Astrium Space Transportation

Safety is not an option, but…

6th IAASS Conference, May 2013

Philippe WATILLON

Together the pioneer of the full range of space solutions
for a better life on Earth

Safety is not an option, but what is the real objective ?

<u>To limit the risk of harm or damage to an accepted level !</u>

The notion of accepted risk is currently driving implementation methods based on failure tolerance requirements.

But the real requirement is acceptable risk, not number of local failure tolerance or level of redundancy.

The world is changing…

Space community has now acquired a significant experience in vehicle development and mission operation.

The new development are now differently challenging than the past one :

- Budgets are more constrained
- Development time is shorter
- Performance requirements are increased

We may come to the conclusion that we have achieved the limits of what we can do in the existing environment

How can we satisfy apparently contradictory requirements ?

Safety is a performance parameter and shall be treated as such in the system optimization.

Safety can no longer be treated as “a posteriori” demonstrated, or dogmatic, characteristic and shall be used to trade different possible system architecture, including the capability to assure failure compensation on an integrated level

Our operational knowledge and functional experience shall be used to improve the flow-down of top level safety objective (in this practical case failure tolerance) to lower level architecture

What should be avoided ?

The major drawbacks of systematically limiting the implementation of system safety requirements to a redundancy and segregation policy are:

- increase of the architecture complexity which may have negative impact on safety even if formally the failure tolerance has been increased
- some oversized “not safety relevant“ areas
- Inability to arbitrate between conflicting requirement (resources, performances, budget, schedule)

How can we make progress ?

Nearly all of our institutional developments are organized in a customer/supplier relation.

The global set of of requirements (technical, programmatic, financial), including safety objectives, can not always be simultaneously satisfied… and in fact it becomes more and more difficult.

The resources are limited, and best use of them is mandatory.

Nobody will find alone the perfect solution.

All together we will be able to meet the challenge.