Product Assurance and management of risks in ESA spatial projects

Alain Heurtel
CNRS/IN2P3/LAL
heurtel@lal.in2p3.fr
Plan

• Product Assurance and Product Assurance Plan
• Principle of the risks policy
• Application : The HFI of the satellite Planck
• Preliminary Risks Analysis
• Reliability calculations
  – Definitions
  – The block diagram method
  – The failure rate determination
  – Examples
• Critical Items List
• Process FMECA
• Conclusion
Product Assurance

- Main characteristics of spatial projects:
  1. No possibility to repair in flight after launch,
  2. Important vibrations during launch,
  3. Necessity of cleanliness to avoid contamination redeposition in-flight.

- Consequences:
  Obligation to master the risks by a reflection accompanying the Project from conception to launch.

This is the domain of « Product Assurance »

As soon as the beginning of the feasibility phase, ESA imposes to draft the « Product Assurance Plan ». It will be up-graded along the project and presented to milestones reviews.
The Product Assurance Plan (1/2)

The Plan contains the guidelines of the general technical activities and methods foreseen by the Project to design, to build, to control, to test the instrument before integration.

It is written by the Product Assurance Manager.
The Product Assurance Plan (PAP) (2/2)

- Product Assurance requirements are defined by the ESA ECSS documents (European Cooperation for Space Standardisation): [http://www.estec.esa.nl/ecss/](http://www.estec.esa.nl/ecss/) (after authorization)
- The PAP should be in agreement with these requirements. It is reviewed by ESA for approval.
- The management of PA is made through a network of Local Product Assurance Managers (one for each sub-system).
Principle of the risks policy

How to master the risks?

1. To search for the risks: early, then continuously:
   - Preliminary Risks Analysis: written at system level by PAM.

2. To classify them according to a hierarchical system considering their seriousness:
   - Critical Items List: written by each team and coordinated by the PAM.

3. To accept them or to treat them:
   - Reliability Analysis: performed by the PAM, in parallel.

4. To analyse the consequences on the Instrument:
   - Failure Mode Effect and Critical Analysis (Process FMECA).

Alain HEURTEL CNRS/IN2P3
The High Frequency (HFI) Instrument of Planck

Planck "cornerstone of ESA programme"

- **Principle**: 2 surveys of the sky by detection of the cosmic background (14 months).
- **Technology**: Detection in mm range by horns and bolometers at 100mK ± 5mK. 280kg.
  3 coolers: Liquid H$_2$ and liquid He are obtained by close loops. Dilution of $^3$He in $^4$He cryostat in an open loop from boarded spheres of gas.
  Satellised at L2 (1.5Mkm / the earth).
- **Management**: International consortium of 250 people and 11 Institutes managed by Institut d’Astrophysique Spatiale (Orsay). Participation of 3 labs. of IN2P3 (LAL, PCC, ISN).
  ESA provides one Alcatel plate-form and launch in 2007 by Ariane V.
- **Budget**: Provisional budget of 100ME, including launch. French part provided by the CNES.
The High Frequency (HFI) Instrument of Planck

- Primary mirror (1.5m in Ø)
- Planck telescope
- Straylight shield
- LFI and HFI instruments
- Thermal shields
- Interface with Herschel
- Service Module screen
- Service module
- Solar cells

ACCELERATOR RELIABILITY WORKSHOP
4 February, 2002 Grenoble
1st step

Objectives:
1. Identification of the basic functional constituents of the instrument by functional analysis,
2. Early identification of the possible failure modes,
3. Timely design improvements to reduce the number of critical items and reduce risks.

Expected results:
- Forces a functional decomposition,
- Provides an early visibility on the adequacy of fault tolerances requirements,
- Guides the design in redundancy possibilities,
- Provides an early understanding of the degraded modes existing after one failure, and safety hazards.
The Preliminary Risks Analysis (2/3)

- ESA failure effect severity:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1a</td>
<td>Function whose failure could result in a catastrophic hazard</td>
</tr>
<tr>
<td>Category 1b</td>
<td>Function whose failure could result in a critical hazard</td>
</tr>
<tr>
<td>Category 2</td>
<td>Function whose failure could result in the loss or suspension of operational capability</td>
</tr>
<tr>
<td>Category 3</td>
<td>All other functions</td>
</tr>
</tbody>
</table>

- Ex: Possibilities of signal degradation along the functional chain.
  (coolers are considered as slaves devices at nominal temperature)
### Functional arborescence

<table>
<thead>
<tr>
<th>Feared events</th>
<th>Criticity</th>
<th>Concerned unit</th>
<th>Observable symptoms</th>
<th>Actions of risks reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Signal repeatability</td>
<td>2</td>
<td>HFI-S/C</td>
<td>- Telescope modelling. Pointing action.</td>
<td></td>
</tr>
<tr>
<td>1- No full sampling of the sky</td>
<td>2</td>
<td>HFI-S/C</td>
<td>- Telescope modelling. Pointing action.</td>
<td></td>
</tr>
<tr>
<td>- Distortions due to telescope layout</td>
<td>3</td>
<td>HFI</td>
<td>- Design control, simulations. Tests of qualification.</td>
<td></td>
</tr>
<tr>
<td>- Miss alignment of detectors along the sky scanning direction</td>
<td>3</td>
<td>HFI</td>
<td>- Design control, simulations. Tests of qualification.</td>
<td></td>
</tr>
<tr>
<td>- Uncertainties on polarisation measurements (leakage, cross-polarisation)</td>
<td>3</td>
<td>HFI</td>
<td>- Design control, simulations. Tests of qualification.</td>
<td></td>
</tr>
<tr>
<td>- Non similarity of beams from a given channel</td>
<td>3</td>
<td>HFI</td>
<td>- Design control, simulations. Tests of qualification.</td>
<td></td>
</tr>
<tr>
<td>- Horn focal centre out of focal centre of Planck</td>
<td>3</td>
<td>TM</td>
<td>- Analyse of electronical chain. Calibration phase and in flight control. Qualification tests.</td>
<td></td>
</tr>
<tr>
<td>3- In flight FPU unsettling due to launch</td>
<td>3</td>
<td>LFI/HFI</td>
<td>- Settling HFI/LFI struts assurance.</td>
<td></td>
</tr>
<tr>
<td>4- Struts breaking between HFI and LFI</td>
<td>3</td>
<td>HFI</td>
<td>- Loss of HFI instrument. Bonding assurance. (SPF)</td>
<td></td>
</tr>
</tbody>
</table>
Reliability : From evaluation to optimisation

• 2nd step (during the design phase)

• Objective: To evaluate the different possible architectures by comparison of their performances by statistic data.

• Conditions: The method must be sufficiently rich to describe the functioning of the product, but the simplest possible to be evaluated by the project.

• Methods of evaluation:
  – The universal generic method does not exist.
  – Limits:
    • Abusive utilization of quantitative analysis to justify risks which are difficult to measure,
    • Tendency to rejection of all quantification. Can lead to incoherent architectures.
  – For HFI we have used the RELIABILITY BLOCK DIAGRAM method. Others are complementary: Fault tree, Markov graph, Petri boxes etc…
Reliability : Definitions

1. Failure rate : $\lambda$

2. Reliability $R$. $\lambda$ is the probability of failure of system between $t$ and $t+dt$ when $dt \to 0$, with the item running at $t$. (Reliable at $t$)

$$\lambda(t) = \frac{dR(t)}{R(t)} \to R(t) = \exp\left(-\int_0^t \lambda(t) dt\right)$$

3. Life curve :

If $\lambda$ is constant during the useful life.

$$R(t) = \exp(-\lambda t)$$
Reliability : Definitions (Cont’d)

Failure rate $\lambda$ is often expressed in fits ($10^{-9}$ failure/hour)
Exp: Processor module $\lambda \approx 1000$ fits $\Rightarrow R_{(10y)} = 0.92$

4. Failure:

$$F(t) = 1 - R(t)$$

5. Associated definitions:

- MTTF : Mean Time To Failures (in hours) for a repairable system = $1/\lambda$
- MTBF Mean Time Before Failure
- If system not repairable MTTF= MTBF

$$R(t) = \exp(-1) = 0.37$$
$$\Rightarrow$$ MTBF is the time the component has a probability of failure of 0.63.
Reliability : The Bloc Diagram Method (BDM) (1/9)

- A chain of elements (mechanics or electronics) simultaneously supplied is figured by a combination of elements in serial or parallel.
- Serial diagram : Loss of the chain if 1 element fails

\[
\lambda_1 \quad \lambda_2 \quad \lambda_i \\
R_i = \exp(-\lambda_i t) \\
R = \Pi(R_i) \quad \lambda = \sum \lambda_i
\]

- Parallel diagram : Loss of the chain if all elements fail

\[
\lambda_1 \\
\lambda_2 \\
\lambda_i \\
R = 1 - [\Pi(1 - R_i)] \\
\frac{1}{\lambda} \approx \sum \left(\frac{1}{\lambda_i}\right)
\]

- Generalisation of the method :
  - Can be enriched by conditional probabilities.
  - If possibilities of redundancy exist, the different states of the system can be represented by a matrix (Markovian treatment). (Only if transition rates are constant : not for wear)

This method is used in CNES to modelise the essential of a satellite
Reliability : The Block Diagram Method (2/9)

- Kinds of redundancy:
  - Active M among N elements: All N elements function simultaneously,
  - Passive M among N: M-N elements are spare elements waiting for failure of active elements,
  - Cold/warm: characterises the energytical state of an element. ($\lambda_{\text{off}} = \lambda_{\text{on}}/10$),
  - Cross strapping: Sharing in elements individually redundated. Complex, slow down, can introduce risks in spite of electronics switches use.

- Recent enrichment of the symbolic:
  - Repairing rate,
  - Rate of use for active elements,
  - Incorporation of spare resources when redundancy is active.
Reliability : The Block Diagram Method (3/9)

- Ex 1: Functional electronics chain representation :
Reliability : The Block Diagram Method (4/9)

• Ex 1 (Cont’d) : Digital Processing Unit (DPU) chain :

Block Diagram representation:

All supplied elements are considered in serial

Problem : How to obtain $\lambda$ ?

$R_{DPU} = 0.9538$
Reliability : BDM (5/9) - $\lambda$ determination -

• Conventional methods : based on observable failures with fits of empirical models.
  Old norms : *reflect the real failure rates but they are not always regularly revisited.*
  – MIL HBK217 FDOD for military and Hi-Rel components only.
  – SRDF (EdF) for nuclear industry,
  – RDF 93 (CNET) for electronics.

• New vast domain of experimentation and investigation based on :
  – Quality tests and accelerated tries (life tests and thermal cycling, fatigue etc..), with application of acceleration factors.
  – Bayesian methods : combination of statistic data based on total probabilities of different causes, with a previous a priori knowledge : (return of experiences, empirical assessments, experts advices).

Recent norms : *returns of experiments and accelerated methods.*
  – RDF 99 UTE 80810 (CNET)
  – RAC 97 (Reliability Analysis Centre)
  – PRISM RAC (US) for mechanisms
  – ESA  PSS-01-302 for mechanics and electronics.
Ex 1: (cont'd)

R total = 0.8676

R total = 0.94043

With cross strapping between DPU and REU = 0.94212

- Clearly: Important increase in reliability if redundancy: ~7% for 2 years.
- Only relative differences are significant.
• Ex 2: $^3$He and $^4$He distribution chains from spheres at RT
Reliability : The Bloc Diagram Method (8/9)

- Reliability of the chain with redundanced element gives 0.966 (1.2% gain).
  Limited by weak point : Pressure reducer,

- For mechanics :
  - Studies are complex: Several possibilities of failure exist for valves depending on applied pressure, mode of functioning (untimely and/or loss of function).
  - Less data available than for electronics.
  - Influence of functioning rate. Are the failure rates applicable when valves are actuated only 2 or 3 times during the mission instead of each hour?

- This domain of failure physics is in expansion :
  - Modelling of extrinsic failure.
  - Priority : Refine models leading to $\lambda$ determination.
Reliability : The Bloc Diagram Method (9/9)

- **Conclusion**:
  - The BDM allowed us to modelise a large part of HFI,
  - The evaluations are still delicate for domains out of electronics,
  - Quantitative results should be used in relative.

- **Tools**:
  - MIL STRESS Item Software
  - REFLEX Reflex Software Corporation
  - FIABEX of CEP System
  - CARE distributed by Ligeron
  - SELECT from RAC
  - SUPERCAB+ from Cabinnovation (Supported by the CNES).

  [http://www.cabinnovation.fr](http://www.cabinnovation.fr)

- **Information** : Centres de Compétences Techniques CCT (CNES):
  Contact : [Andre.Cabarbaye@cnes.fr](mailto:Andre.Cabarbaye@cnes.fr)
  [Roland.Laulheret@cnes.fr](mailto:Roland.Laulheret@cnes.fr)
Critical Items List (CIL) (1/4)

- 3rd step of the ESA risk management policy.
- Definition of a critical element:
  « All element (hardware or software) or an elementary process, which may particularly endanger the development or mission success. It offers a reduced degree of confidence about their own performances in operation, if not previously "adequately" controlled on ground, during manufactures and tests phases ».
- Applicable for:
  - Not yet developed item,
  - Items that cannot be controlled for the relevant properties without degradation,
  - Items whose functionality can no longer tested after integration as they may fail during acceptance testing unnoticed,
  - Items provided by inexperienced institutes,
  - Items located at interfaces.
Critical Items List : (2/4)

• The actions to be taken :
  – Render them non-critical,
  – Control the criticality by dedicated actions.

• Methodology :
  – On demand of the Project, the lists of Critical Items and proposed actions to reduce them are written by the different groups,
  – They are centralised at Project level by the Product Assurance Manager,
  – Each group is responsible for its actions of risk reduction.
  – Each group shall inform the Project when the action is closed, for validation.

• Official diffusion :
  The actualised List is sent to each group and to ESA with the Monthly Report.
### Critical Items List (CIL) (3/4)

- **Format of the list**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITEM NUMBER</td>
<td>Relative to the considered S/S</td>
<td></td>
</tr>
<tr>
<td>HFI SUPPLIER CODE (LABEL)</td>
<td>HFI Supplier code as identified in the Project</td>
<td>See Product tree</td>
</tr>
<tr>
<td>CRITICAL CATEGORY</td>
<td>The categories as identified in three groups</td>
<td>A: Safety or reliability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B: Fracture critical items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C: Limited life</td>
</tr>
<tr>
<td>CRITICALITY</td>
<td>The categories as identified in two groups</td>
<td>M: Major: Special attention and treatment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by the Project Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>m: minor</td>
</tr>
<tr>
<td>ITEM IDENTIFICATION</td>
<td>The item is identified univocally with the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration number and / or a synthetic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>RISK</td>
<td>Reason for criticality</td>
<td>e.g.: process not space qualified, ESD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sensitive, …</td>
</tr>
<tr>
<td>ACTIVITY FORESEEN OR</td>
<td>Control plan, actions implemented and completion</td>
<td>e.g.: analysis resistance, test verification</td>
</tr>
<tr>
<td>IMPLEMENTED</td>
<td>data</td>
<td>foreseen, visual inspection to be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>performed, …</td>
</tr>
<tr>
<td>STATUS</td>
<td>Open / close</td>
<td>In case of closure, provide the reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of closure (MoM, fax, report, …)</td>
</tr>
</tbody>
</table>

| REFERENCE OF DOCUMENT     | TO CLOSE THE ACTION                              |                                            |

Alain HEURTEL CNRS/IN2P3
## Critical Items List: Ex. of worksheet (4/4)

<table>
<thead>
<tr>
<th>N°</th>
<th>LABEL</th>
<th>CRITICAL CATEGORY</th>
<th>CRITICALITY</th>
<th>ITEM IDENTIFICATION</th>
<th>RISK</th>
<th>ACTIVITY FORESEEN OR IMPLEMENTED</th>
<th>STATUS</th>
<th>REFERENCE DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PHAABM</td>
<td>A</td>
<td>SPF</td>
<td>M</td>
<td>Clamping mechanism between 0.1K and 4K during launch</td>
<td>No opening of the 3 fingers</td>
<td>Evaluation / Qualification Program to be proposed. Lubrication to be proposed to avoid permanent molecular contact</td>
<td>Open</td>
</tr>
<tr>
<td>2</td>
<td>PHEF</td>
<td>B</td>
<td>m</td>
<td>Dilution cooler</td>
<td>Temperature fluctuations.</td>
<td>Assurance of correct DC functioning. Evaluation program to be proposed as soon as the mock-up.</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>PHAA</td>
<td>A</td>
<td>m</td>
<td>Welding of capillaries and gluing of tubes on plate heat exchanger</td>
<td>Residual molecular contamination by fluxes</td>
<td>Evaluation / Qualification Program to be proposed for tubes welding process.</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>PHAD</td>
<td>A</td>
<td>m</td>
<td>Electrical insulation of FPU</td>
<td>Faraday cage might be not correctly closed</td>
<td>Design, Evaluation / Qualification Program to be proposed for the Faraday cage setting</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>PHAA</td>
<td>A</td>
<td>m</td>
<td>HfY bulk material</td>
<td>To be qualified for space utilization</td>
<td>Evaluation / Qualification Program</td>
<td>Close</td>
<td>ESA TOS-QMC report 00/80</td>
</tr>
<tr>
<td>6</td>
<td>PHABC</td>
<td>A</td>
<td>m</td>
<td>CuBe bolometers plate</td>
<td>Wrong centering / FPU</td>
<td>Design, Verification Program to be proposed to centre the plates by optical and/or optical method</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>PHAAM</td>
<td>A</td>
<td>m</td>
<td>Cu plate beneath CuBe bolometer plate</td>
<td>Wrong setting, wrong thermal control</td>
<td>Design, Evaluation / Qualification Program to be proposed to study conditions of setting</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>PHAABM</td>
<td>A</td>
<td>m</td>
<td>Screws at internal plates with respect to vibrations</td>
<td>Risks of screws failure</td>
<td>Evaluation / Qualification Program to be proposed for correct screw and couple determination</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>PHAC</td>
<td>A</td>
<td>m</td>
<td>PIDs on bolometers plate (or beneath dilution plate)</td>
<td>In time incorrect assembly (gluing and/or screwing)</td>
<td>Evaluation / Qualification Program to be proposed to verify PID's assembly</td>
<td>Open</td>
<td></td>
</tr>
</tbody>
</table>
• 4th step of action in risk reduction.
• Aim: The instrument should keep the same performance along the mission. So, necessity to perform the analyse of possible degradation modes in flight, as soon as the design phase.

• Method:
  1. Detailed review of possibilities of failures (on time degradation and/or brutal failures) of each part of equipment and relevant interfaces.
  2. Determination of the damages and interferences on other sub-systems in terms of severity, by the mean of analyses:
     • made at system level for the instrument,
     • made at component level for the interfaces with the spacecraft,
     • applicable to all functions and all units: For on-board software special analysis is foreseen as soon as soft begins to be written.

• Result:
  – Modifications and recommendations are proposed to increase the reliability using to procedures (see example later-on).
  – Auto-check of the whole instrument before fabrication
ACCELERATOR RELIABILITY WORKSHOP
4 February, 2002, Grenoble
Process Failure Mode Effects and Critical Analysis (FMECA) (2/8)

• The criteria: "severity"

<table>
<thead>
<tr>
<th>Severity category</th>
<th>Nature</th>
<th>Failure effect At system level</th>
<th>Failure effect At sub-system level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Catastrophic</td>
<td>Loss of mission</td>
<td>Propagation to other subsystems</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Loss of system</td>
<td>Loss of functionality</td>
</tr>
<tr>
<td>3</td>
<td>Major</td>
<td>Mission degradation</td>
<td>Degradation of functionality</td>
</tr>
<tr>
<td>4</td>
<td>Negligible</td>
<td>Any other effect</td>
<td>Any other effect</td>
</tr>
</tbody>
</table>

• Rubrics of worksheets are different along the position of the element in the chain:

<table>
<thead>
<tr>
<th>Intermediate sub-system</th>
<th>End of system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td></td>
</tr>
<tr>
<td>Assumed failure mode</td>
<td></td>
</tr>
<tr>
<td>Local effect</td>
<td>Effect on sub-system</td>
</tr>
<tr>
<td>Next higher effect</td>
<td>Observable symptom</td>
</tr>
<tr>
<td>End effect</td>
<td>Prevention method</td>
</tr>
<tr>
<td>Failure detection method</td>
<td></td>
</tr>
<tr>
<td>Severity and redundancy</td>
<td></td>
</tr>
<tr>
<td>Isolation method</td>
<td></td>
</tr>
<tr>
<td>Recovery method</td>
<td></td>
</tr>
<tr>
<td>Remarks</td>
<td></td>
</tr>
</tbody>
</table>
• In practice:
  – To be efficient FMECA should be practised in each group in charge of sub-system and conducted by a cognizant manager,
  – All actors involved in a sub-system should participate to the analyses meetings,
  – All functions are successively analysed with their interfaces,
  – Worksheets are fulfilled during the meeting,
  – Manager gathers FMECA sheets and write the recommendations.
### Example: Precedent valve box

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Function</th>
<th>Assumed failure mode</th>
<th>Effect on subsystem</th>
<th>Observable symptoms</th>
<th>Prevention methods</th>
<th>Recovery method</th>
<th>Remarks/Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Entering connectors between valve box and spheres (1 for 'He and 3 for 'He)</td>
<td>Links spheres and valves box</td>
<td>Leaks in order</td>
<td>Helium for dilution cooling</td>
<td>Decreasing of flow through</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>High pressure transducer</td>
<td>Pressure measurements at entrance of valve box</td>
<td>Leakage</td>
<td>Helium for dilution cooling</td>
<td>Decreasing of flow through</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>High pressure transducer</td>
<td>Pressure measurements at entrance of valve box</td>
<td>Defective indication</td>
<td>Uncertainty on helium throughput</td>
<td>Wrong pressure indication</td>
<td>Consistency between T, P and mass flow</td>
<td>SPF</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>First stage of bistable valves</td>
<td>Helium spheres</td>
<td>Spheres selection</td>
<td>No helium flow from 1 or 2 or 3 spheres</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF (Red for 'He)</td>
<td>Redundancy only for 'He sphere</td>
<td>Functioning in degraded mode</td>
</tr>
<tr>
<td>5</td>
<td>Low pressure transducers</td>
<td>Provide helium low pressure</td>
<td>Leakage</td>
<td>Helium for dilution cooling</td>
<td>Decreasing of flow through</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF (Red for 'He)</td>
<td>Redundancy only for 'He sphere</td>
</tr>
<tr>
<td>6</td>
<td>Low pressure transducers</td>
<td>Provide helium low pressure</td>
<td>Incorrect pressure indication</td>
<td>Uncertainty on helium P and throughputs</td>
<td>Wrong pressure indication</td>
<td>Consistency between T, P and mass flow</td>
<td>SPF</td>
<td>None</td>
</tr>
<tr>
<td>7</td>
<td>Precooling valve on ground</td>
<td>Precooling valve on ground</td>
<td>Leakage</td>
<td>Decreasing of helium available quantity for dilution</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>8</td>
<td>'He and 'He safety valves</td>
<td>Evacuation of excessive gas flow (see precedent chapter)</td>
<td>Leakage</td>
<td>Helium for dilution cooling</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>9</td>
<td>Electro valves</td>
<td>To control throughputs</td>
<td>Loss of bistable function</td>
<td>No exact helium feed command</td>
<td>Impossibility to adjust throughputs</td>
<td>Quality assurance: - electronic circuit of command</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>Electro valves</td>
<td>To control 'He throughputs</td>
<td>Leakage / outside box</td>
<td>Helium for dilution cooling</td>
<td>Quality assurance: - life tests - helium proof joints - scrwering with appropriate couple</td>
<td>SPF</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
### Process FMECA (5/8)

**Ex : For the DPU (Data Processing Unit)**

<table>
<thead>
<tr>
<th>Num.</th>
<th>Item</th>
<th>Function</th>
<th>Assumed failure mode</th>
<th>Most probable cause</th>
<th>Local effects</th>
<th>Next higher Level</th>
<th>End Effects</th>
<th>F&amp;ailure detection Method</th>
<th>Severity/Redundancy</th>
<th>Isolation method</th>
<th>Recovery method in-flight</th>
<th>Remark/Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Boot PROM</td>
<td>Storage of Boot Program code</td>
<td>Permanent bit/word failure</td>
<td></td>
<td>Bad Instruction Reading</td>
<td>Boot Program crash</td>
<td>DPU out of order</td>
<td>Watchdog – No com.</td>
<td>I</td>
<td>None</td>
<td>Redundancy</td>
<td>Low probability</td>
</tr>
<tr>
<td>2</td>
<td>Boot PROM</td>
<td>Storage of Boot Program code</td>
<td>Permanent block/chip failure</td>
<td></td>
<td>Bad Instruction Reading</td>
<td>Boot Program crash</td>
<td>DPU out of order</td>
<td>Watchdog – No com.</td>
<td>I</td>
<td>None</td>
<td>Redundancy</td>
<td>Low probability</td>
</tr>
<tr>
<td>3</td>
<td>EEPROM</td>
<td>Storage of default version and new version of Application Program (code and constants)</td>
<td>Permanent bit/word failure</td>
<td></td>
<td>Lost of OBSW integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
<td>Error correcting</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EEPROM</td>
<td>Storage of default version and new version of Application Program (code and constants)</td>
<td>Permanent block/chip failure</td>
<td></td>
<td>No storage of 1 or 2 OBSW version</td>
<td>Case 1 : no Application Program execution after reset</td>
<td>HFI in degraded mode</td>
<td>Error Checksum</td>
<td>IV</td>
<td>None</td>
<td>Patch of the Application Program in RAM after each reset</td>
<td>No room for Application Program</td>
</tr>
<tr>
<td>5</td>
<td>Program RAM</td>
<td>Storage of Application Program</td>
<td>Temporary bit flip</td>
<td>SEU</td>
<td>Bad Instruction Reading</td>
<td>Application Program crash or bad execution</td>
<td>Watchdog – Boot Program checking</td>
<td>IV</td>
<td>None</td>
<td>DSP and RAM Watchdog Reset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Program RAM</td>
<td>Storage of Application Program</td>
<td>Permanent small block failure</td>
<td></td>
<td>Bad Instruction Reading</td>
<td>Application Program crash or bad execution</td>
<td>Watchdog – Boot Program checking</td>
<td>IV</td>
<td>None</td>
<td>Relocation of Application Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Program RAM</td>
<td>Storage of Application Program</td>
<td>Permanent large block failure</td>
<td></td>
<td>Bad Instruction Reading</td>
<td>Application Program crash or bad execution</td>
<td>Watchdog – Boot Program checking</td>
<td>I</td>
<td>None</td>
<td>Redundancy</td>
<td>Boot Program can send only Diagnostic Pack</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Data RAM</td>
<td>Storage of variables and constants</td>
<td>Temporary bit flip</td>
<td>SEU</td>
<td>Wrong Data Reading</td>
<td></td>
<td></td>
<td></td>
<td>IV</td>
<td>None</td>
<td>Tag of corrupted Data</td>
<td>DSP and RAM reset if needed</td>
</tr>
<tr>
<td>9</td>
<td>Data RAM</td>
<td>Storage of variables and constants</td>
<td>Permanent small block failure</td>
<td></td>
<td>Wrong Data Reading</td>
<td></td>
<td></td>
<td></td>
<td>IV</td>
<td>None</td>
<td>Relocation of Data and block access forbidden</td>
<td></td>
</tr>
</tbody>
</table>
Process FMECA (6/8)

- Follow-on actions:
  - Case (a) : Ex. of recommendation for Data Processing Unit (DPU).

  “Several other important points, remarks and questions can be made on September 2001. It is necessary to define:
  - Conditions of survival must be defined if the satellite voltage falls to or if it increases considerably. Procedures of stopping and procedures of starting have to be written,
  - Conditions of safety mode have to be written and consequences for the electronics boards must be determined and written,
  - Consequences of an impedance variation on the bus has also to be determined,
  - Consequences of one voltage variation of 1% between output connector and the supply of sub-system.
  - Consequences of activation of protection by Latch Current Limiter (LCL),
  - Consequences of brief and important power appeal on FPGA or and after restarting, for example,
  - Implementation of one redundancy policy for starting the different relays,
  - Filtering of current peak coming from the relays when starting,
  - After failure of the LCL, what procedure is foreseen to switch on the Data Processing Unit (DPU),
  - Procedure of management of power failures for Readout Unit-Processor and the Dilution Cooler Electronics.”
Process FMECA (7/8)

- **Follow-on actions** *(cont'd)*:
  - Case (b) : rejection of recommendation by the S/S team.
    - Rejected with the rationale for rejection.
  - Case (c) : alternative recommendation from the S/S team.
    - Action and a **due date** for the implementation,
    - The modified situation shall be treated on the same process FMECA worksheet to identify the improvements.
Process FMECA (8/8)

- 3 other documents will be issued from the FMECA
  - The Summary Failure Detection Isolation and Recovery (FDIR).
    
    \textit{How to manage the different potentialities of redundancies}.
  - The Worst Case Analysis on critical interfaces parameters, (for electronic components).
    
    For HFI, the ESA asked analyses is only the verification of margins.
    
    \textit{In theory, it would be done by analytical analysis of the transfer function of the device (Monte Carlo simulation). Can be a complex and heavy analysis.}
  - Hardware Software Interaction Analysis (HSIA).

- The 2 first documents should be presented one month before the PDR (Preliminary Design Review) to be evaluated by ESA.
  
  \textit{They can condition the passage in the phase of fabrication.}
Conclusion (1/2)

• The ESA policy in matter of risks is defined very early in the Project by the Product Assurance Plan based on the ECSS requirements.

• The methods, complementary each other, allowing to identify and to treat potential risks in terms of prevention and protection during the design phase are:
  – Preliminary Risks Analysis at system level: Determination of the basic functional constituents and of their failure mode.
  – Reliability analysis: Can size correctly the systems in function of needs. The Block Diagram Method, used for Planck, gives assessments on reliability for the whole instrument.
  – Critical Item List: For elements or processes which can endanger the mission success.
  – The Process FMECA: To determine the possible modes of degradation in functioning and their propagation.
Conclusion (2/2)

• ESA Product Assurance policy entails an inter-active reflection and a continuous feed-back through the different teams of the project during the design phase.

This risk policy is now mandatory in all spatial projects: final gained time is estimated by previous experiences, at a minimum 10 times time spent to realize these analysis.