The Preliminary Risk Analysis Approach: Merging Space and Aeronautics Methods

J. Faure, A. Cabarbaye & R. Laulheret
CNES, Toulouse ,France

ABSTRACT: Based on space industry but also on aeronautics methods, we will expose the necessary steps to control system's risks, from the early phases of specifications to the final design validation. In that scope, the Preliminary Risk Analysis is a powerful tool that we will present in this paper, as well as the best aeronautics practices.

1 CONTEXT OF SATELLITES PROJECTS

1.1 *Space Projects*

Space systems are produced almost always as prototypes (each one is a "one of a kind system"), are non-repairable and therefore require in depth dependability analysis prior to launch such as:

- FMECA,
- Derating analysis,
- Worst case analysis,
- Hazard analysis, etc

The Product Assurance specifications and the requirements in general define the necessary analysis for each project.

1.2 *Requirements Context*

We apply at the French Space Agency the following process for the safety and dependability programme of satellites projects:
The first step is to define the Product Assurance specifications and specially the Safety and Reliability requirements that shall be met. The requirements are tailored from the ECSS standards concerning Safety (ECSS-Q-40) or ISO 14620-1 "Safety of Space Systems" and dependability (ECSS-Q-30).

1.3 *Reality of Projects*

However, space projects design process is under tight cost and schedule constraints, which most of the time, ask for a tailorisation of the dependability requirements concerning the deliverable analyses. For example, only FMECA synthesis or interfaces FMECA may be delivered by some sub-systems suppliers.

Moreover, industrial property rights prevents some suppliers to show the detailed design of hardware for evaluation of its robustness.

In addition to that, the effectiveness of conventional FMECA are increasingly limited by the evolution of technology (highly-integrated components such as FPGA, ASICs with indeterminist failure modes) and by the complexity of the space vehicles: performing FMECA for all the systems of one satellite is unrealistic and time-consuming. We rather promote the following approach:

2 THE PRELIMINARY RISK ANALYSIS APPROACH

2.1 *PRA in Context*

As shown in Figure 1, the Preliminary Risk Analysis starts in the early phase of design. FMECA are performed at functional level and then component level – only for critical functions – until RCD.

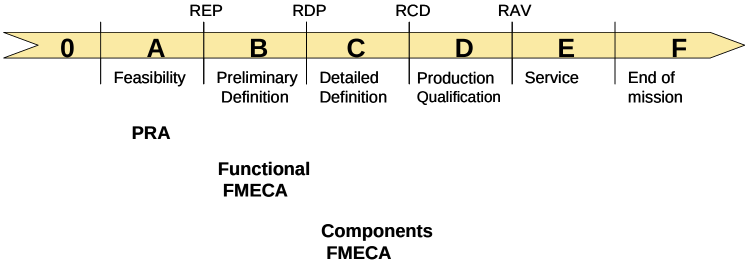

Figure1. PRA in project schedule

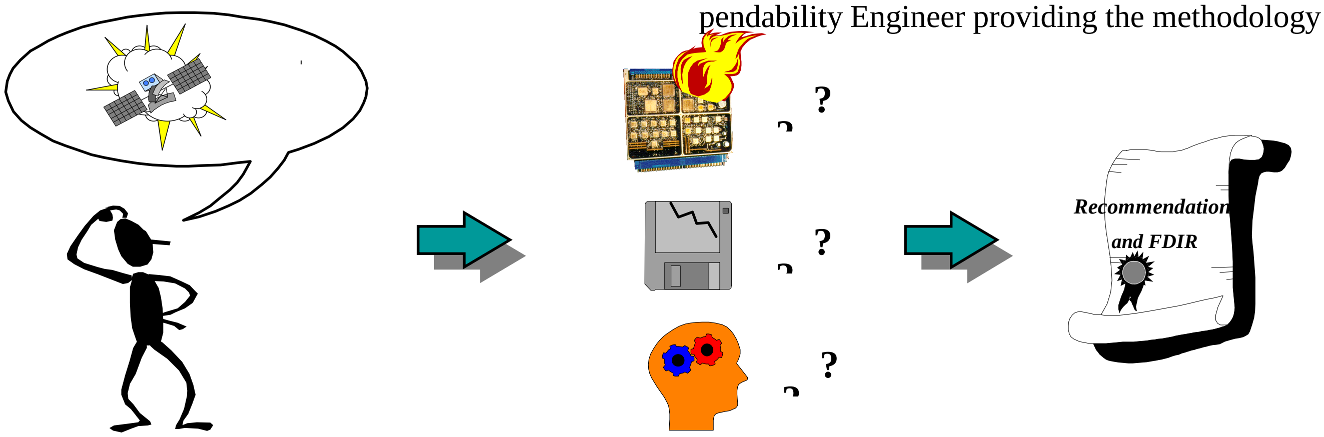

Fig2: PRA deductive approach

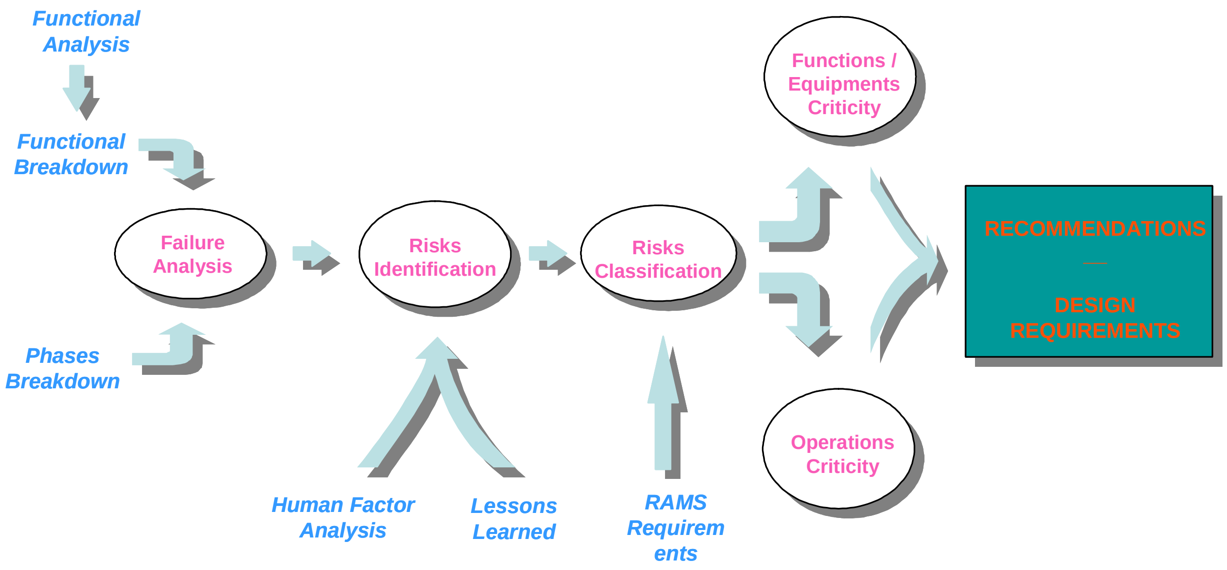

Fig3: Preliminary Risk Aanalysis Process

2.2 *Preliminary Risk Analysis Methodology*

The Preliminary Risk Analysis is a deductive analysis (top-down) approach starting from system-level feared events (FE), as shown in Figure 2.

Then we identify the possible causes (hardware, software, human factor...) and the main outputs is to propose recommendations and actions to reduce and control risks.

It also allows to build the FDIR (Failure Detection Isolation and Recovery) strategy and associated reconfiguration means.

One key result is to target additional analyses on critical functions: worst case, derating (part stress)…, to allocate objectives at sub-systems level, to study sub-systems interaction and also common-cause risks.

The best results are obtained when the analysis is performed by a working group including the Dependability Engineer providing the methodology and the System Designers providing the knowledge of the system architecture and functioning.

The Figure 3 shows the global process for performing the Preliminary Risk Analysis.

The risks identification is resulting from:

- Lessons learned: company experience database
- Use of more exhaustive systematic analyses such as:

- Functional failure analysis that evaluates the effects (and risks), for each function of the system, of the loss, the degradation or the untimely activation

Multiple failure are taken into account when Safety aspects are considered. (In that case, Fault-Tree can be used)

- Zonal Analysis to avoid failure propagation or incorrect interaction between different subsystems The Zonal Analysis is mostly used for launchers, and aircrafts as we will see later on in this paper. Satellites are more likely covered by tests.

- Human Factors: to insure the maximum effectiveness of tasks by operators

Table1: Risks classification table

Severity Classification	*Effects*
Catastrophic	Loss of human life, loss of launch site facilities or loss of system, severe detrimental environment effects.
Critical	Temporary disabling injury, major damage to flight systems or to ground facilities, major detrimental environment effects.
Marginal	Minor injury, minor disability, minor occupational illness, or minor system or environmental damage.
Negligible	Less than minor injury, disability, occupational illness, or less than minor system or environmental damage.

The classification can be tailored to each project for the mission success effects. (Safety effects are always standardized) In Table 1 is an example based on ISO-14620-1 “Space Systems Safety Requirements”.

2.3 *Outputs of the PRA: Recommendations / Requirements*

Of different kind :

- Requirements on functions, operations, hardware, software (one or multiple failure tolerance, robustness for environment constraints, ...)
- Design modifications such as specific protection, local redundancy, specific observable…
- Specific Operators training, …
- Need of focused analysis on some critical functions / parts: (FMECA, Worst Case Analysis, …)

2.4 *Preliminary Risk Analysis Advantages*

- Possible to start the PRA during early Project phases, without a clear defined design
- Early analysis having a real impact on the design: creation of monitoring, protections, redundancies or tests needs and controlling the technical, planning and costs risks
- Takes into account all the systems components (hardware, software, human factor) and their interactions
- Allows to target the focused analyses (FMECA to study failure propagation risks) that are complex and costly (time and money) on the identified critical items.
- Improves the specifications to the lower levels (e.g. dependability requirements for equipments suppliers, expressed as feared events)
- Fosters mutual understanding and exchanges between customers and suppliers
- Allows to keep record of technical choices

2.5 *Preliminary Risk Analysis Disadvantages*

Difficulty to evaluate beforehand the volume of the analyses required (contract problems)
Cultural difficulties caused by the company’s culture because the Dependability Engineer has a real impact on the design, and is not only a quality controller.
The results strongly depend on the quality of the inputs and participation of the designers.
No recognized norms: Preliminary Risk Analysis not a Safety Analysis!
Some difficulties to change the usual way of working pose some challenges. Indeed, the Preliminary Risk Analysis is not described in an ECSS standard, that recognize only the FMECA as a well-known, standard practice, specially among major private companies. Therefore, the PRA is typically a system-level activity.

3 CIVIL AIRCRAFT

3.1 *General Process*

The large civil aircraft are produced at industrial scale and standard certification process exist to control the system's risk in a well established certification process.
According to my experience on the Civil Aircraft JAR 25 certification process, the following steps are the baseline, with reference to the ARP 4754 and sister documents.

- Functional Hazard Analysis or FHA
- Preliminary System Safety Assessment or PSSA ("System" for the Aircraft stands for "Sub-system" for the Satellite)
- System Safety Assessment, leading to the certification completion

3.2 *Verification & Validation*

In addition to these formal steps, validation and verification tools exist at Aircraft level, allowing to exchange the safety and dependability requirements between interfaces systems, such as power supply for instance.

3.3 *Software DAL*

The DO 178B allocates for each level of severity a DAL or Degree of Assurance Level as shown in Table 2.
For each DAL exist a set of development rules. For example DAL A is required for systems with catastrophic potential failure such as flight controls. In that case, an extensive testing process and independent validation are required.
This simple, easy to understand rule is the most interesting point of the aircraft safety process.
This approach is introduced in the ECSS-Q-80C currently under public review.

Table 2: DAL allocation

DAL	Safety Effects	Safety Effects Description
A	Catastrophic	Prevents continued safe flight and landing
B	Hazardous	- Large reduction of safety margins or functional capabilities - Physical distress or higher workload for the crew - Serious or potentially fatal injuries to a small number of occupants
C	Major	Could reduce capability of the aircraft or the capability of the crew to cope with adverse operating conditions
D	Minor	Would not significantly reduce aircraft safety, and would involve crew actions well within their capabilities
E	No effects	Do not affect the operational capability of the aircraft or increase the crew workload

3.4 *Specific Analyses*

CCA Common Cause Analysis is sub-divised in the following analysis:

- CMA Common Mode Analysis
- ZSA Zonal Safety Analysis: to check that there are no possible physical interactions between independent systems
- PRA (Particular Risk Analysis in that case) : for specific risk with multiple-system impacts such as lightning strike, hail, tyre burst etc…

3.5 *Advantages of the Civil Aircraft Certification Process*

The main advantages of the civil aircraft certification process are:

- Systematic approach
- Strong guidelines and well established process
- Long experience of systems interaction validation tools

4 MERGING SPACE AND AERONAUTICS METHODS

4.1 *Benchmarking*

Still using our Preliminary Risk Analysis allowing to target the critical functions we would like to introduce improvements.

In a bench-marking approach, we propose to take the best practices from both worlds, in order to improve our dependability process.

Proposed improvements for space systems

- Systematic use of validation and verification tools to export requirements between systems: already beginning for some projects, hopefully the systematic process will be put in place in the coming years.

- Systematic introduction of DAL for the software and hardware according to the criticity of the functions: this is the most interesting outcome, because it simplifies the development process, with the condition that the DAL requirements are correctly assessed. Specially, that the PRA and FMEAs outputs (list of critical functions) are well transferred to the software / hardware developers.

4.2 *ARP 4754 Tailoring*

Inspired by the paper of Mr Audard, we could apply to space vehicles a tailoring of the ARP4754 process, just like he suggests for the Umanned Aerial Vehicles. Its main steps would be FHA, PSSA and CCA. Indeed, the UAV is very similar to satellite because it relies on on-board autonomy but also needs a ground control system.
This approach is very seducing to make the satellite dependability and safety process in a systematic way.

4.3 *Software Development*

Developing a safe and reliable software is facing the following potential problems:

- decorrelation between RAMS activities and software quality activities

- software reliability is not included in satellite reliability predictions

- software should be studied not as a stand alone but as part of system's functions, implemented by both hardware and software

5 CONCLUSION

Interesting perspective to compare space systems design to aircraft practices, those bigger interest is standardization and robustness. We can already witness that convergence has started on the DAL and on the validation process.

We hope to foster this exchanges and to be an active part of the standardization of the safety and dependability process for space systems.

6 REFERENCES

6.1 *Normative References*

- SAE ARP 4754: Certification considerations for highly-integrated or complex aircraft systems. (11.1996)
- SAE ARP 4761: Guidelines and methods for conducting the safety assessment process of civil airborne systems and equipment (12.1996)
- DO 178B: Software considerations in airborne systems and equipment certification (26.03.1999)
- European Cooperation for Space Standardization ECSS-Q-30B: Dependability (08.03.2002)
- European Cooperation for Space Standardization ECSS-Q-40B: Safety
- European Cooperation for Space Standardization ECSS-Q-80B Software Product Assurance (10.10.2003)
- European Cooperation for Space Standardization ECSS-Q-80C Software Product Assurance DRAFT2 (15.02.2008)
- ISO 14620-1: “Space Systems Safety Requirements”

6.2 *Publications*

- Audard, C (2006), “Innovative Methodology for Safety Assessment of medium to large civil Unmanned aerial vehicle”, EURO-UAV 2006
- “Dependability and safety issues for aerospace software”, G. Gigante & A. Vozella, Italian Centre for Aerospace Research, ESREL 2006
- “RAMS for aerospace: Better early or late than never”, A. Vozella, G. Gigante, L. Travascio & M. Compare, Italian Centre for Aerospace Research, ESREL 2006