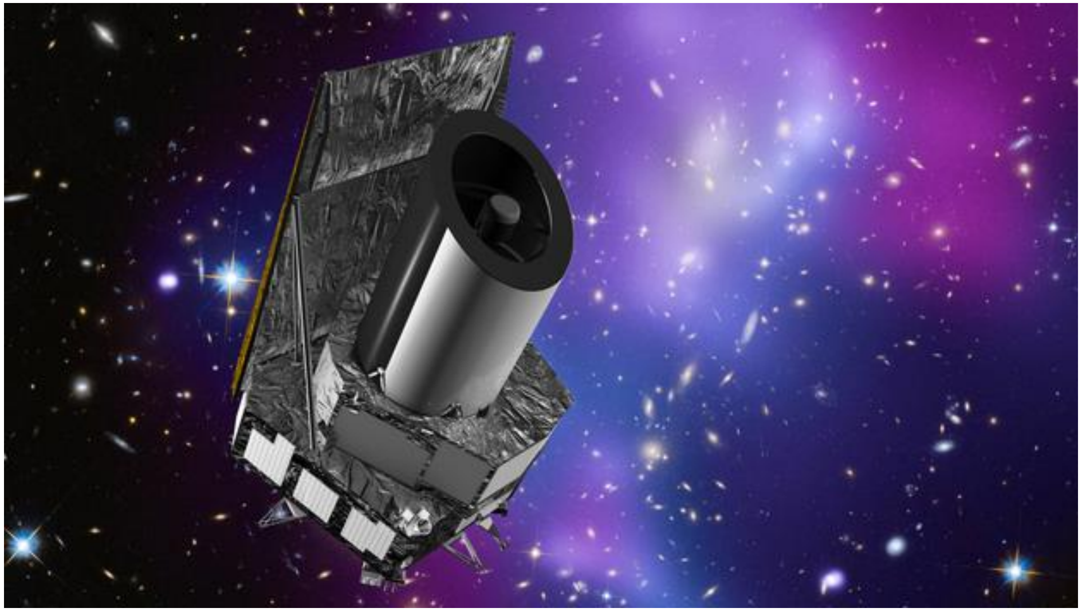
DE LA RECHERCHE À L'INDUSTRIE

DEPENDABILITY OF SPACE BORNE INSTRUMENTATION



JEAN FONTIGNIE – PA/QA MANAGER AT CEA/IRFU

www.cea.fr

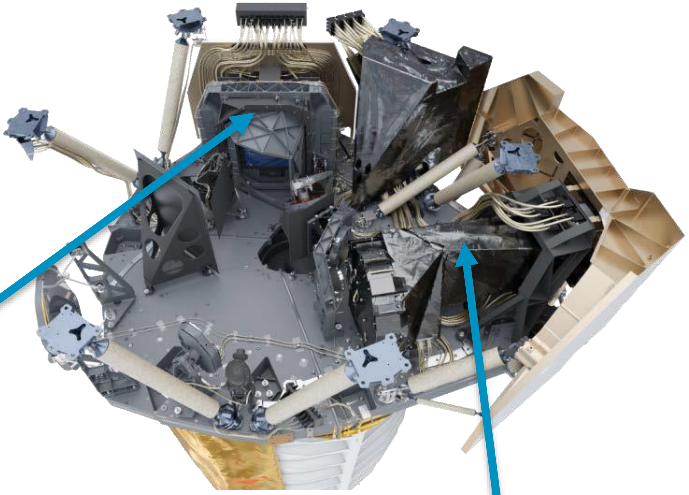
OVERVIEW OF SPACE PROJECT ORGANIZATION

- Space agency (CNES-France, ESA-Europe) : Client
- Industrial contractor (Thales Alenia, Airbus D&S)
- Consortium of research labs for instruments

Example on Euclid Mission

Thales is prime contractor

Airbus Defense & Space is in charge of telescope and payload module



VIS (photometer) : Consortium managed by MSSL (UK), with contributions from UK / France / Switzerland / Italy

NISP (spectro) : Consortium managed by LAM (Marseille), with contributions from France / Italy / Spain

COMMON REFERENCE – GOLD RULE

Complex organization, mixing different cultures

Space Agencies impose a common reference to all “contractors”

European Coordination for Space Standards (doc tree : bonus slide / www.ecss.nl)

Dependability , Electronic components procurement & Rad hardness

Material & Mechanical parts & processes procurement , Software

Rule : Each lab in charge of a “flight deliverable” identifies a “PA/QA manager” in charge of those matters + Quality Assurance

Space mission duration

- 100% ON - availability without maintenance
- > 100.000 hours

Compare to well known object

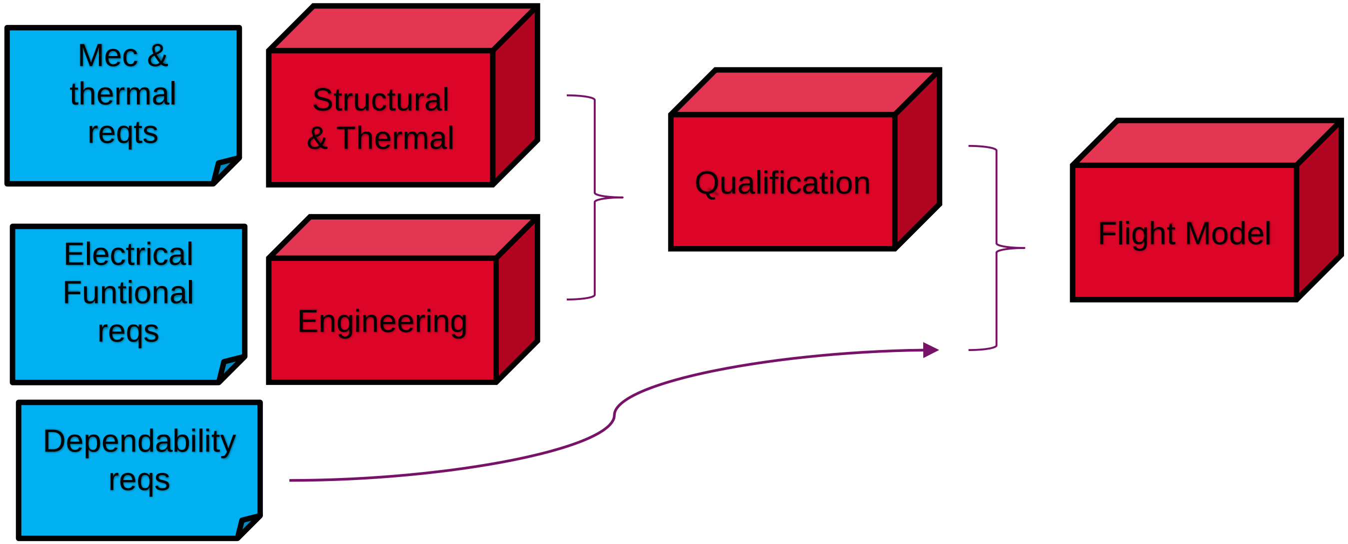
- A car : 150.000km @50km.h^{-1}
- 3000 hr with maintenance

Gold rule for space instrumentation : Schmitt axiom (lesson learnt)

- part I : What is not identified as a requirement is not verified
- part II : What is not verified, don’t expect it to work properly
- Part III : Early verification will lower failure consequence

MODEL PHILOSOPHY

Early verification needs early model/prototypes



Mec & thermal reqts

Structural & Thermal

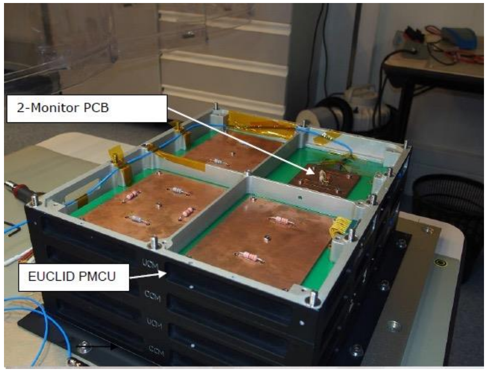
Electrical Funtional reqs

Engineering

Dependability reqs

Qualification

Flight Model



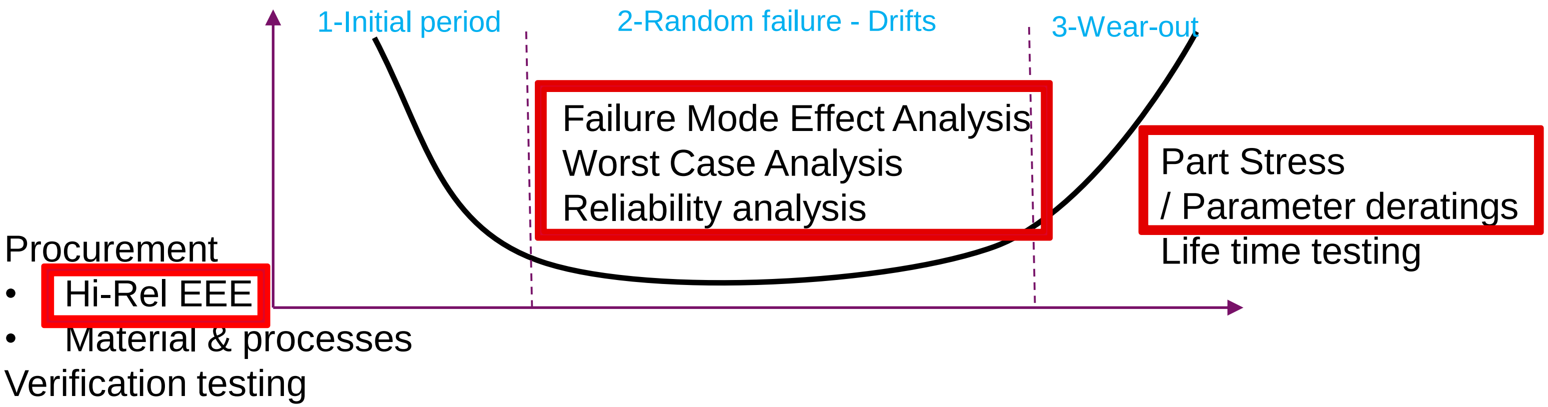
STM

QM

DEPENDABILITY ACTIVITIES

Dependability requirements :

- Implemented on the flight model
- Anticipated since the early model / studies
- Verified through all the program
- Concern all phase of mission



1-Initial period

2-Random failure - Drifts

3-Wear-out

Failure Mode Effect Analysis
Worst Case Analysis
Reliability analysis

Part Stress
/ Parameter deratings
Life time testing

Procurement
- Hi-Rel EEE
- Material & processes

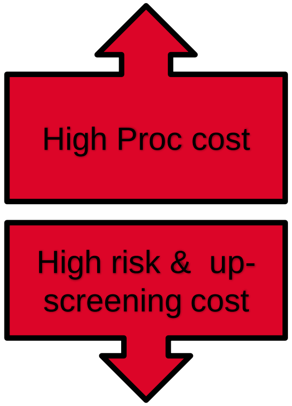
Verification testing

HIREL EEE PROCUREMENT

Quasi exclusive use of space qualified HiRel components

- Procurement spec
  [min-max] for critical parameters
  Test conditions for verification of parameters & frequency
- Adding Target for failure rates -> Quality level

Passive components	**Active components**
ESA SCC – MIL S	ESA SCC MIL QML V / JAN S
MIL R	MIL QML Q / JANTXV
MIL P - Automotive	MIL 883B
Commercial	Commercial


High Proc cost

High risk & up-screening cost

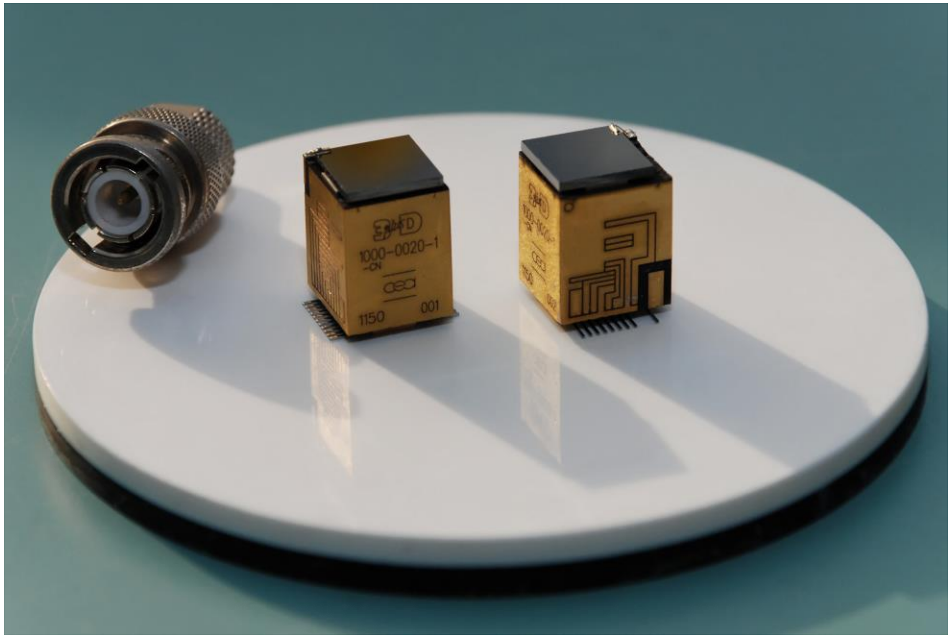
- Up-screening : procurement with lower Q level + testing
- For high volume, up-screening may be competitive
- High proc cost (passive 5€ to 100€; op amp 500€ ; FPGA 15 k€)
- Limited access to recent / high perfo EEE

EEE – CASE STUDY OF UP-SCREENING

Very integrated Hi-Energy particle detector

Need for a internal filtering capacitor

Volume/capacitance constraint



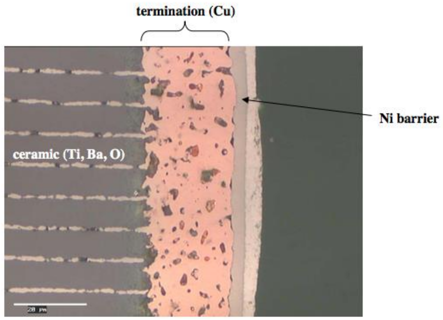
Decision :
Study possibility of up-screening of an "automotive" ceramic capacitor (6.3V 10µF 0805)

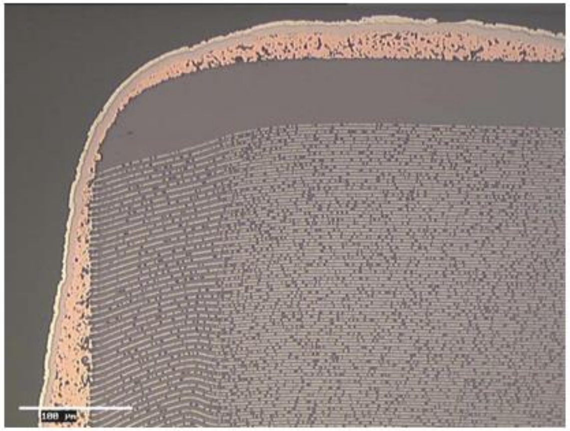
EEE - EXAMPLE OF UP-SCREENING

Procurement of a single batch

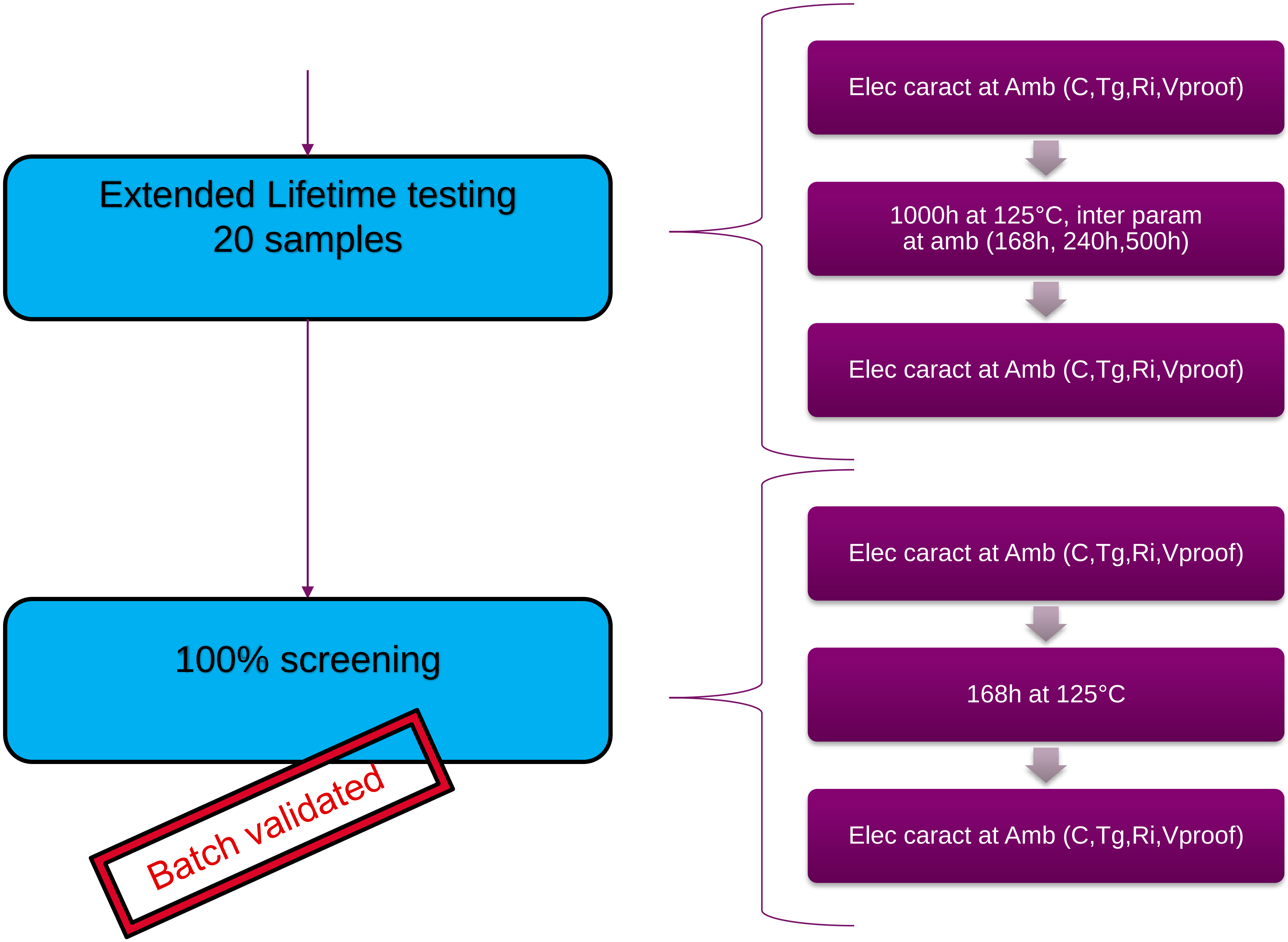
Destructive part analysis
(2 samples)

SERMA TECHNOLOGIES





EEE – EXAMPLE OF UP-SCREENING



Extended Lifetime testing
20 samples

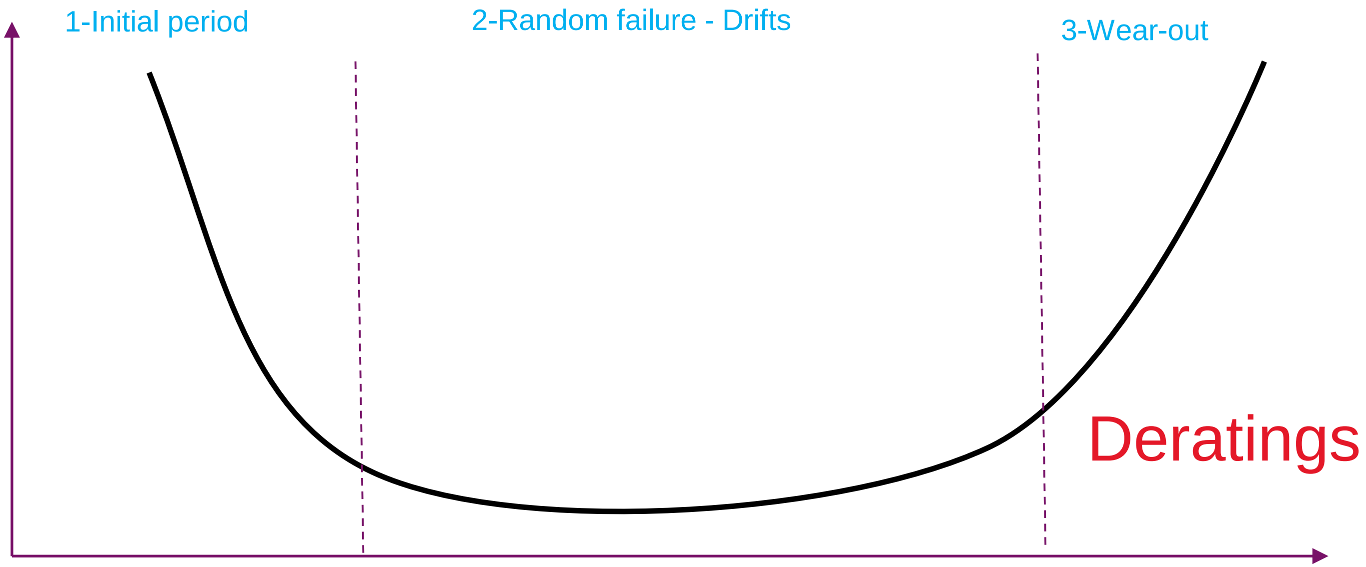
- Elec caract at Amb (C,Tg,Ri,Vproof)
- 1000h at 125°C, inter param at amb (168h, 240h,500h)
- Elec caract at Amb (C,Tg,Ri,Vproof)

100% screening

- Elec caract at Amb (C,Tg,Ri,Vproof)
- 168h at 125°C
- Elec caract at Amb (C,Tg,Ri,Vproof)

Batch validated

PART STRESS - DERATINGS

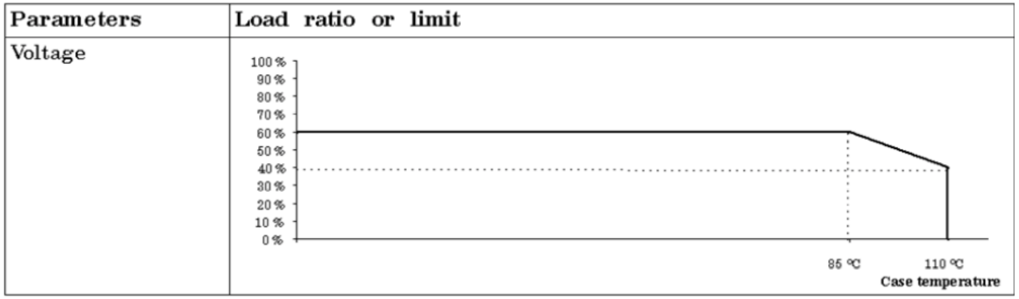


How can I defer the wear-out zone of components?

PART STRESS – DERATINGS REQUIREMENTS

Any EEE component shall show margin between operating conditions and max ratings established by manufacturer (NON NEGOCIABLE)
Margin detailed for each family (ref ECSS-Q-ST-30-11C)
Applies to all modes, in standard conditions (not in fault conditions), steady & surge

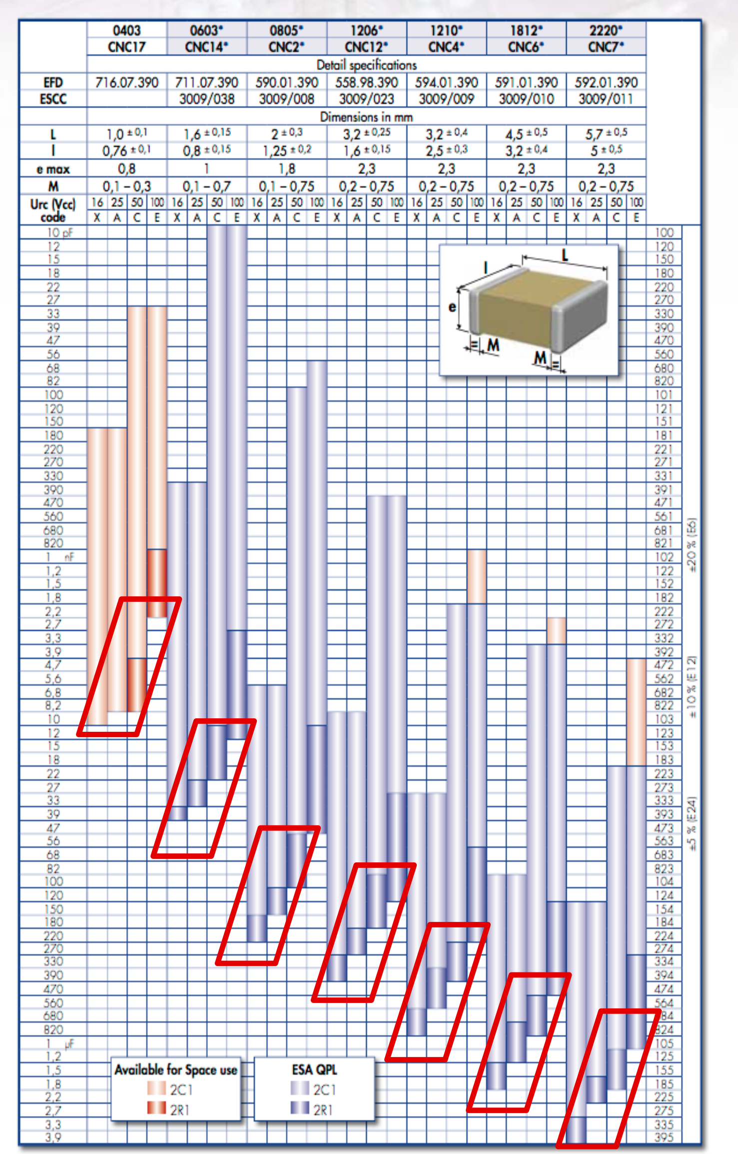
Example : Solid tantalum capacitors



Parameters	Load ratio or limit
Voltage	

Requirement
The capacitor stress sum value of steady-state voltage, AC voltage shall not exceed the load ratios specified
Surge current shall be derated to 75 % of the Isurge max. Isurge max is defined as Vrated/(ESR+Rs). 100 % surge current screening shall be applied for all surface mounted capacitors types.
Reverse voltage shall not exceed 75 % of the manufacturer’s specified maximum value for the reverse voltage.
The dV/dt rating capability of the capacitors shall be respected

PART STRESS – 2ND KIND



	0403 CNC17	0603* CNC14*	0805* CNC2*	1206* CNC12*	1210* CNC4*	1812* CNC6*	2220* CNC7*
	Detail specifications						
EFD	716.07.390	711.07.390	590.01.390	558.98.390	594.01.390	591.01.390	592.01.390
ESCC		3009/038	3009/008	3009/023	3009/009	3009/010	3009/011
	Dimensions in mm						
L	1,0 ± 0,1	1,6 ± 0,15	2 ± 0,3	3,2 ± 0,25	3,2 ± 0,4	4,5 ± 0,5	5,7 ± 0,5
l	0,76 ± 0,1	0,8 ± 0,15	1,25 ± 0,2	1,6 ± 0,15	2,5 ± 0,3	3,2 ± 0,4	5 ± 0,5
e max	0,8	1	1,8	2,3	2,3	2,3	2,3
M	0,1 – 0,3	0,1 – 0,7	0,1 – 0,75	0,2 – 0,75	0,2 – 0,75	0,2 – 0,75	0,2 – 0,75
Urc (Vcc)	16 | 25 | 50 | 100	16 | 25 | 50 | 100	16 | 25 | 50 | 100	16 | 25 | 50 | 100	16 | 25 | 50 | 100	16 | 25 | 50 | 100	16 | 25 | 50 | 100
code	X | A | C | E	X | A | C | E	X | A | C | E	X | A | C | E	X | A | C | E	X | A | C | E	X | A | C | E

Available for Space use
🟧 2C1
🟥 2R1

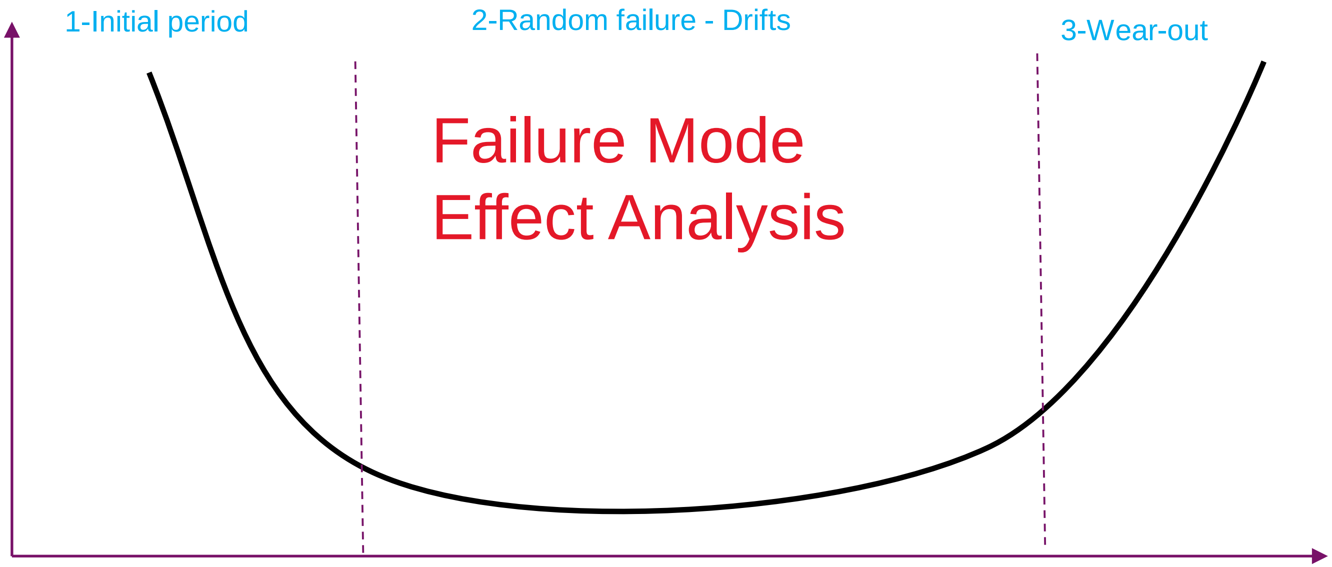
ESA QPL
🟪 2C1
🟦 2R1

2ND Deratings applied (not required by a ”standard”), “in house practice”.

For passive components, as far as possible, we do not choose extreme value within a package

Problem most often occurs on those extreme areas (limit of technology / construction)

FMEA - FMECA



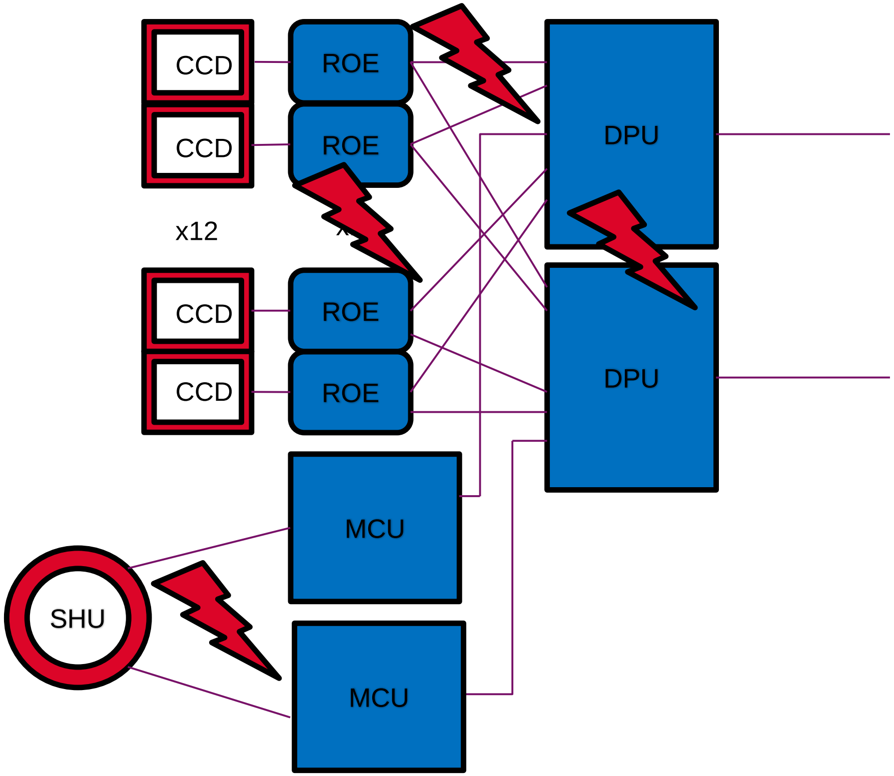
Failure Mode
Effect Analysis

Failure will occur, OK. But can the instrument survive?

FMEA – FAILURE TOLERANCE REQUIREMENTS

Failure tolerance is present in requirements (linked to space operations)

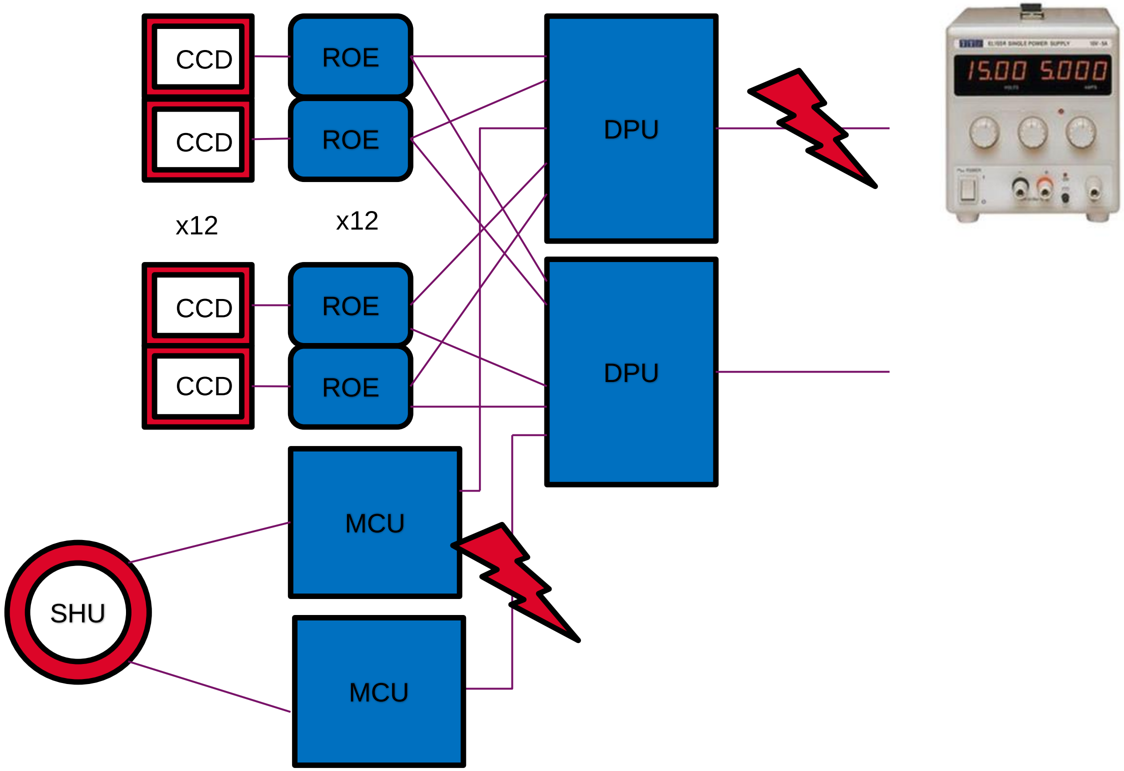
- No SPF (Single Point Failure) shall lead to mission loss (Consequence)
- No possible failure propagation between redounded units
- No possible failure propagation through cross-strapped IF
- Provide Housekeepings to allow ground diagnostic & on board FDIR



FMEA - FMECA

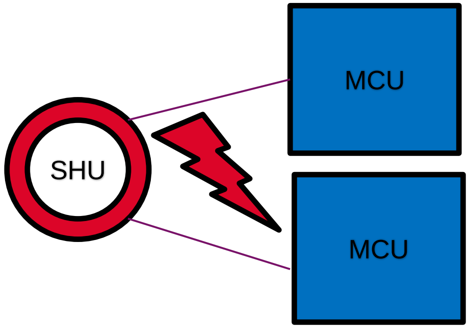
Others – Lesson learnt – ground activities – failure segregation

- No possible failure propagation between units
- No possible failure propagation from test equipment to flight equipment
- Electronic board shall survive to an unintended loss of power (complete or partial eg +5V/+12V/-12V)
- ”Power interface” shall incorporate V or I limiters



FMEA - PRELIMINARY

Early project step – preliminary design
Functional FMEA : identification of critical areas



Function	Failure mode	Effect	Rank	Detection	Recovery	Reco

FMEA – LAST COMMENTS

Some SPF are withdrawn through simple reco’s
(see bonus slide for example component level FMEA on SHU power amplifier)

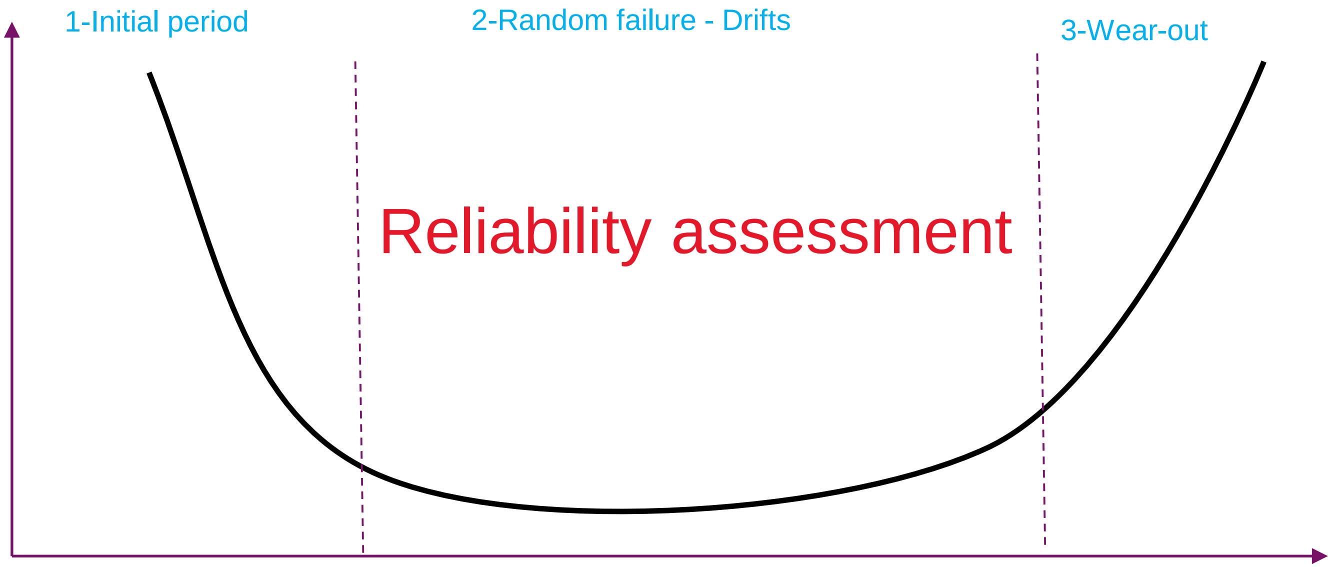
Some Single Point Failure remain
purpose of FMEA is to identify remaining SPFs
and make associated risk accepted at mission level

For each subsystem : the Interface Control Document should identify maximum ratings on it’s interfaces (not only operating conditions)

Some requirements are not accessible to verification through analysis
->Test on prototype / Early model

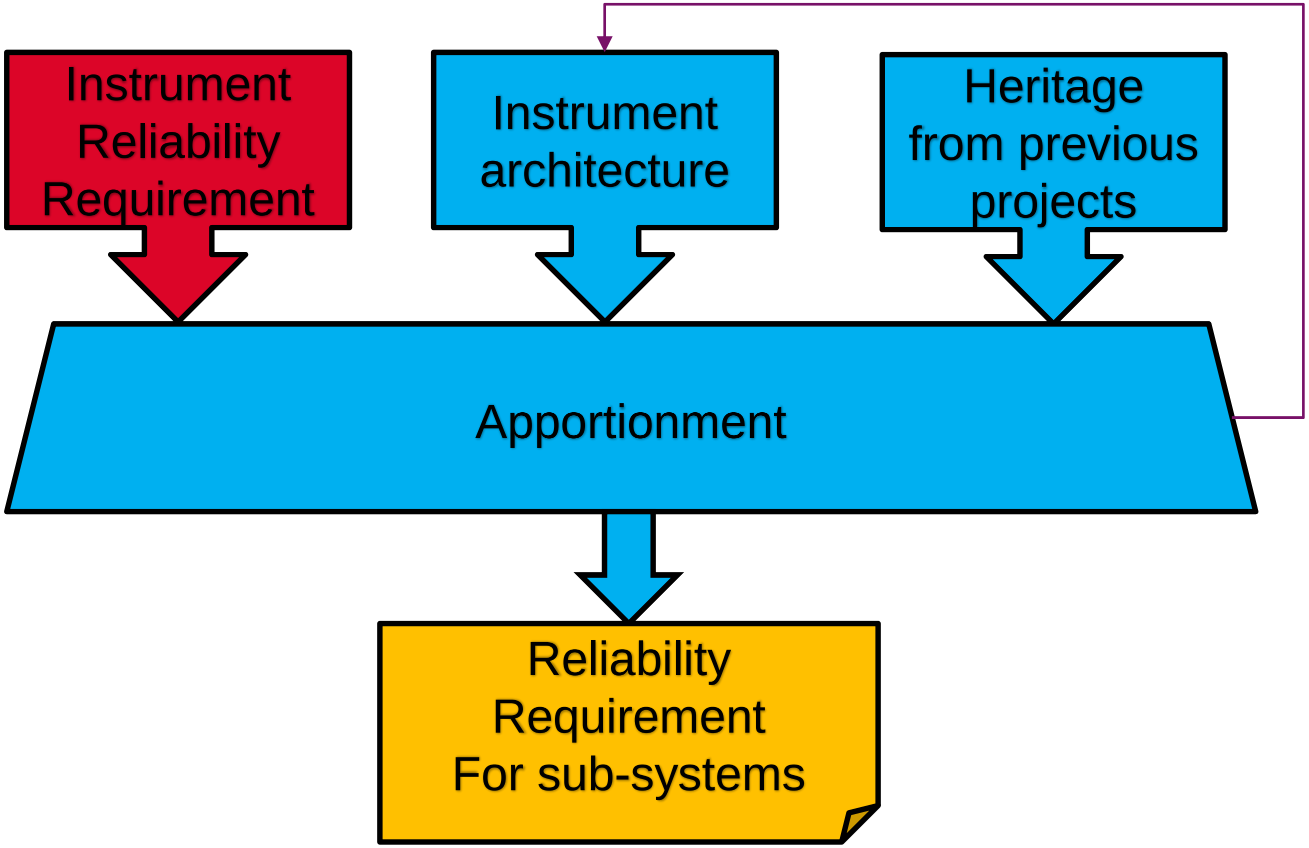
Example : “Electronic board shall survive to an unintended loss of power (complete or partial +5V/+12V/-12V)”

RELIABILITY ASSESSMENT



Failure will randomly occur, OK. But how often?

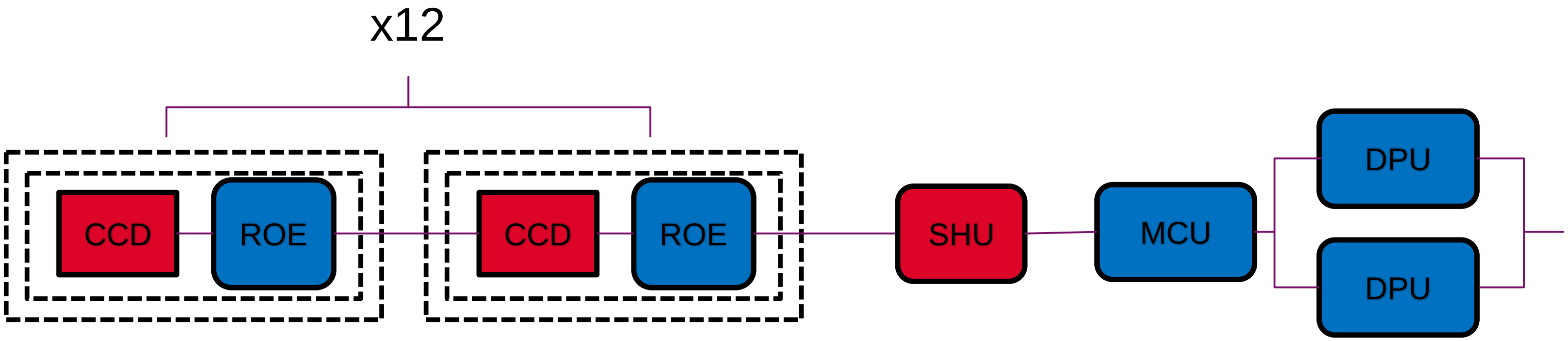
Reliability apportionment – Early project phase



Purpose : check adequacy of instrument architecture / reliability targets

RELIABILITY DIAGRAM

Target : Mission 6.25y, R=0,92
Subsystems failure rate in FITs (λ failure / 10^9h)
Reliability over period t : R=Exp(- λ.t)



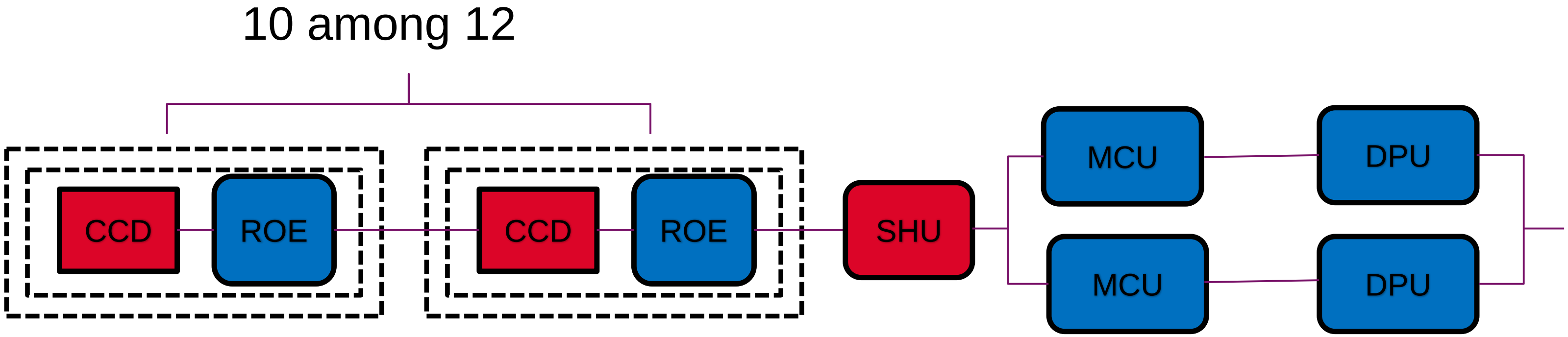
Instrument reliability $R= \prod R_{subsyst}$ = 0.581 (see bonus slide for details)

Any possible science in degraded mode (10 or 11 ROE-CCD blocks)?
R(11 blocks) = 0,857 / R(10 blocks) = 0,931

Cold redundancy for PMCU?
R(11 blocks) = 0,904 R(10 blocks)=0,982

OUTCOME OF RELIABILITY APPORTIONMENT

Updated architecture / operation scenario of instrument



Requirement document of subsystem :

- MCU : cold redundancy, <1000 FITs,
- no cross-strapping on DPU-MCU
- DPU : cold redundancy, < 1500 FITs
- ROE : < 800 FITs
- Cross strapping ROE_DPU
  + change on mission scenario (less minimum active surface end of life)

RELIABILITY ASSESSMENT – DETAILED DESIGN

Verification of compliance to reliability targets

Summing λ of EEE parts when design stable

EEE part λ estimation

- MIL-HDBK-217F reliability handbook (preferred)

- Alternative IEC-TR-6230, FIDES

- Example of using MIL-HDBK-217F -> see bonus slide
- Use of dedicated commercial tools or spreadsheets

- For complex / recent EEE, MIL-HDBK gives too high λ
- Eg FPGA ACTEL RTAX2000 : $\lambda_{die} > 1000$ Fits
- Use of extended life time testing data to predict reliability over mission and
- See example in bonus slide : $\lambda_{die} = 7$ Fits

PART STRESS - DERATINGS

Some components will have some drifts. Is the instrument tolerant?

WORST CASE ANALYSIS

Phenomenon

a) Random caracteristics of components inside the [min-max] range of the proc spec
b) Drifts will occur along the mission with ageing & radiation.

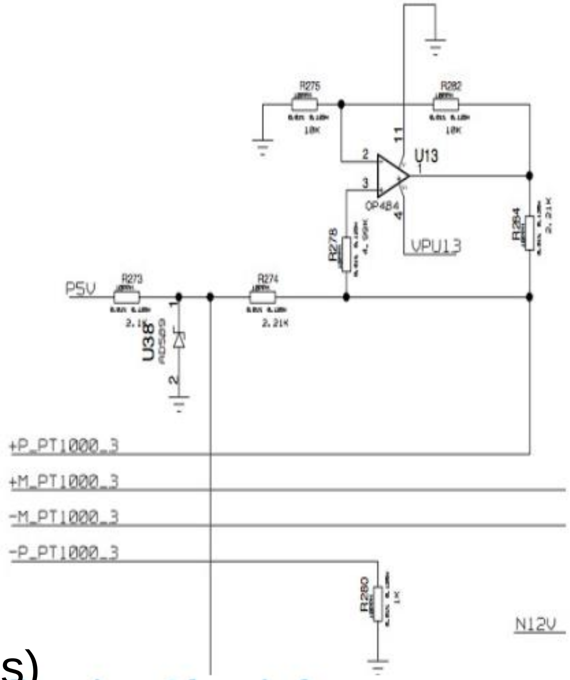
Cumulation of those phenomenon may bring instrument out of performance requirement
Impact of a) will be detected during ground testing (but schmitt part iii)
Impact of b) is only accessible to analysis (WCA)

Worst Case Analysis performed on focused area only
(decision from design engineer / Dependability engineer)
Criteria : critical function, long chain

WORST CASE ANALYSIS – CASE STUDY

Method

- identify function/area : temperature probe bias
- Identify awaited min perfo : 0.5% accuracy
- Identify components and key parameters



Component	parameter
U13 op amp	Vos, Ib, Ios
U38 volt ref	Vo
Res	R

- For each paramater identify
  - ➢ Min-Max in procurement spec
  - ➢ Drifts due to radiation (radiation test reports)
  - ➢ Drifts due to ageing

For ageing : drifts from accelerated life test & Acc factor
Acceleration factor = arrhénius law (125° C -> T op)
+ linear dependance to time

WORST CASE ANALYSIS – CASE STUDY

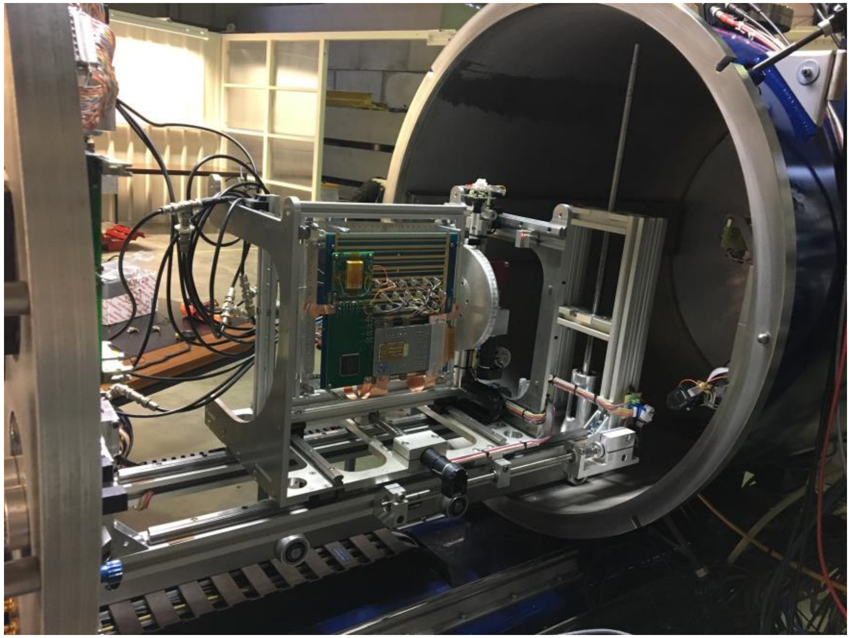
- Drifts for operational amplifier

Op amp	**initial**	**Radiation**	**Ageing**
Vos	+/- 150µV	--	1µV
Ib	3nA	20nA	30pA
Ios	1nA	5nA	--

- Designer : provide a model (spreadsheet) of circuit perfo from key parameters & drifts
- Model used to predict mission drifts
  - Nominal 550µA
  - Initial +/- 11µA
  - Ageing & radiation +/- 0.2µA
- Initial drift out of 0.5% accuracy but compensated (calibration)
- Mission drift within specification

End

Space instrumentation community is a user of accelerator test facilities (calibration of instruments, radiation testing of EEE)



Single Event Latch-up
/ Heavy Ions testing
On a space detector IC
@ Louvain - Belgium

We encourage accelerator community to continue their effort on reliability / dependability

Further question & clarification
jean.fontignie@cea.fr

Bonus slide - Material & process procurement

Materials / Mechanical parts :

- Known behaviour in launch & space environment through expereince & database
- Procured through procurement specification (either int’ standard or dedicated)

Processes : special focus on

- Gluing, Surface treatment

  Process documented (controlled through a procedure)

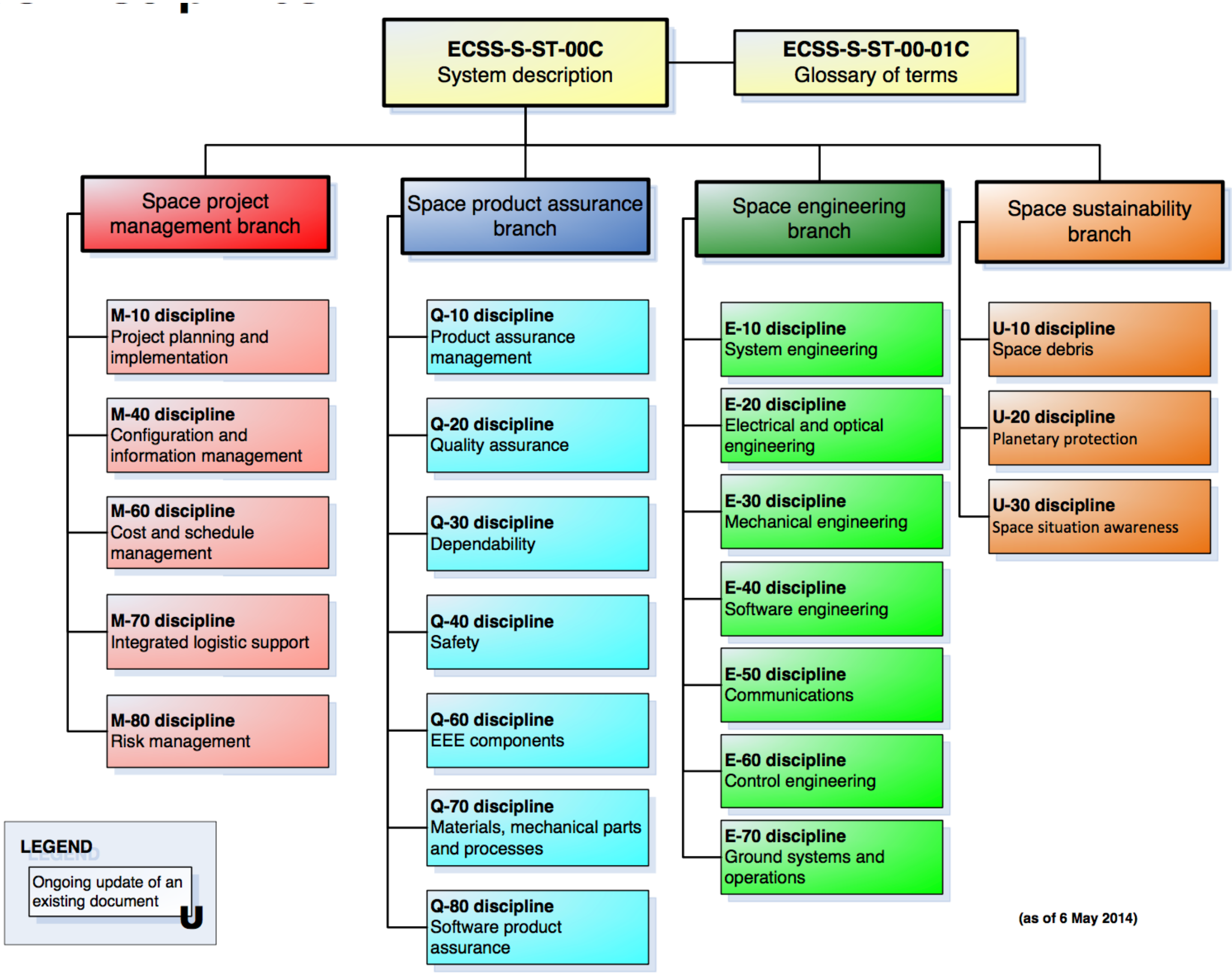
  characteristics (mechanical or optical) verified after exposition to stress (thermal cycling / thermal shock)
- Electronic assembly processes

  HiRel / Hicost components need HiRel PCB & HiRel process for assembly on PCB (and HiRel PCBs)

  Verification of process through testing on samples (PCB + components)

  100% inspection, Agreed & documented success criteria

Bonus slide – ECSS stanbdards doc tree



ECSS-S-ST-00C
System description

ECSS-S-ST-00-01C
Glossary of terms

Space project management branch

- **M-10 discipline** Project planning and implementation
- **M-40 discipline** Configuration and information management
- **M-60 discipline** Cost and schedule management
- **M-70 discipline** Integrated logistic support
- **M-80 discipline** Risk management

Space product assurance branch

- **Q-10 discipline** Product assurance management
- **Q-20 discipline** Quality assurance
- **Q-30 discipline** Dependability
- **Q-40 discipline** Safety
- **Q-60 discipline** EEE components
- **Q-70 discipline** Materials, mechanical parts and processes
- **Q-80 discipline** Software product assurance

Space engineering branch

- **E-10 discipline** System engineering
- **E-20 discipline** Electrical and optical engineering
- **E-30 discipline** Mechanical engineering
- **E-40 discipline** Software engineering
- **E-50 discipline** Communications
- **E-60 discipline** Control engineering
- **E-70 discipline** Ground systems and operations

Space sustainability branch

- **U-10 discipline** Space debris
- **U-20 discipline** Planetary protection
- **U-30 discipline** Space situation awareness

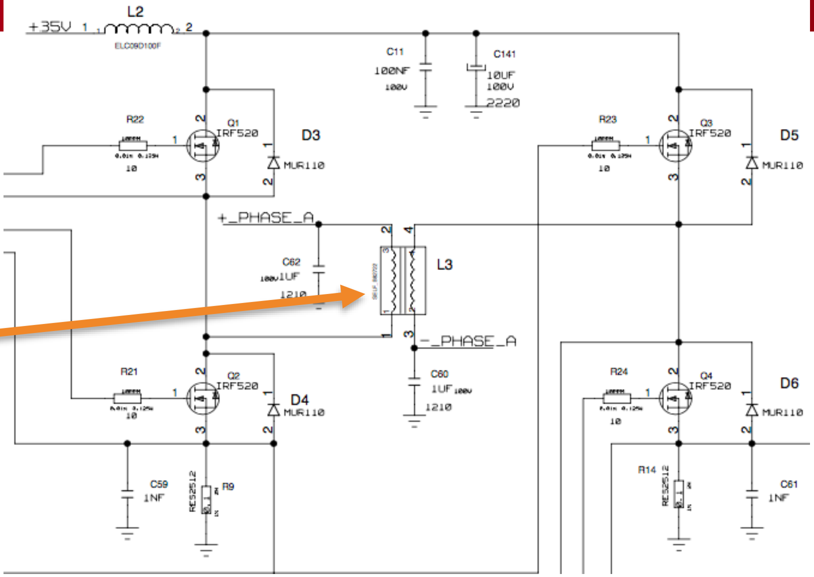
LEGEND

Ongoing update of an existing document **U**

(as of 6 May 2014)

FMEA - DETAILED

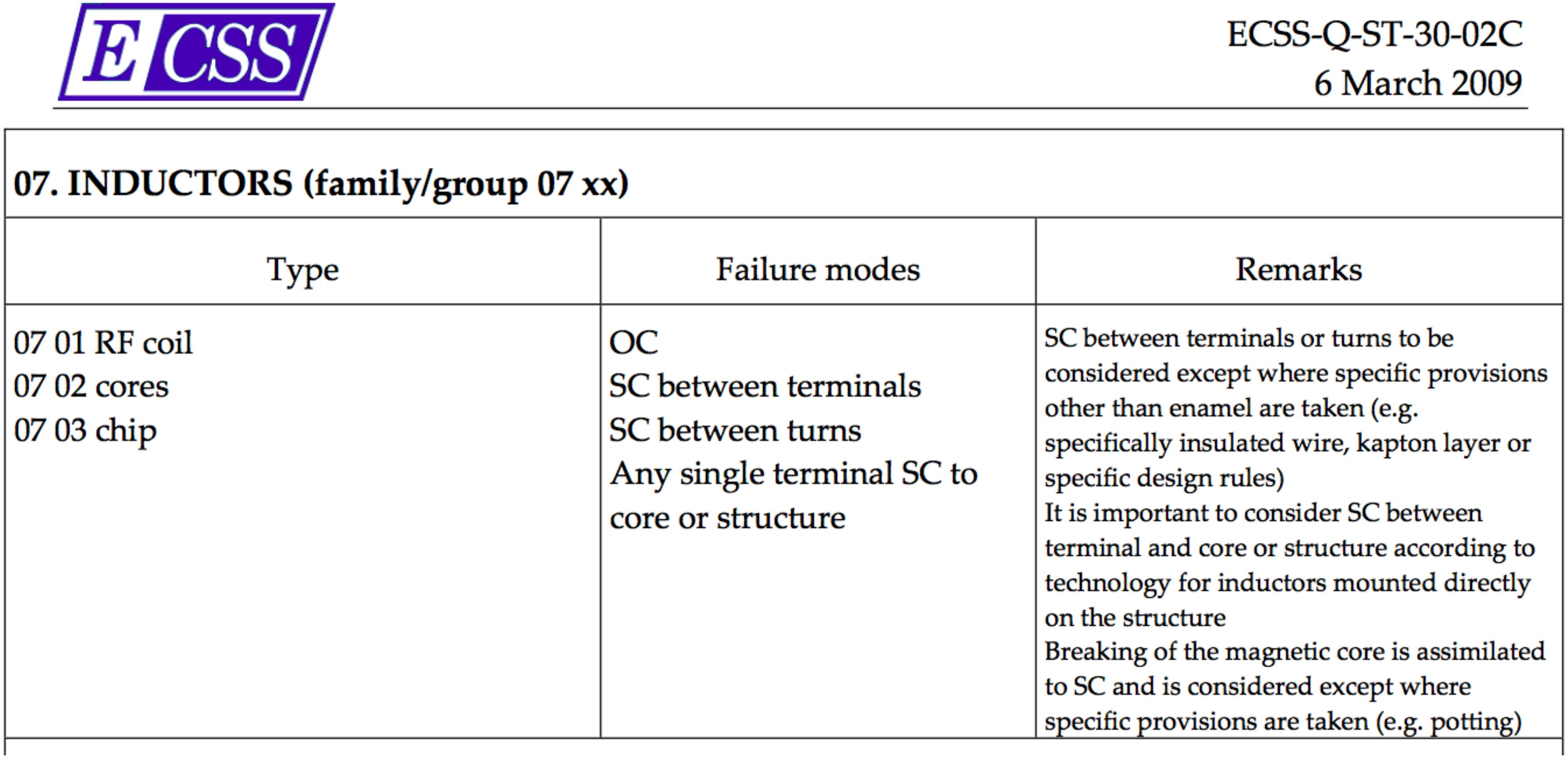
Later project step – detailed design
Update functional FMEA
+ Component level FMEA on critical areas
(See bonus slide for EEE failures)



L3

Component	Failure mode	Effect	Rank	Detection	Recovery	Reco
L3	Short Circuit (On mode)	Short circuit of Pha/PhB, no current in stepper motror	1S	PhaseA/B current HK	Switch to redundant may be inefficient	Change from common mode filter to standard coils
	Short circuit (Off mode)	Current loop in L3 Loss of SHU torque	1S	Loss of steps, wrong end position	Switch to redundant to redundant inefficient	Change from common mode filter to standard coils

FMEA – FAILURES MODE OF COILS



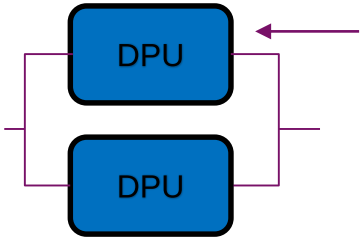
ECSS-Q-ST-30-02C
6 March 2009

07. INDUCTORS (family/group 07 xx)

Type	Failure modes	Remarks
07 01 RF coil 07 02 cores 07 03 chip	OC SC between terminals SC between turns Any single terminal SC to core or structure	SC between terminals or turns to be considered except where specific provisions other than enamel are taken (e.g. specifically insulated wire, kapton layer or specific design rules) It is important to consider SC between terminal and core or structure according to technology for inductors mounted directly on the structure Breaking of the magnetic core is assimilated to SC and is considered except where specific provisions are taken (e.g. potting)

Bonus slide – Reliability Formula

Cold redundancy



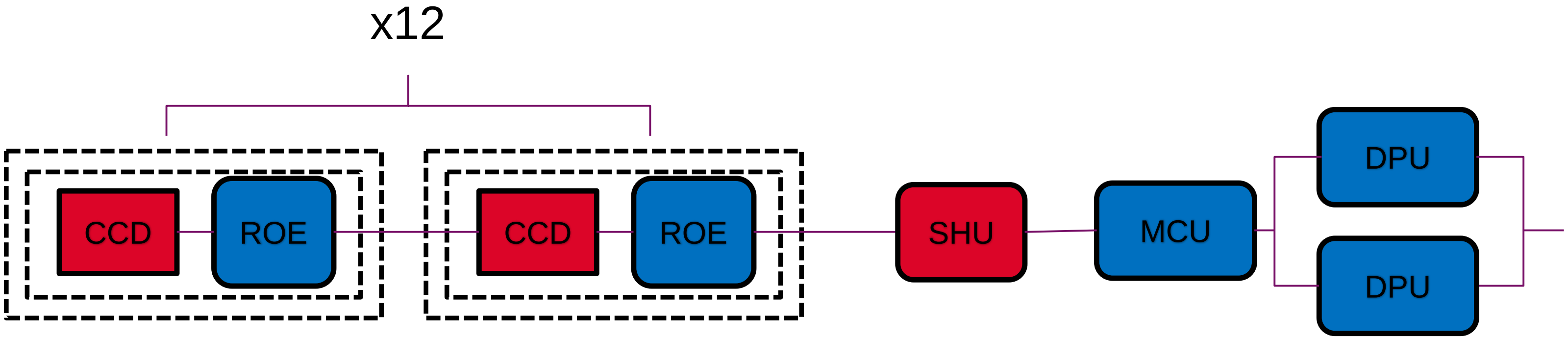
Failure rate = λ

$R(t) = e^{-\lambda t} \,.\, [1+10.(1-e^{-\lambda t/10})]$, Assuming $\lambda_{off} = \lambda_{on}/10$

Hot redundancy (10 among 12)

$R(t) =$ $e^{-12\,\lambda\,t}$. -> 12 are OK
$+12\, e^{-11\,\lambda t}\ (1-e^{-\lambda t})$ -> 11 are OK, 1 has failed
$+\ 66\, e^{-10\,\lambda t}\ (1-e^{-\lambda t})2$ -> 10 are OK, 1 has failed

RELIABILITY ESTIMATION -DETAIL



	CCD	ROE	SHU	MCU	DPU
Failure rate	0 FITS	800 FITS	0 FITS	1000 FITS	1500 FITS
Reliability		0,591 (12 ROE)		0,947	0,921 0,996

Cold redundancy

Instrument reliability $R= \prod R_{subsyst} = 0.581$

RELIABILITY FEED BACK LOOP

Weakest element CCD-ROE

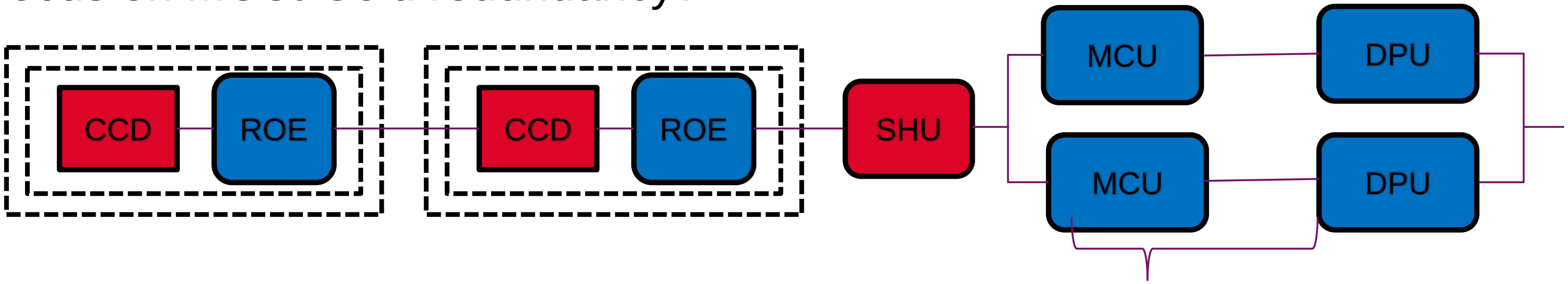
a) Enhance ROE reliability? Would need lower than 150 FITs!

b) any possible science with 10 or 11 CCD-ROE (degraded mode)?

(see bonus slide for reliability formula of ”n among m”)

	CCD	ROE	SHU	MCU	DPU	Instrument
Failure rate	0 FITS	800 FITS	0 FITS	1000 FITS	1500 FITS	
Reliability		0,591		0,947	0,996	0,558
11 CCD-ROE		0,909		0,947	0,996	0,857
10 CCD-ROE		0,987		0,947	0,996	0,931

Focus on MCU. Cold redundancy?



11 CCD-ROE		0,909			0,991	0,904
10 CCD-ROE		0,987			0,991	0,982

RELIABILITY ASSESSMENT – DETAILED DESIGN

Verification of compliance to reliability targets

Summing λ of EEE parts when design stable

EEE part λ estimation

- MIL-HDBK-217F reliability handbook (preferred)

- Alternative IEC-TR-6230, FIDES

- Example Ceramic capacitor

$$\lambda_p = \lambda_b\, \pi_t\, \pi_c\, \pi_v\, \pi_{sr}\, \pi_q \pi_e$$

symbol	contrib	Value/formula
λ_b	Intrinsic	0.00099
π_t	Temp	Arrhenius, Ea = 0.35
π_c	Cap value	(Cap Value)$^{0.23}$
π_v	Voltage	(Op volt. / 0.6 Max volt.)^{3} +1
π_q	Q level	0.001 to 1.5 -> 0.01
π_e	Environ^{t}	0.5 to 40 -> 0.5 (Space)

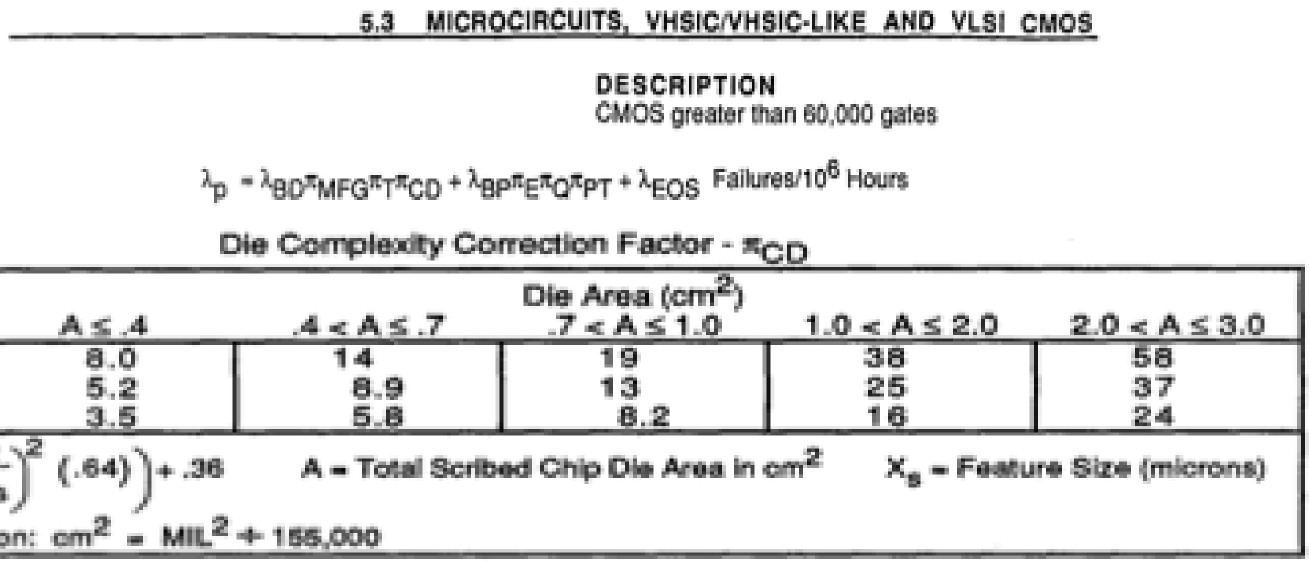
$$\pi_T = \exp\left(\frac{-Ea}{8.617 \times 10^{-5}}\left(\frac{1}{T + 273} - \frac{1}{298}\right)\right)$$

- Use of dedicated tools or spreadsheets

Reliability assessment – complex EEE

Complex EEE would need to extrapolate beyond limits of MIL-HDBK

ACTEL RTAX2000 Rad tolerant FPGA 250Kgates, 0.15µm techno, Die 2.25cm^2



5.3 MICROCIRCUITS, VHSIC/VHSIC-LIKE AND VLSI CMOS

DESCRIPTION
CMOS greater than 60,000 gates

$\lambda_p = \lambda_{BD}\pi_{MFG}\pi_T\pi_{CD} + \lambda_{BP}\pi_E\pi_Q\pi_{PT} + \lambda_{EOS}$ Failures/10^6 Hours

Die Complexity Correction Factor - π_{CD}

Feature Size (Microns)	Die Area (cm^2) A ≤ .4	.4 < A ≤ .7	.7 < A ≤ 1.0	1.0 < A ≤ 2.0	2.0 < A ≤ 3.0
.80	8.0	14	19	38	58
1.00	5.2	8.9	13	25	37
1.25	3.5	5.8	8.2	16	24

$\pi_{CD} = \left(\left(\frac{A}{.21}\right)\left(\frac{2}{X_s}\right)^2(.64)\right) + .36$ A = Total Scribed Chip Die Area in cm^2 X_s = Feature Size (microns)

Die Area Conversion: cm^2 = MIL^2 ÷ 155,000

Using such formula would lead to

$$\lambda p > \ 10^3\ FITs$$

Reliability assessment – (too) complex EEE

Use of field reliability data for die (Hi-Rel components manufacturer release them)
Use of MIL-HDBK for package
Based on extended lifetime testing data performed on any component batch

$$\lambda = \frac{\chi^2}{2.Af.Device\ Hours}$$

Chi-square at 60% level confidence level
2f+2 degrees of freedom (f number of failure)
Device hours : number of tested devices tested x duration of lifetime testing
AF : acceleration factor
(Arrhenius with Ea=0.7, 125° C test)

$$\lambda_{die} = 7\ FITs$$