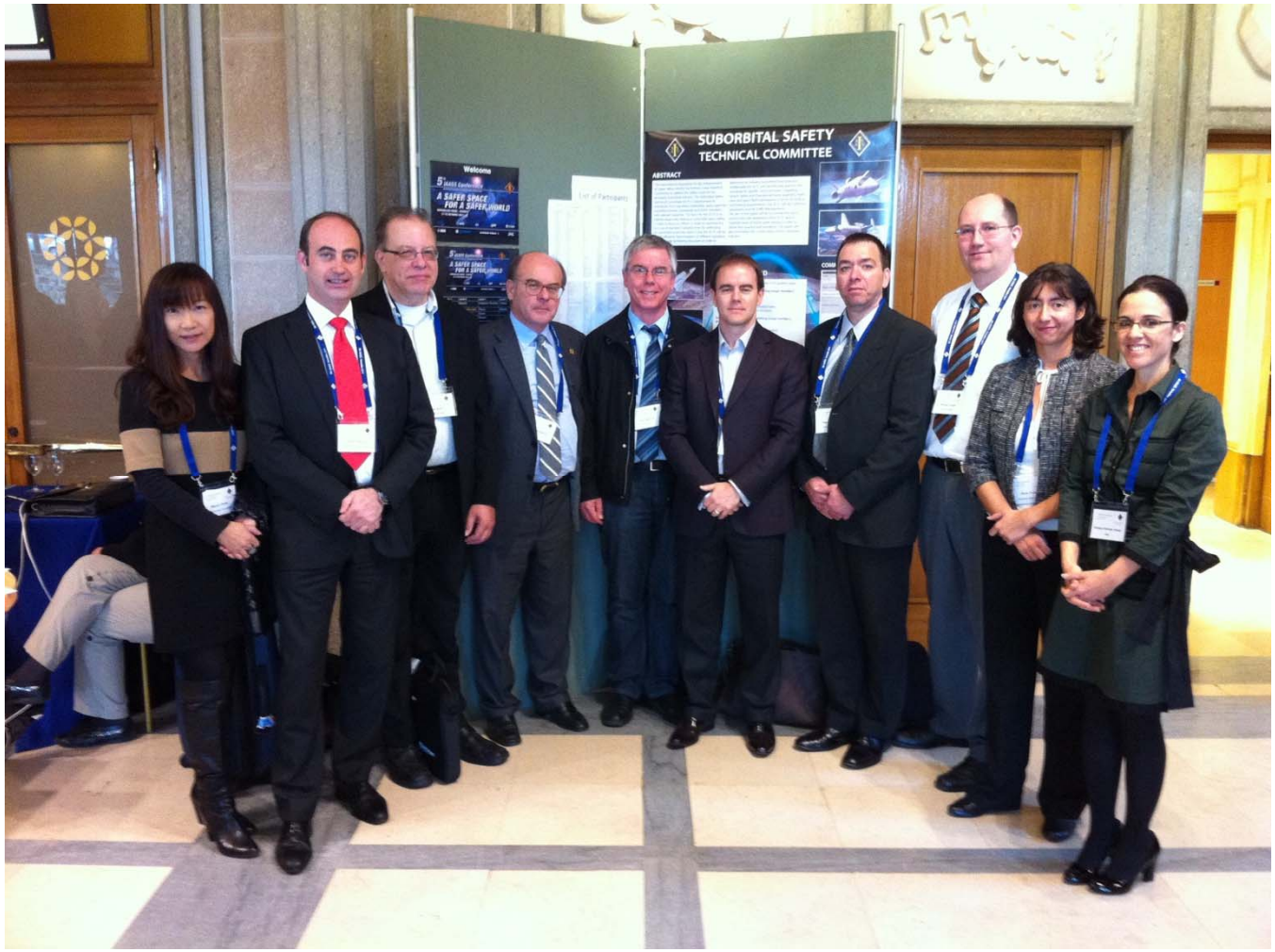
Proposed IAASS SW Safety Standard and Guidelines

techcos

gmv INNOVATING SOLUTIONS

Content

- IAASS SS TC Objectives
- Motivation of the Standard
- The challenge of defining a SW Safety Standard
- The Standard & Guidelines
- About the future
- Conclusions



Why a SW Standard?

...time ago in Versailles

From Versailles to ….

Suborbital **S**afety
Technical **C**ommittee
Proposed **IAASS**

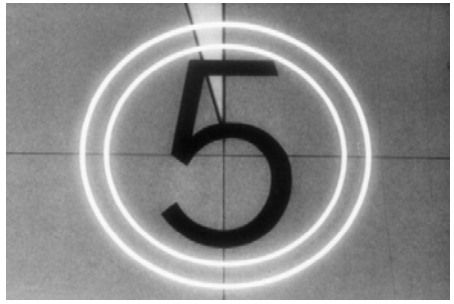
Standards & **G**uidelines

SS2300 – Software Safety

SGM2300 - Guidance Material

WHY?

Motivation of this Standard



Current situation

- Need of industry harmonization and self-regulation
- Open issues regarding regulatory and legal aspects.

Objectives

- Qualification of embedded software
- Facilitate risks understanding and discussion
- Establish a common worldwide industry (suborbital) best practices.

Addressed to

- vehicle designers, operators and regulators in suborbital domain

© Charles Ebbets

The Challenge

Do we need to define

a SW standard from scratch?

Criteria to define the standard

- The aim of SS TC was to **define a simple set of principles and rules** ensuring that crucial activities are been carried out to assess and deal with software risks and to implement an appropriate **assurance level for development activities**.
- Other requirements considered for the definition of the standard were:

  – **Universal** and **unbiased**, not influenced by any particular interest.
  – **Independent** of any existent role or certification authority.
  – **Relevant to** characteristics of **suborbital flights**.
  – Focused on the '**qualification**' of software.

Surfing other industries: SW Standards (Rationale)

- Do not re-invent the wheel !
  - Check whether potentially applicable standards and / or guidelines exist
  - Build on existing knowledge in the industry

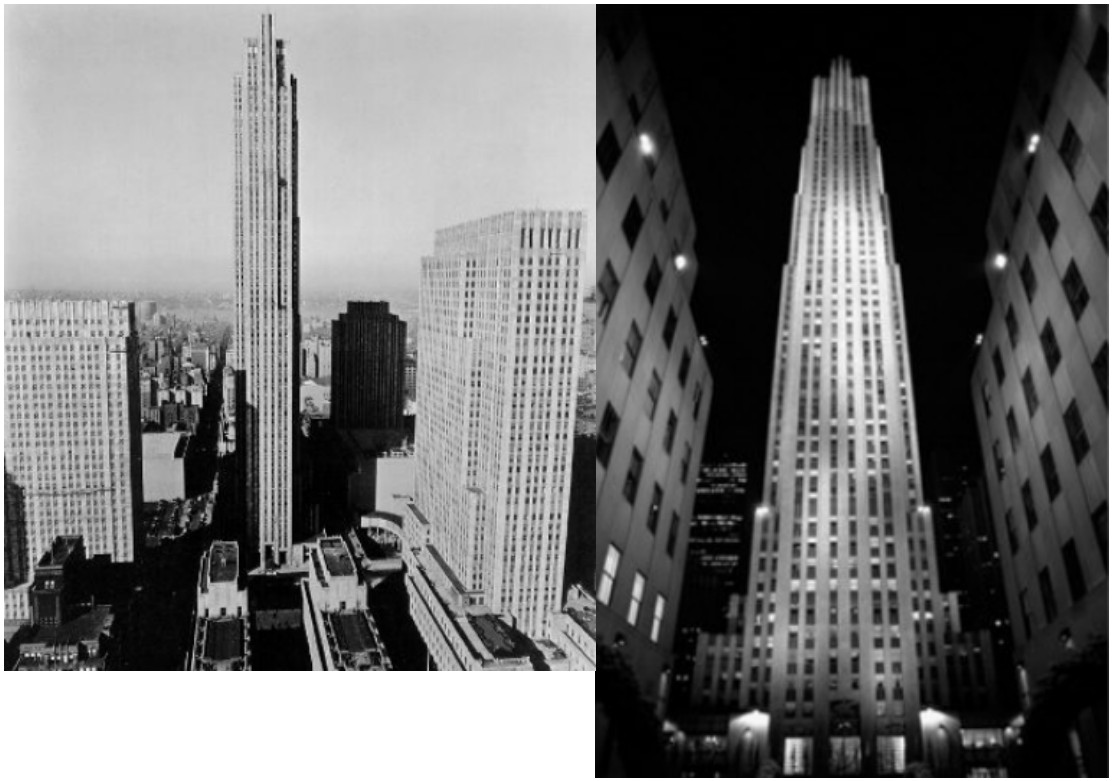
- Facilitate use of COTS components
  - Commercial suborbital (and ultimately orbital) spaceflight will gradually use more and more components originally developed for other applications – and therefore under different safety standards

Surfing other industries: SW Standards (Findings)

- No standard investigated was found to suit the needs of suborbital flight

- Reasons for lack of suitability:
  - Standards structurally focused on relationship with certification authority: DO-178, ATM standards, medical device safety standards
  - Standards tailored to the specifics of certain industrail applications: Nuclear, Automotive,
  - Standards that presume exclusive government use and operation of a system: NASA, ESA standards, military standards

- Way ahead for the TC:
  - Take the most suitable approaches and try to combine them!
    - No certification authority presumed, “self-certification” under a limited number of requirements!
    - No prescriptive requirements, safety case based approach



The result

SS2300 – Software Safety

SGM2300 - Guidance Material

SS2300 – Software Safety

Ten requirements grouped in topics

- (A) & (J) Scope of compliance and qualification
- (B) & (C) & (I) Risk assessment and mitigation process
- (D) & (E) Risk classification to establish SW assurance level
- (G) Risk reduction strategy
- (F) & (H) SW Safety Assurance Process: Objectives, Activities, Evidences and Documentation

IAASS Standards
SS2300 –
Software Safety

SS2300 – Software Safety

Basics

- SW criticality level drives safety assurance rigor and level of confidence.

Safety Event Severity	Software Criticality Level	Description	Remarks / Typical System capabilities involved (examples)
Catastrophic	Level SO-A	On-Board Software that causes or contributes to catastrophic hazards in case of failure.	Flight critical systems
Hazardous	Level SO-B	On-Board Software that causes or contributes to critical hazards in case of failure.	
Major	Level SO-C	On-Board Software that causes or contributes to major or minor hazards in case of failure.	Flight management system
Minor	Level SO-D	On-Board Software that causes or contributes to minor hazards in case of failure.	Systems without direct avionics interaction such as: payloads, entertainment systems, etc. (Lack of interaction with more critical (sub)systems will have to be demonstrated)
Negligible	Level SO-E	On-Board Software that cannot contribute to hazards in case of failure or Software that interacts with on-board systems but is operated outside the vehicle (ground systems, maintenance systems, ...) and cannot contribute to hazards in case of failure.	(Lack of interaction with more critical (sub)systems will have to be demonstrated)

IAASS Standards
SS2300 – Software Safety

SS2300 – Software Safety

Basics

- Risks reduced to a tolerable level:
  - SW components / relation with other systems.
  - Unsafe system operating conditions known.
  - Design approach for HMI.
  - Error handling, corrective actions, warnings.
- Verification / Documentation / Traceability
- Compliance to Standard accredited: pre-flight condition.
- Means to compliance → SGM2300

IAASS Standards
SS2300 – Software Safety

SGM2300 – Guidance Material (Overview)

- SGM2300 containes 4 parts
  - A) definitions used in SS2300 and SGM2300
  - B) Potentially applicable software safety standards, including remarkls on how to take credit for suborbital systems
  - C) Acceptable means of compliance for software in suborbital applications
  - D) Appropriate Assurance, additional remarks

- Most material references to well-known aeronautical standards as they are familiar to many manufacturers and operators of suborbital systems

SGM2300 - Guidance Material (Discussion highlight)

- One of the more contentious points: What is enough and appropriate evidence that software is acceptably safe ?
  - Some standards very silent on V&V requirements
  - Software has no quantitative failure probability, how does it fit into the system-level safety target approach ?

- Approach 1: As software assurance is qualitative, it does not relate directly to the numerical system safety target. Therfore the highest system risk classes (with respcect to different application domains) always require a similar set of assurance measures regardless of the accepted system risk
- Approach 2: Based on aeronautical standards as a benchmark, a level of software assurance corresponding to the system risk level is required. As the acceptable system risk is 2 orders of magnitude higher in suborbital flight, SO-A basically should correspond to DO-178B Level B
- <u>Approach 1 was ultimately chosen after intense discussion!</u>

© Charles Ebbets

Future amendments…

Future Work

- There is a lot to be done:
  - Detail software system requirements
  - Prepare for potential future regulatory regimes for non.winged vehicles
  - Expand SGM on complex hardware/software systems (for example FPGA's and the likes...)

- We would hope for some user material and feedback to further enhance relevance and quality of the standard and the guidance material

- Any comments are welcome !

© Roberto Pérez Toledo

Conclusions

..and Acknowledges

Conclusions

- Advent of commercial suborbital fligths requires regulation.
- IAASS to tackle safety issues and to propose suitable standards: operational, medical, legal, management and system aspects.
- **SS2300 + SGM2300 to deal with SW risks**.
- Complex process to elaborate the standard: survey of existent SW standard, applicability, certification authorities →

  Definition of a SW standard tailored with 'best-fit' standards.
- As result, good starting point with future enhancements → **feedback required**.

Thanks to the IAASS
To all the SS TC members
To SS TC chairman

And thank you for your attention!

Amaya Atencia Yépez
aatencia@gmv.com

Michael Klicker
klicker@techcos.de