

# Safety parameters management in ASTRIUM

6th IAASS Conference, May 2013

Laurence MEREDITH (ASTRIUM Satellites)

Cedric MAGNIN (ASTRIUM Space Transportation)

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

# ECONOMICAL CONTEXT VERSUS SAFETY

- Significant budget reductions for new developments compared to similar previous developments
  - Competition is very hard in space business for both institutional and private operators and satellite/launcher price is a major influence
- 
- Nevertheless, safety remains a major constraint and levels of system safety cannot be decreased
  - Not only safety issues have a human impact but they also lead to a bad company image and thus major financial consequences

- ➔ Need to design & produce ASTRIUM products
  - ➔ With high quality and high safety levels
  - ➔ With reduced cost AND compliant with customer requirements
- ➔ Use of Ranking Of Product Characteristics Process (ROPC)

# WHAT ABOUT ROPC PROCESS?

## ROPC : Ranking Of Product Characteristics

For which product ?

**All launchers, satellites, facilities or handling Systems... with Safety issues**  
(Reliability and availability issues as well)

Objectives ?

**To correctly size the design and manufacturing effort to build reliable and safe systems without over design**

Stakes ?

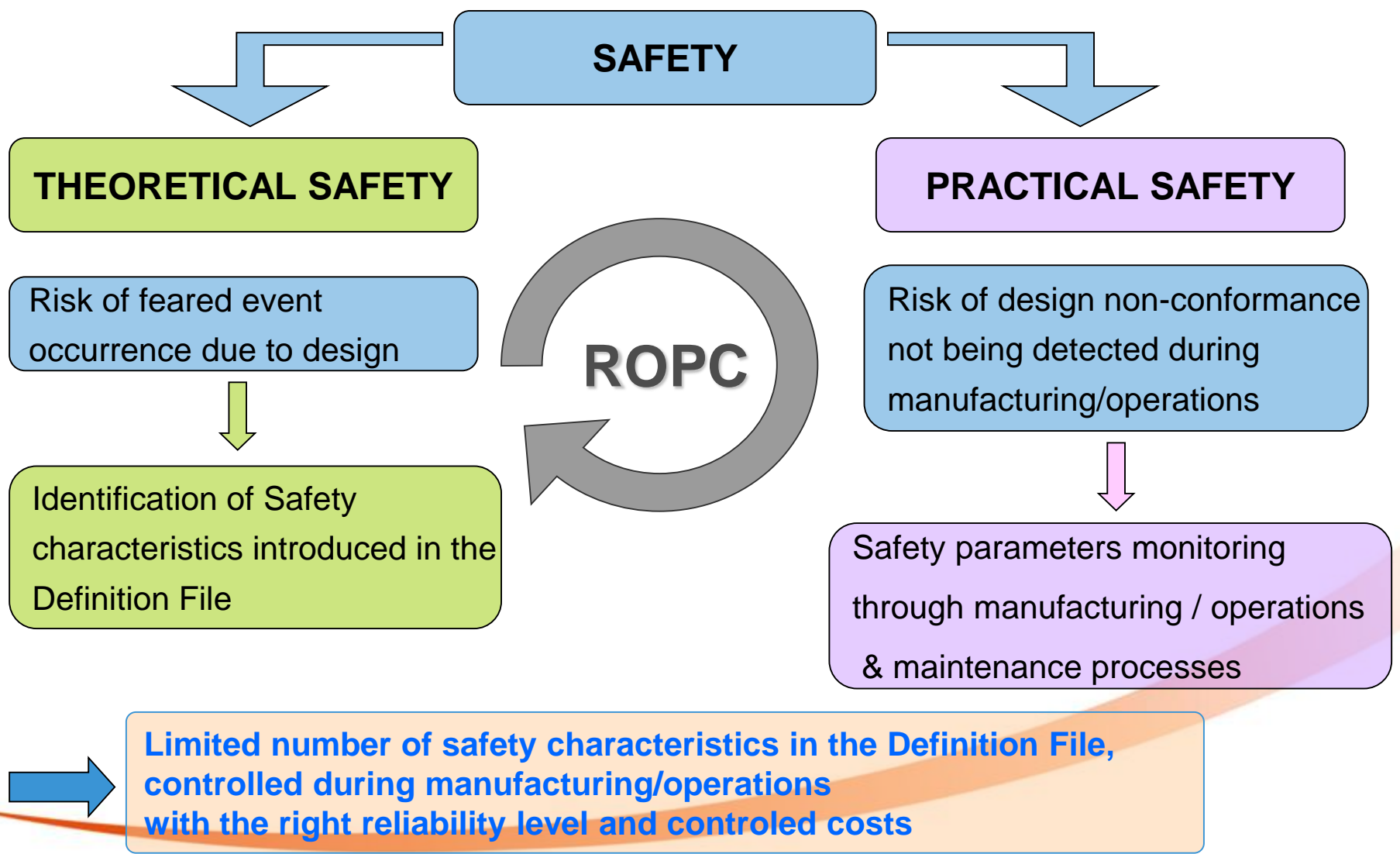
**Provide our customers with reliable and safe systems at the lowest possible price**

Applicability?

**From design to operations including maintenance and end of life**

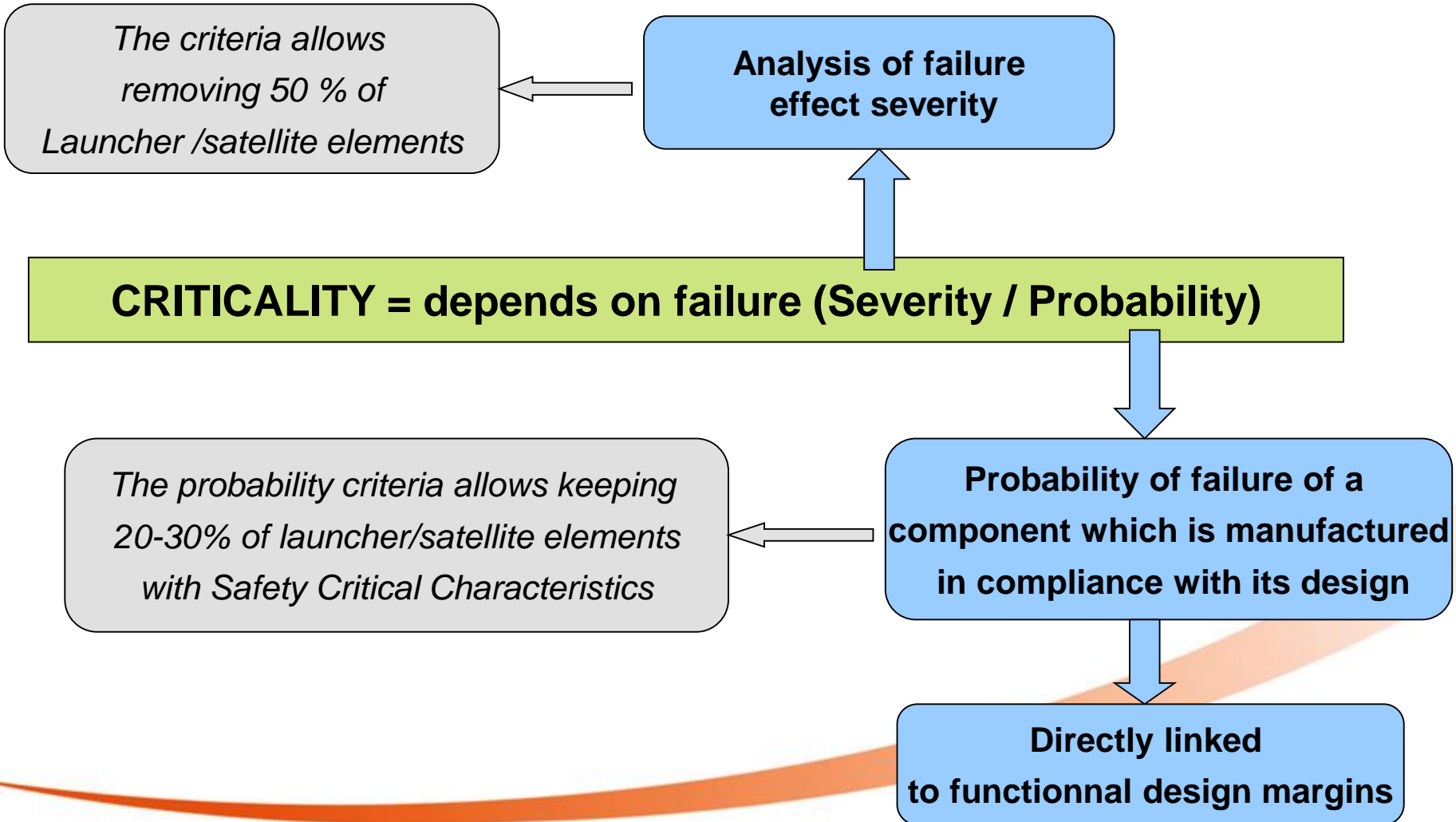
**ROPC**

# ROPC PROCESS TO ANSWER SAFETY ISSUES



This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

# Criteria for Ranking Of Product Characteristics



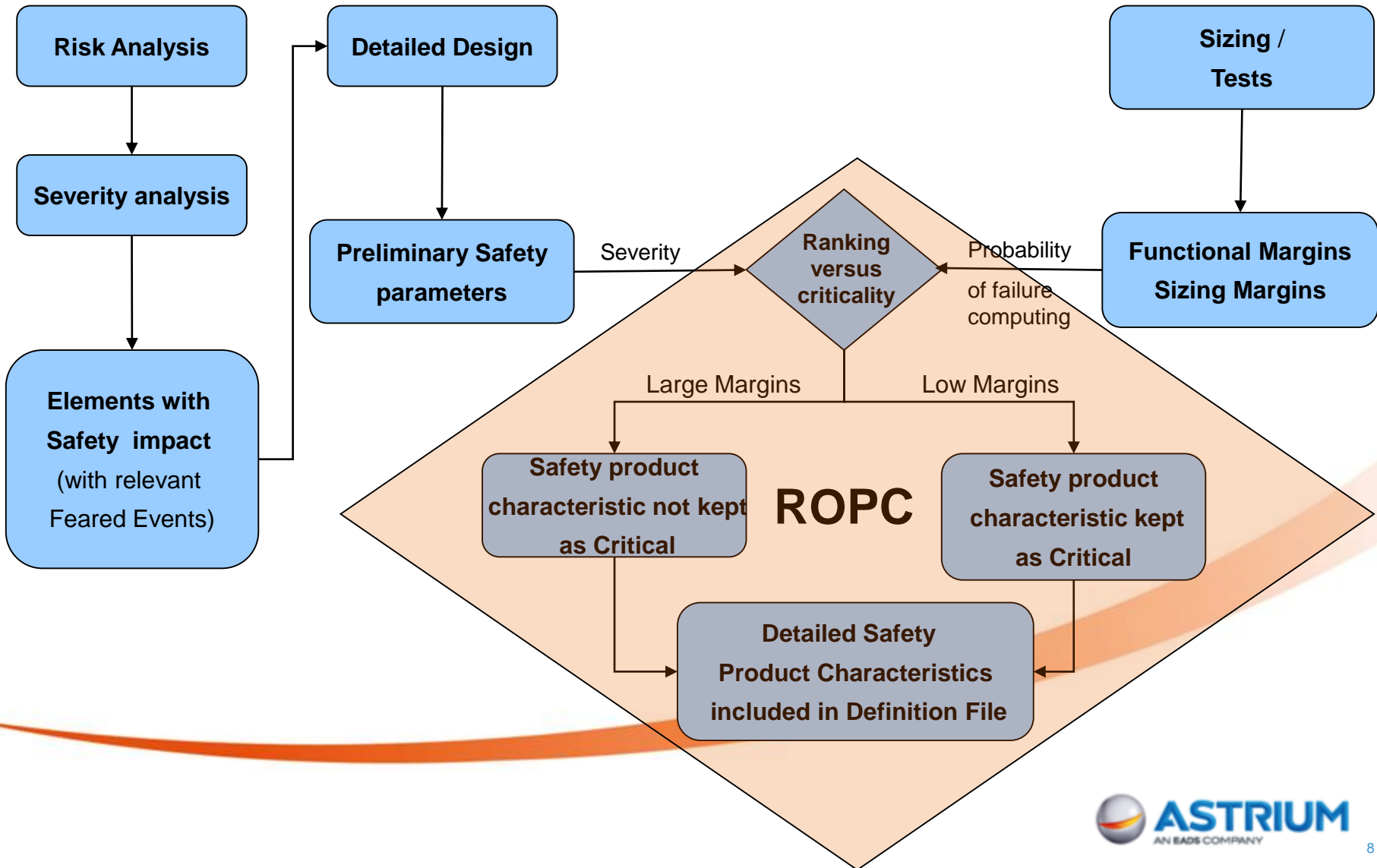
# Definition of safety severity

| Severity  | Level | Dependability<br>(refer to ECSS-<br>Q-30)     | Safety<br>(ECSS-Q-40)   |
|---|-------|---|---|
| <b>Catastrophic</b>   | 1     | Failures propagation                          | Loss of life, life-threatening or permanently disabling injury or occupational illness;   |
|   |       |   | Loss of system;   |
|   |       |   | Loss of an interfacing manned flight system;  |
|   |       |   | Loss of launch site facilities;   |
|   |       |   | Severe detrimental environmental effects.   |
| <b>Critical</b>   | 2     | Loss of mission                               | Temporarily disabling but not life-threatening injury, or temporary occupational illness; |
|   |       |   | Major damage to interfacing flight system;  |
|   |       |   | Major damage to ground facilities;  |
|   |       |   | Major damage to public or private property;   |
|   |       |   | Major detrimental environmental effects.  |
| <b>Major</b>  | 3     | Major mission degradation                     | ---   |
| <b>Minor or Negligible</b>  | 4     | Minor mission degradation or any other effect | ---   |
| Note: When several categories can be applied to the system or system component, the highest severity takes priority |       |   |   |

# ROPC Criticality Grid

| Probability<br>(theoretical)<br>linked to design<br>margins | Failure Severity |                  |       |
|---|------------------|------------------|-------|
|   | Safety issue     | Mission<br>issue | Minor |
| High  | Critical         | Major            | Minor |
| Average   | Critical         | Major            | Minor |
| Low   | Minor            | Minor            | Minor |
| <b>CRITICALITY</b>  |                  |                  |       |

# LINKS BETWEEN ROPC & THEORETICAL SAFETY



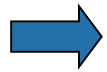
This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].



# LINKS BETWEEN ROPC & PRACTICAL SAFETY

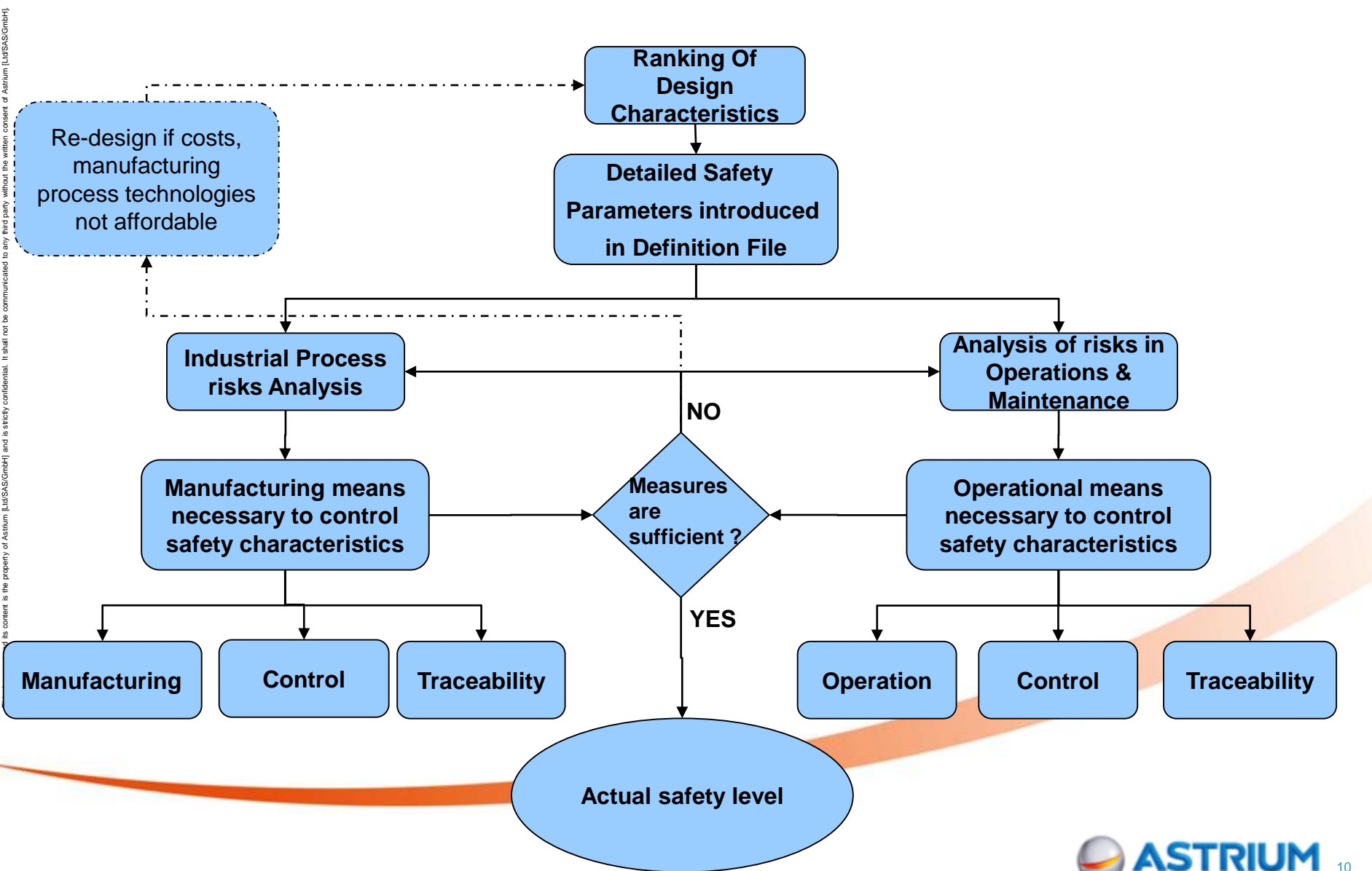
ROPC allows :

- Identifying the actual safety critical product characteristics (critical safety parameters)
- Concentrating efforts on those characteristics and put in place additional controls to those nominally performed during manufacturing/operations/maintenance/end of life



Those additional controls allow guaranteeing a probability of undetected non-conformity coherent with the expected safety level

# LINKS BETWEEN ROPC & PRACTICAL SAFETY



its content is the property of Astrium [LtdSAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [LtdSAS/GmbH].

# CONCURRENT ENGINEERING WITH SAFETY ENGINEER AND OTHERS STAKEHOLDERS

## Program Management / Customer

- Translation of customer requirements into design features for the system to be compliant with requirements
- Justification of safety level reached by the system
- Show relevant evidences

## Design

- Influence the design to be compliant to RAMS requirements
- Identify characteristics to be put in the ROPC

## Safety Engineer

## ILS Operations and Maintenance

- Participation in operational & maintenance safety critical procedures and in the Definition of the relevant required traceability
- Validation with Quality people that the operational & maintenance procedures reach the expected reliability level

## Manufacturing

- Participation in manufacturing safety critical procedures and in the definition of the relevant required traceability
- Validation with quality people that the manufacturing procedures reach the expected reliability level



# ROPC COHERENCY TABLE

- Design Definition :

| DEFINITION |             |                     |   |                                      |             |                                  |                    |                                  |                  |                  |   |
|------------|-------------|---------------------|---|--------------------------------------|-------------|----------------------------------|--------------------|----------------------------------|------------------|------------------|---|
| N°         | Component   | Component reference | Preliminary RAMS Product Characteristic | Product Characteristic (for ranking) | Value       | Function                         | RAMS parameter (s) | RAMS parameter (s) reference (s) | Proposed Ranking | Retained Ranking | Justification (including requirement traceability required by the manufacturing and control file) |
| 1          | Upper frame | L22H3210            | Design non conformity                   | Lower thickness of frame             | e= 4mm      | Ensure the subassembly integrity | Safety             | SA-001                           | critical (*C*)   | Critical         | Low margin (30% ) of frame  |
| 2          | phi12 screw | L22H3877            | Screw strength                          | Tightening torque                    | 19 Nm/+-10% | Fatigue strength of equipment    | Safety             | SA-005                           | critical (*C*)   | Critical         | Low margin after tightening.  |



Item



Characteristic



Safety or RAM reference parameter



Ranking



Justification

This document and its content are the property of Astrium Ltd (SAS/GmbH) and is strictly confidential. It shall not be commu

# ROPC COHERENCY TABLE

■ Manufacturing :

| MANUFACTURING  |  |   |  |                              |                   |   |                            |                         |          |                |               |           |
|--|--|---|--|------------------------------|-------------------|---|----------------------------|-------------------------|----------|----------------|---------------|-----------|
| Manufacturing and control process  |  |   |  |                              | Probability level |   |                            |                         |          | RAMS agreement |               | Actions   |
| Manufacturing  | Control  | Reference from manufacturing & control file (Manufacturing Order/Certificate of Conformity) | Certificate of Conformity from Quality Control | Evidence (value, conformity) | Objective         | Probability of occurrence of the source | Probability of propagation | Probability of no event | Result   | Agreement      | Justification |           |
| Use of numerically controlled machine. Machining 472/11.   | 3D Control.  | L22H11A2  | PV850F   | value 4+/-0,3                | 1,00E-05          | 1,00E-03                                | 1,00E-01                   | 1,00E-02                | 1,00E-06 | yes            |               |           |
| Tightening of the bolt in accordance with specific procedure & lock key. Use newscrews in every assembly | Control at 80% of tightening torque with independent loc key | SPI22H42  | PV007M   | Conformity                   | 1,00E-06          | 1,00E-03                                | 1                          | 1,00E-03                | 1,00E-06 | yes            |               | No action |



Controls relevant to supply and manufacturing

Tests and controls

Traceability

Probability

This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].

# ROPC COHERENCY TABLE

## Integrated Logistic Support

| Integrated Logistic Support                          |   |   |  |                              |                   |   |                            |                         |          |                |               |           |
|--|---|---|--|------------------------------|-------------------|---|----------------------------|-------------------------|----------|----------------|---------------|-----------|
| Relevant Manual (User's Manual / Maintenance Manual) | Reference of User's Manual / Maintenance Manual | Operation   | Control  | Evidence (value, conformity) | Probability level |   |                            |                         |          | RAMS agreement |               | Actions   |
|  |   |   |  |                              | Objective         | Probability of occurrence of the source | Probability of propagation | Probability of no event | Result   | Agreement      | Justification |           |
| no removable structure / no need of maintenance      |   |   |  |                              |                   |   |                            |                         |          |                |               |           |
| Maintenance Manuel                                   | MM2234  | Disassembling of equipment for preventive maintenance every 10 years. Use new screws. Tightening torque of 19 N.m | Control at 80% of tightening torque with independent loc key | conformity                   | 1,00E-06          | 1,00E-03                                | 1                          | 1,00E-03                | 1,00E-06 | yes            |               | No action |



Maintenance parameters



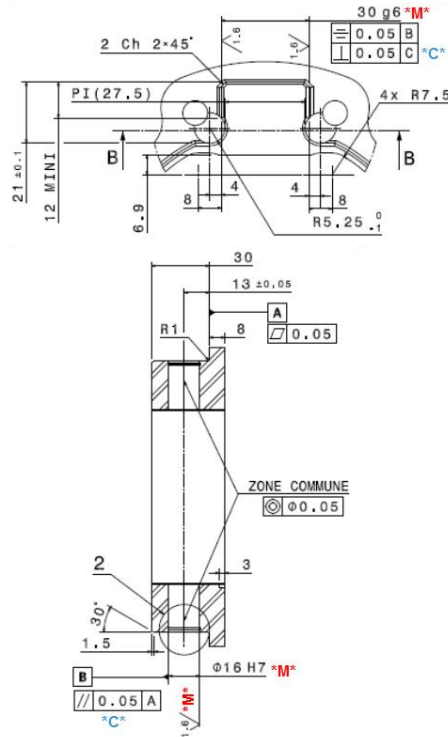
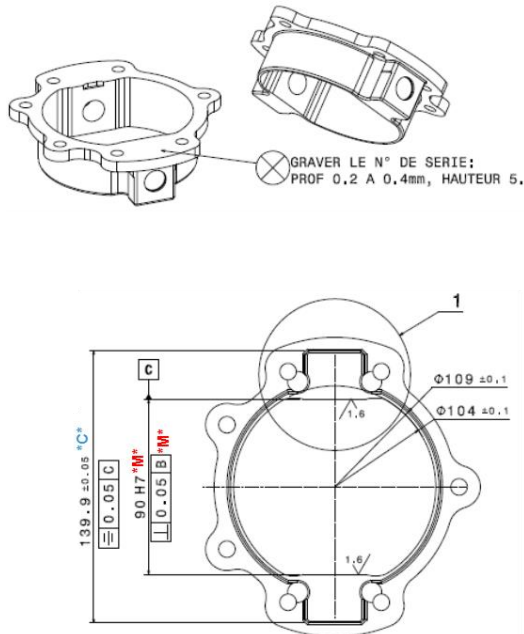
Probability

This document and its content is the property of Astrium [Ltd/SAS/GmbH] and is strictly confidential. It shall not be communicated to any third party without the written consent of Astrium [Ltd/SAS/GmbH].





# EXAMPLE TAKEN FROM ASTRIUM ST PRODUCT



## Manufacturing:

- Material supplied in accordance with standards required by Design Definition File
- At reception: check of material conformance by specified controls
- Reinforced traceability at each manufacturing step
- Manufacturing performed with certified tools with locked access
- Manufacturing by qualified personnel

## Control :

- Systematic control of each piece of equipment
- tridimensionnal control with automatic reference and auto-verification
- Controls follow certified locked programs

## Traceability :

- Items allowing traceability to the material used
- ROCP characteristics of the retained material
- References to procedures and programs used
- Value of each dimension figure retained in the ROCP

# CONCLUSION

## ■ ROCP allows :

- Focusing efforts on actual safety characteristics without over design or over budget
- Coherence all through the system development and lifetime phases, even in the case of product evolution
- Delivering products compliant with safety / RAM requirements with evidences all through the life cycle.

## ■ ROCP is being applied on current developments and costs saving are promising :

- Around only 20/30% of safety critical characteristic are kept in the ROCP tables, the others are rejected due to criticality selection criteria,
- Reduced number of rejected manufactured product are foreseen, reducing cost of treatment of non Quality
- Safety level compliant with the specifications with all evidences gathered in a single table