ESRF

Accelerator Reliability Workshop
4 February, 2002

IN2P3
Institut National de Physique Nucléaire et de Physique des Particules

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.

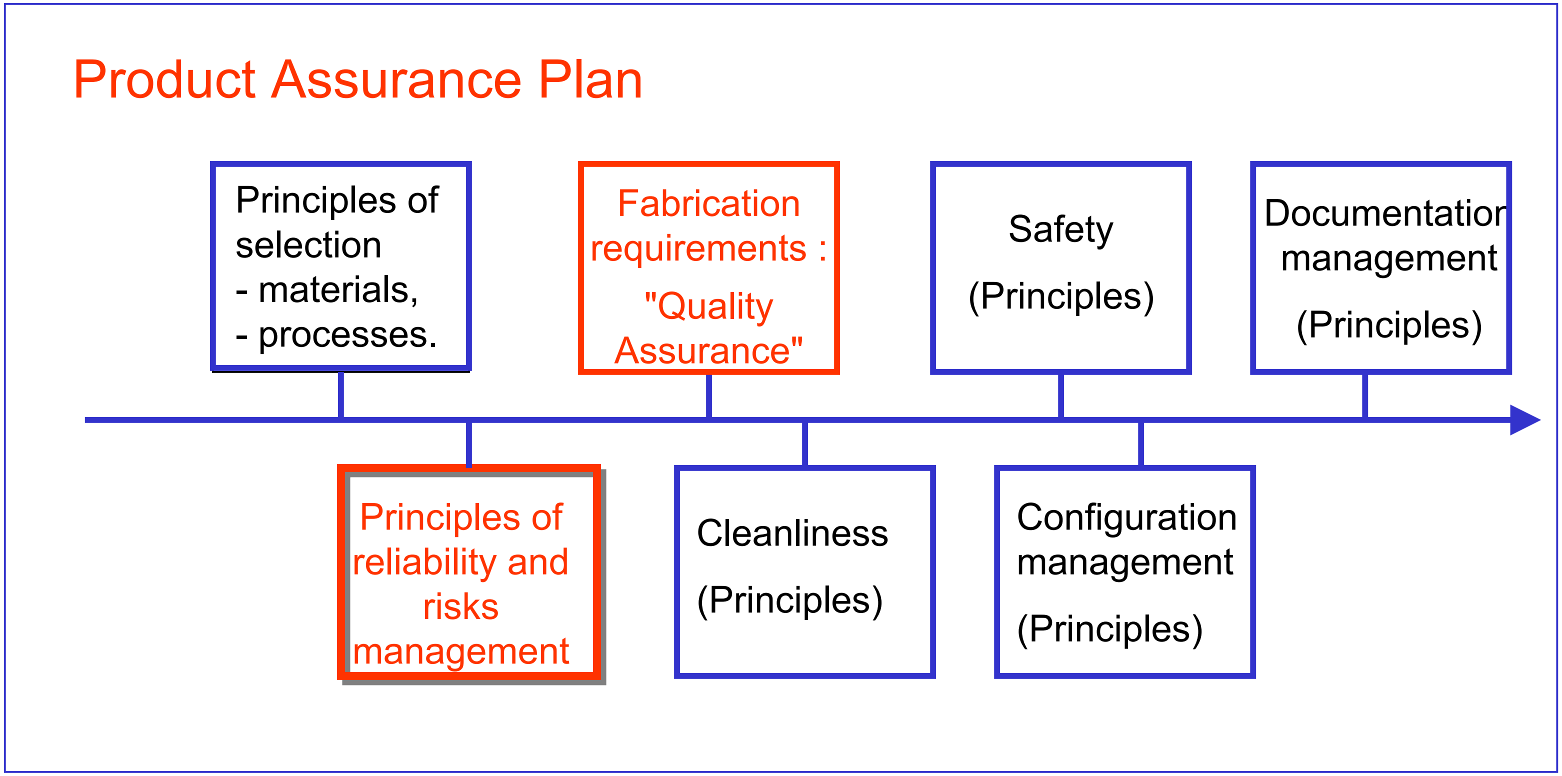
This is the domain of « Product Assurance »

> *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/ *(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).

Principe of the risks policy

How to master the risks?

1. To search for the risks : early, then continuously :

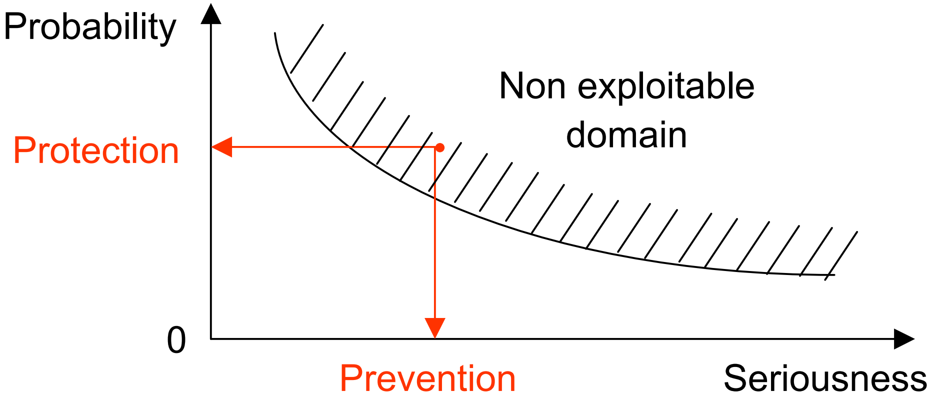
→ *Preliminary Risks Analysis : written at system level by PAM.*

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) .*

The High Frequency (HFI) Instrument of Planck

Planck "cornerstone of ESA programme"

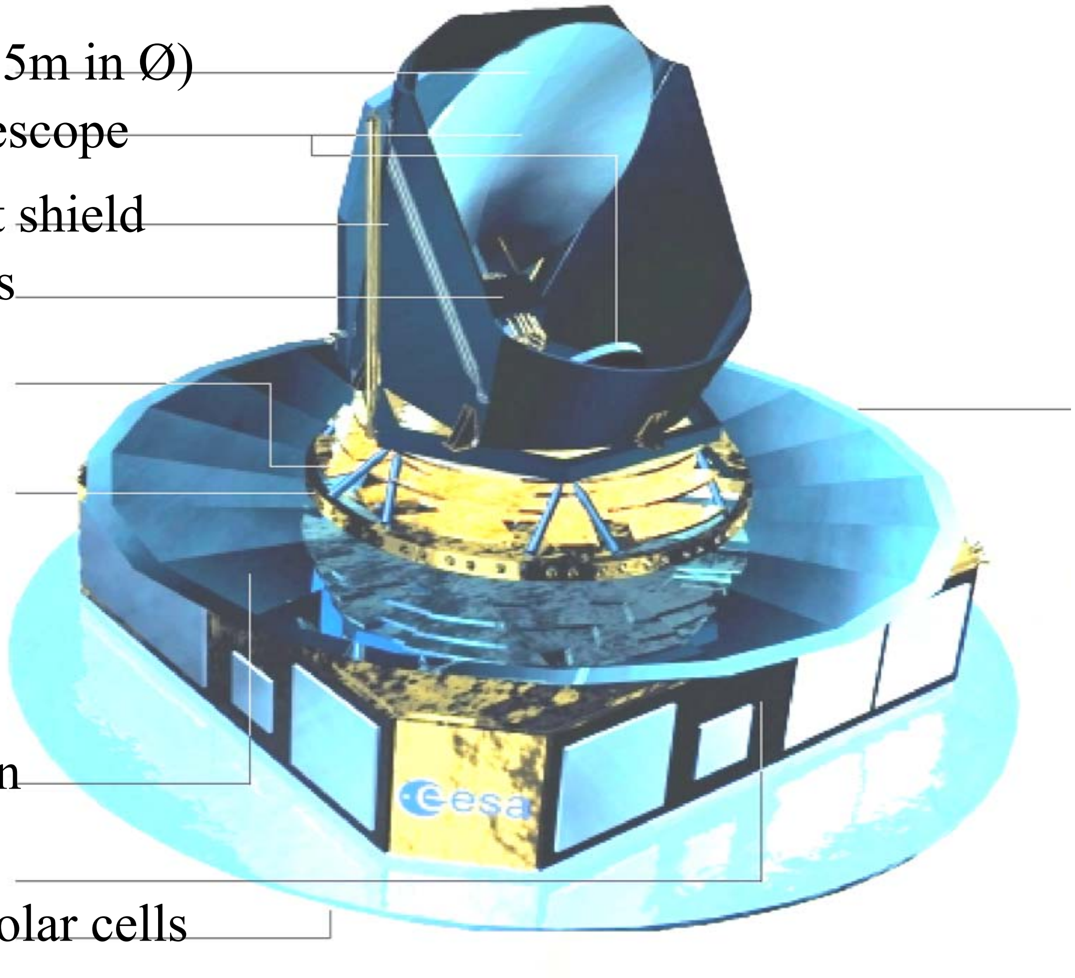
- Principle : 2 surveys of the sky by detection of the cosmic background (14 months).
- Technology : Detection in mm range by horns and bolometers at 100mK ± 5mK. 280kg.

  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

Panneaux solaires

The Preliminary Risks Analysis (1/3)

- 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.

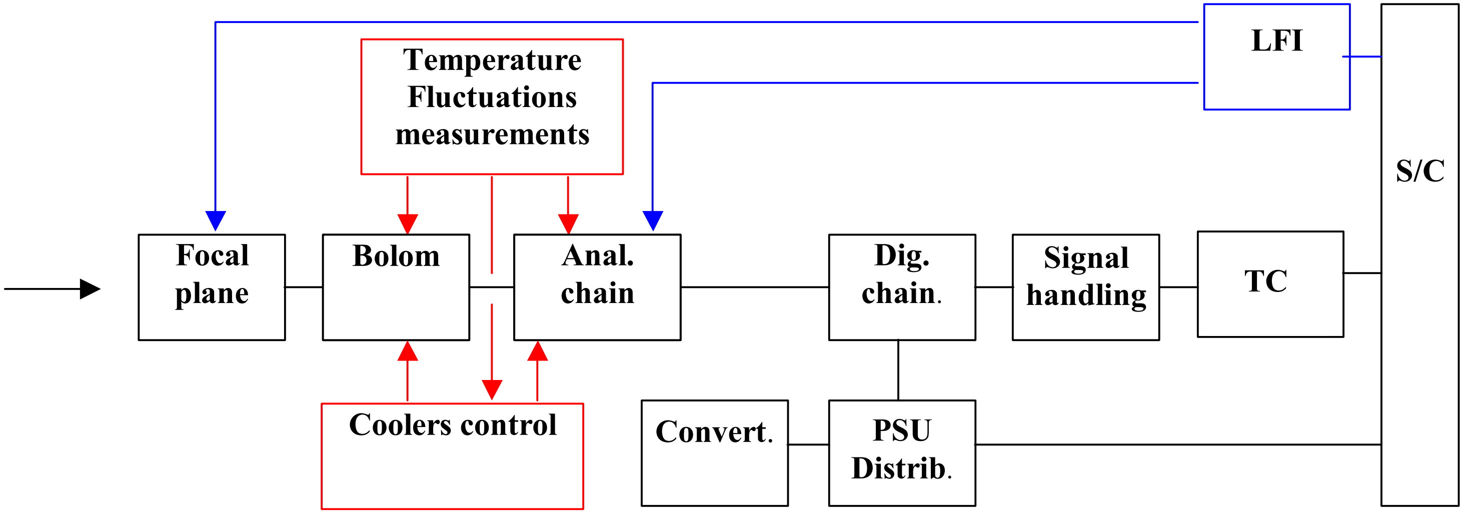
- Expected results :
  - Forces a functional decomposition,
  - Provides an early visibility on the adequacy of fault tolerances requirements,
  - Guides the design in redundancy possibilities,
  - Provides an early understanding of the degraded modes existing after one failure, and safety hazards.

The Preliminary Risks Analysis (2/3)

- ESA failure effect severity :

Category 1a	Function whose failure could result in a catastrophic hazard
Category 1b	Function whose failure could result in a critical hazard
Category 2	Function whose failure could result in the loss or suspension of operational capability
Category 3	All other functions

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



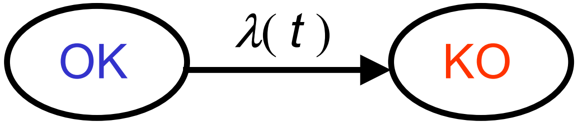
Preliminary Risks Analysis : (3/3) worksheet

Functional arborescence	Feared events	Criticity	Concerned unit	Observable symptoms	Actions of risks reduction
1. COLD OPTICAL SCIENTIFIC SIGNAL **1.1 Signal repeatability**	1- No full sampling of the sky	2	HFI-S/C		- Telescope modelling. Pointing action.
	2- Depointing				
	- Telescope focus shape not optimised	3	HFI		- Design control, simulations. Tests of qualification.
	- FPU positioning error/LFI	3	HFI		- Mounting, setting, Calibration Plan, Assurance of correct bonding with LFI.
	- Horns mis alignment with telescope	3	HFI		- Alignment Plan and Calibration Plan.
	- Distortions due to telescope layout	3	HFI-S/C		- Telescope modelling. Telescope Plan Tests.
	- Mis alignment of detectors along the sky scanning direction	3	HFI		- Design, fabrication, simulations on ground during calibration. Qualification tests.
	-Uncertainties on polarisation measurements (leakage, cross-polarisation)	3	HFI		- Design and horns fabrication. Development Plan. Qualification tests.
	- Non similarity of beams from a given channel	3	HFI	TM	- Analyse of electronical chain. Calibration phase and in flight control. Qualification tests.
	- Horn focal centre out of focal centre of Planck	3	HFI		- Modelling, calibration, Alignment Plan.
	3- In flight FPU unsettling due to launch	3	LFI/HFI		- Settling HFI/LFI struts assurance
	4- **Struts breaking between HFI and LFI**	1a	HFI		- **Loss of HFI instrument. Bonding assurance. (SPF)**

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 RELIABLITY BLOCK DIAGRAM method. Others are complementary : Fault tree, Markov graph, Petri boxes etc…

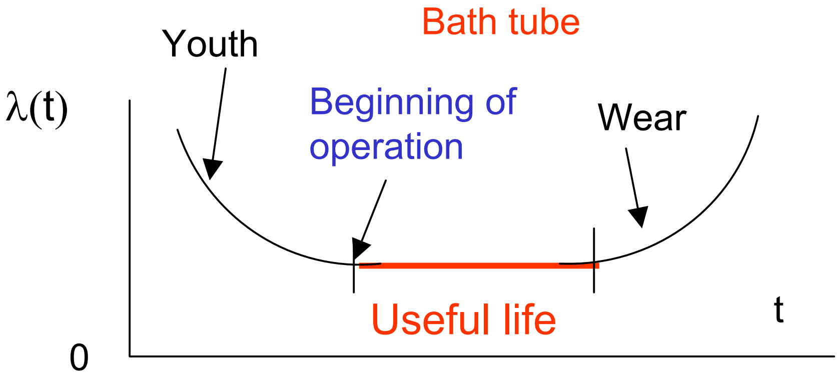
Reliability : Definitions



1. Failure rate : λ
2. Reliability R. λ is the probability of failure of system between t and t+dt when dt ⟶ 0, with the item running at t. (Reliable at t)

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

3. Life curve :



If λ is constant during the useful life.

$$\boxed{R(t) = \exp(-\lambda t)}$$

Reliability : Definitions *(Cont'd)*

Failure rate λ is often expressed in fits $(10^{-9}$ failure/hour)

Exp : Processor module $\lambda \cong 1000$ fits ⇒ $R_{(10y)} = 0.92$

4. Failure :

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

5. Associated definitions :

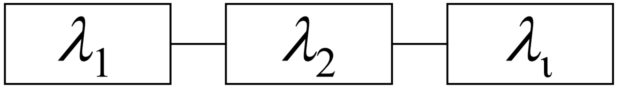
- MTTF : Mean Time To Failures (in hours) for a repairable system = $1/\lambda$
- MTBF Mean Time Before Failure
- If system not repairable MTTF= MTBF

$R(t) = \exp(-1) = 0.37$

⇒ MTBF is the time the component has a probability of failure of 0.63.

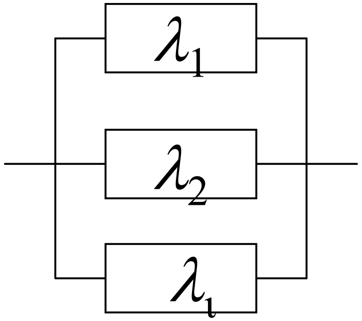
Reliability : The Bloc Diagram Method (BDM) (1/9)

- 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



$R_i=\exp-(\lambda_i t)$ $\quad R=\Pi(R_\iota)$ $\quad \lambda=\sum\lambda_i$

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



$R=1-[\Pi(1-R_\iota)]$ $\quad \frac{1}{\lambda}\approx\sum(\frac{1}{\lambda_i})$

- 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

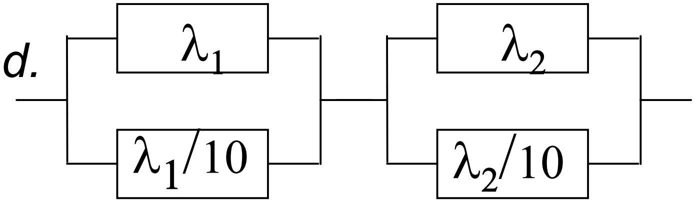
Reliability : The Block Diagram Method (2/9)

- 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.* ($\lambda_{off}=\lambda_{on}/10$),
  - Cross strapping :

    Sharing in elements individually redundated.

    Complex, slow down, can introduce risks

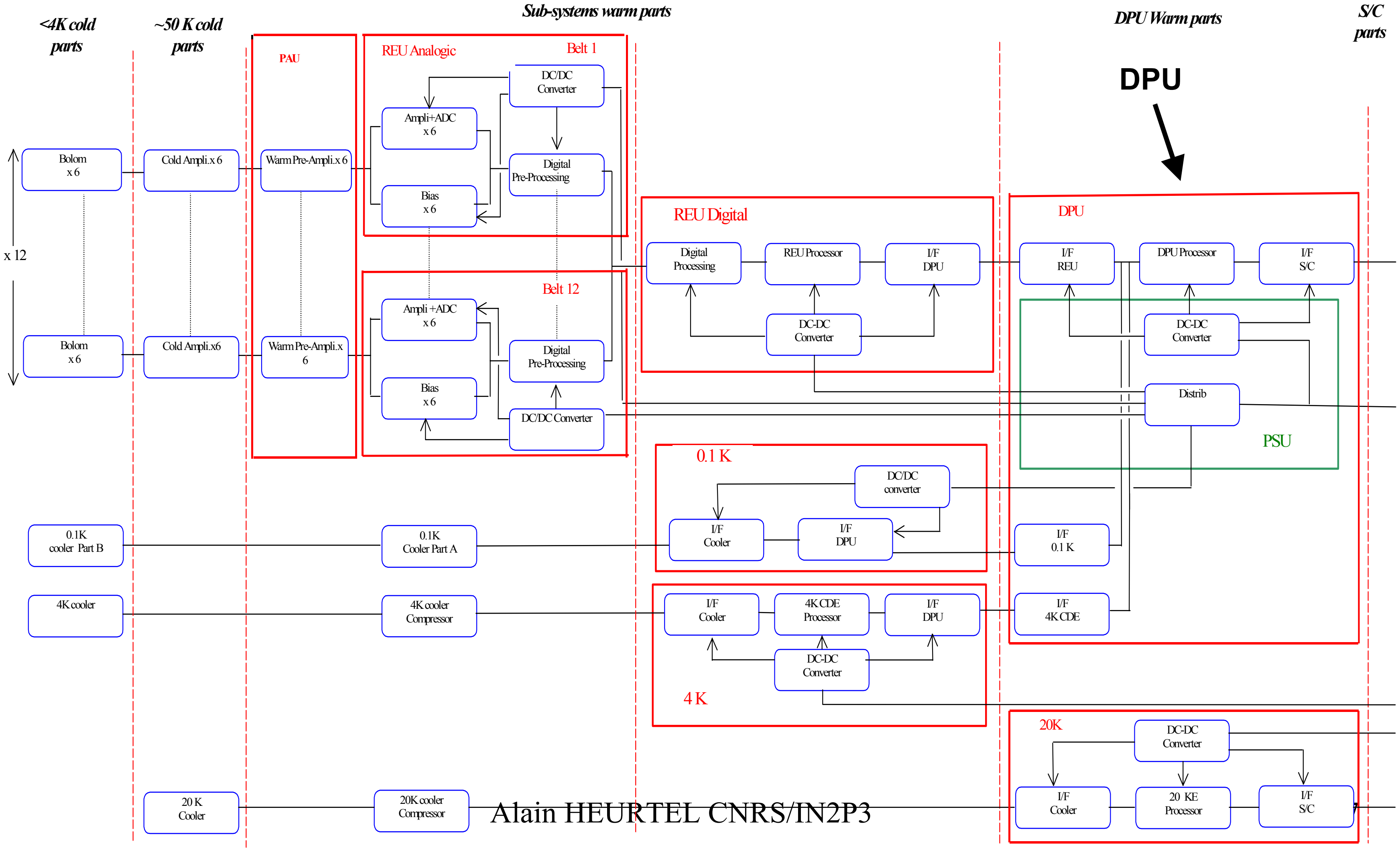
    in spite of electronics switches use.



- 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 :



<4K cold parts

~50 K cold parts

Sub-systems warm parts

DPU Warm parts

S/C parts

DPU

PAU

REU Analogic

Belt 1

DC/DC Converter

Ampli+ADC x 6

Digital Pre-Processing

Bias x 6

Bolom x 6

Cold Ampli.x 6

Warm Pre-Ampli.x 6

x 12

Belt 12

Ampli +ADC x 6

Digital Pre-Processing

Bias x 6

DC/DC Converter

Bolom x 6

Cold Ampli.x6

Warm Pre-Ampli.x 6

REU Digital

Digital Processing

REU Processor

I/F DPU

DC-DC Converter

I/F REU

DPU Processor

I/F S/C

DC-DC Converter

Distrib

PSU

0.1 K

DC/DC converter

I/F Cooler

I/F DPU

0.1K cooler Part B

0.1K Cooler Part A

I/F 0.1 K

4K cooler

4K cooler Compressor

I/F Cooler

4K CDE Processor

I/F DPU

DC-DC Converter

4 K

I/F 4K CDE

20K

DC-DC Converter

I/F Cooler

20 KE Processor

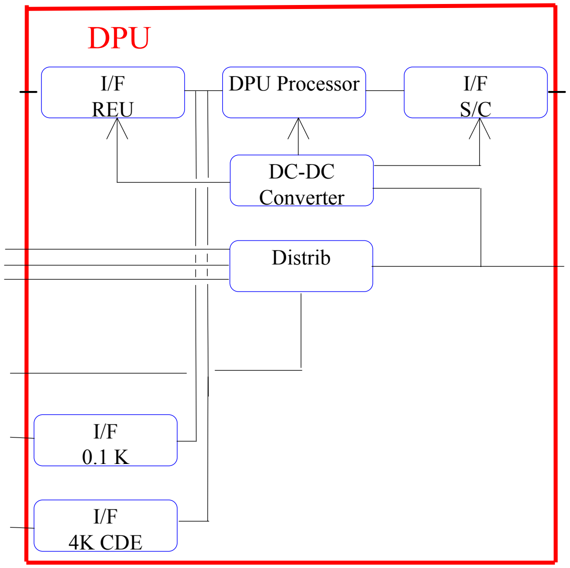
I/F S/C

20 K Cooler

20K cooler Compressor

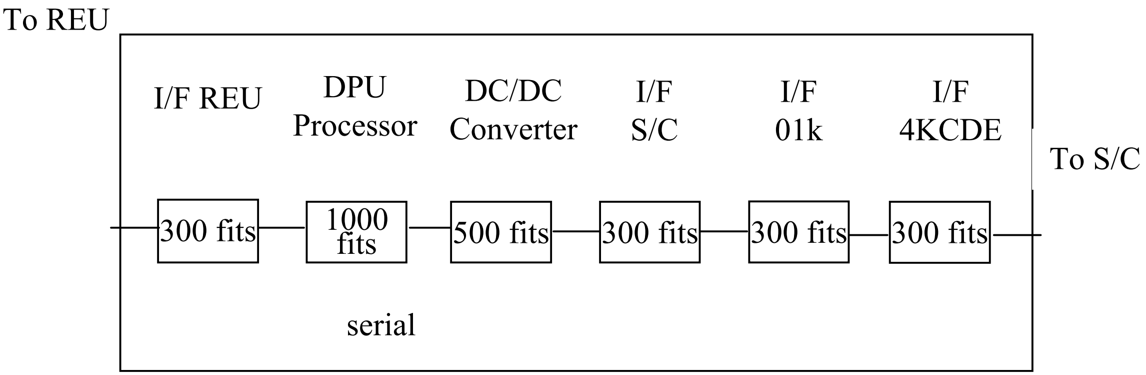
Reliability : The Block Diagram Method (4/9)

- Ex 1 *(Cont'd)* : Digital Processing Unit (DPU) chain :



Block Diagram representation:

All supplied elements are considered in serial



R_{DPU}=0.9538

Problem : How to obtain λ ?

Reliability : BDM (5/9) - λ 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).

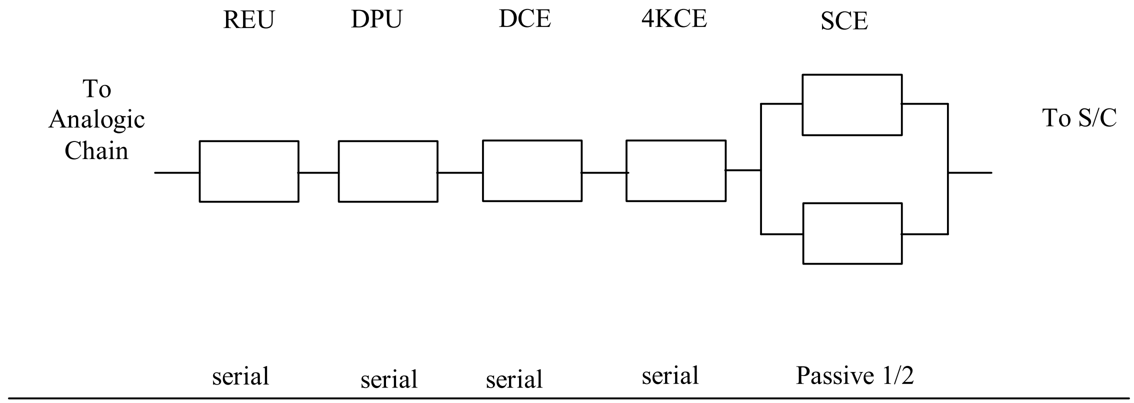
Recent norms : *returns of experiments and accelerated methods.*

- – RDF 99 UTE 80810 (CNET)
- – RAC 97 (Reliability Analysis Centre)
- – PRISM RAC (US) for mechanisms
- – ESA PSS-01-302 for mechanics and electronics.

Reliability : The Bloc Diagram Method (6/9)

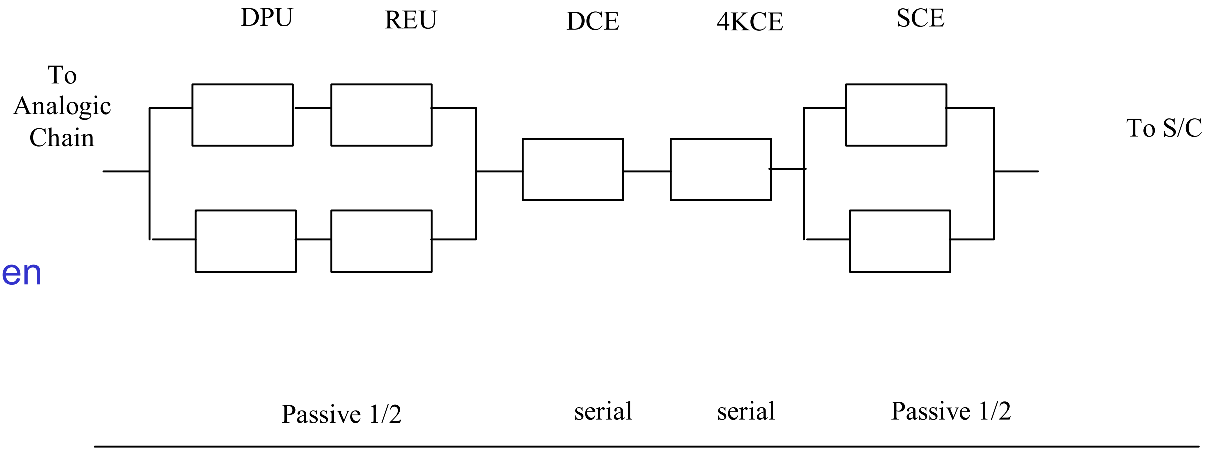
- Ex 1: *(cont'd)*

R total=0.8676



R total=0.94043

With cross strapping between DPU and REU = 0.94212

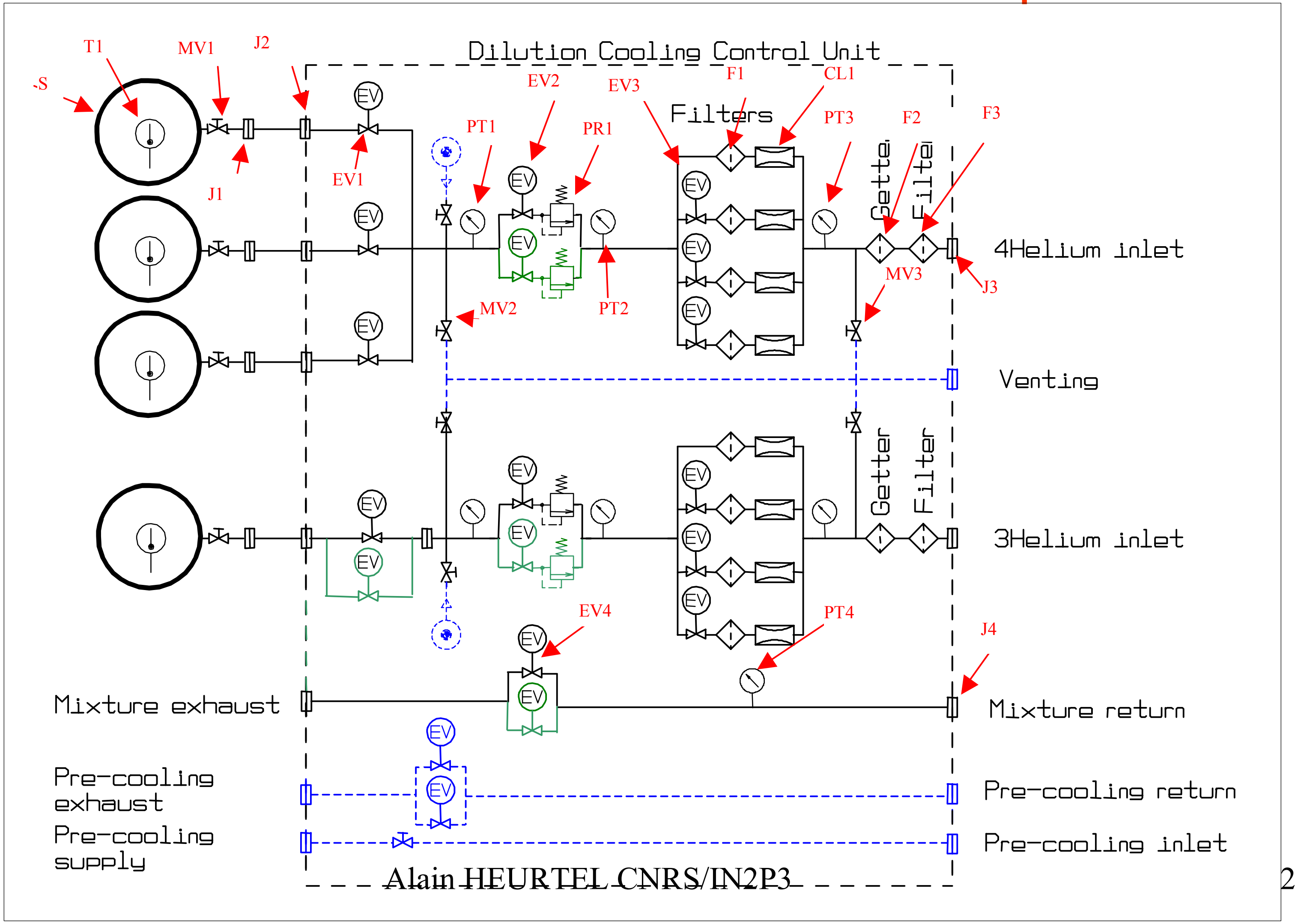


- Clearly : Important increase in reliability if redundancy : ~7% for 2 years.

- Only relative differences are significant.

Reliability : The Bloc Diagram Method (7/9)

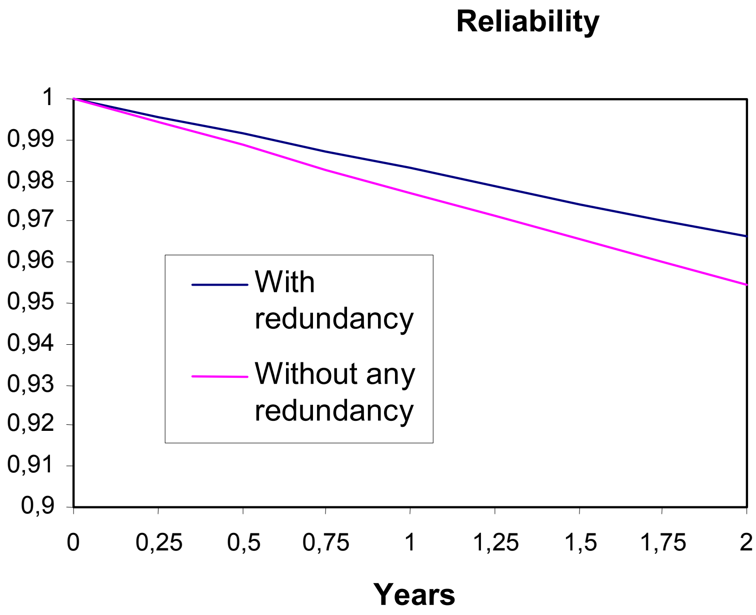
- Ex 2: ^{3}He and ^{4}He distribution chains from spheres at RT



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 λ 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
- Information : Centres de Compétences Techniques CCT (CNES) :

  Contact : Andre.Cabarbaye@cnes.fr
  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

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

Critical Items List : Ex.of worksheet (4/4)

N	LABEL	CRITICAL CATEGOR	CRITIC ALITY	ITEM IDENTIFICATION	RISK	ACTIVITY FORESEEN OR IMPLEMENTED	STATU	REFERENCE DOCUMENT
IAS (0.1K DILUTION COOLER WITH SUPPLIERS)					Management of actions to be taken by IAS			
1	PHAABM	A SPF	M	Clamping mechanism between 0.1K and 4K during launch	No opening of the 3 fingers	Evaluation / Qualification Program to be proposed. Lubrication to be proposed to avoid permanent molecular contact	Open	
2	PHEF	B	m	Dilution cooler	Temperature fluctuations.	Assurance of correct DC functioning: evaluation program to be proposed as soon as the mock-up.	Open	
3	PHAA	A	m	Welding of capillaries and gluing of tubes on plate heat exchanger	Residual molecular contamination by fluxes	Evaluation / Qualification Program to be proposed for tubes welding process.	Open	
4	PHAD	A	m	Electrical insulation of FPU	Faraday cage might be not correctly closed	Design. Evaluation / Qualification Program to be proposed for the Faraday cage setting	Open	
5	PHAA	A	m	HoY bulk material	To be qualified for space utilization	Evaluation/Qualification Program	Close	ESA TOS-QMC report 00/80
6	PHABC	A	m	CuBe bolometers plate	Wrong centering / FPU	Design. Verification Program to be proposed to centre the plates by optical and / or optical method	Open	
7	PHAAAM	A	m	Cu plate beneath CuBe bolometer plate	Wrong setting, wrong thermal control	Design. Evaluation / Qualification Program to be proposed to study conditions of setting	Open	
8	PHAABM	A	m	Screws at internal plates with respect to vibrations	Risks of screws failure	Evaluation / Qualification Program to be proposed for correct screw and couple determination	Open	
9	PHAC	A	m	PIDs on bolometers plate (or beneath dilution plate)	In time incorrect assembly (gluing and / or screwing)	Evaluation / Qualification Program to be proposed to verify PID's assembly	Open	

Process Failure Mode Effects and Critical Analysis (FMECA) (1/8)

- 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

Process Failure Mode Effects and Critical Analysis (FMECA) (2/8)

- The criteria : "severity"

Severity category	Nature	Failure effect	
		At system level	At sub-system level
1	Catastrophic	Loss of mission	Propagation to other subsystems
2	Critical	Loss of system	Loss of functionality
3	Major	Mission degradation	Degradation of functionality
4	Negligible	Any other effect	Any other effect

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

Intermediate sub-system	**End of system**
Number	
Item	
Function	
Assumed failure mode	
Local effect	Effect on sub-system
Next higher effect	Observable symptom
End effect	Prevention method
Failure detection method	
Severity and redundancy	
Isolation method	
Recovery method	
Remarks	

Process FMECA (3/8)

- 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.

Process FMECA (4/8)

- Example: Precedent valve box

Num.	Item	Function	Assumed failure mode	Effect on subsystem	Observable symptoms	Prevention methods	Severity/Redundancy	Isolation method	Recovery method in-flight	Remark/ Recommendation
1	Entering connectors between valve box and spheres (1 for ^{3}He and 3 for ^{4}He)	Links spheres and valves box	- Bad SS solder leading leakage with time - Leakage between intermediate part	Pipe is not transporting helium for dilution cooling	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF	None	None	
2	High pressure transducer	Pressure measurements at entrance of valve box	Leakage	Pipe is not transporting helium for dilution cooling	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF	None	None	$\sim 10^{-4}$ mb/ls leakage rate for internal leakage across valves and $\sim 10^{-6}$ mb/ls for external leakage.
3	High pressure transducer	Pressure measurements at entrance of valve box	Defective indication	Uncertainties on helium throughputs	Wrong pressure indication	Consistency between T, P and mass flow	2	None	None	
4	First stage of bistable valves	Helium spheres	Spheres selection	Impossibility to select all spheres	No helium flow from 1 or 2 or 3 spheres	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF (Red for ^{3}He)	Possible by electro valves actuation	Redundancy only for ^{3}He sphere.	Functioning in degraded mode. Note that two smaller ^{3}He spheres would lead to utilise a greater quantity of helium (down to 20 bars) than for only one.
5	Low pressure transducers	Provide helium low pressure	Leakage	Pipe is not transporting helium for dilution cooling	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF (Red for ^{3}He)	Redundancy only for ^{3}He sphere.	Redundancy only for ^{3}He sphere.	Functioning in degraded mode
6	Low pressure transducers	Provide helium low pressure	Incorrect pressure indication	Uncertainties on helium P and throughputs	Wrong pressure indication	Consistency between T, P and mass flow	2	None	None	Precise measure of instantaneous flow with sensors and measure of T of spheres
7	Precooling valve on ground	Precooling valve on ground	Leakage	Decreasing of ^{4}helium available quantity for the dilution	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF	None	None	Functioning in degraded mode
8	^{3}He and ^{4}He safety valves	Evacuation of excessive gas flow **See precedent chapter**	Leakage	Pipe is not transporting helium for dilution cooling	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF	None	None	**To be justified**
9	electro valves	To control throughputs	loss of bistable function	No exact helium feed command	Impossibility to adjust throughputs	Quality assurance: - electronic circuit of command	1	None	None	
10	electro valves	To control He throughputs	Leakage / outside box	Pipe is not transporting helium for dilution cooling	- Decreasing of flow throughput - Decreasing of pressure indication	Quality assurance: - life tests - helium proof joints - screwing with appropriated couple	1 SPF	None	None	

Process FMECA (5/8)

- Ex : For the DPU (Data Processing Unit)

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

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 Procsssing 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).

    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.

    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.

  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.