ESA UNCLASSIFIED – Releasable to the Public

esa estec

Keplerlaan 1
2201 AZ Noordwijk
The Netherlands

TECHNICAL NOTE

Guidelines for the utilization of COTS components and modules in ESA

Prepared by	**COTS topic 11 WG** **ESA**
Reference	**ESA-TEC-TN-021473**
Issue/Revision	**3.0**
Date of Issue	**21/10/2024**
Status	**issued**

European Space Agency
Agence spatiale européenne

APPROVAL

Title Guidelines for the utilization of COTS components and modules in ESA	
Issue Number 3	**Revision Number** 0
Author COTS topic 11 WG	**Date** 04/07/2024
Approved By	**Date of Approval**
D. Pilz	

CHANGE LOG

Reason for change	Issue Nr.	Revision Number	Date
Issue for public release	3	0	04 July 2024
First formal issue	2	0	16 March 2022
Second draft issue	1	2	17 May 2021
First draft issue	1	1	19 February 2021
Preliminary issue	1	0	17 December 2020

CHANGE RECORD

Issue Number 3	**Revision Number** 0		
Reason for change	**Date**	**Pages**	**Paragraph(s)**
Release of public version	04/07/2024	9, 26, 33, 90, various (editorials)	3, 9, 10.5.1, annex 1, various (editorials)

DISTRIBUTION

Name/Organisational Unit

Table of contents:

1 INTRODUCTION 7
2 SCOPE 8
3 EXECUTIVE SUMMARY 9
4 ACRONYMS 14
5 DEFINITIONS 17
6 REFERENCE DOCUMENTS 21
7 REFERENCE STANDARDS 23
8 FIRST IMPORTANT REMARKS 25
9 GENERAL APPROACH TO COTS COMPONENTS AND MODULES 26
10 CRITICALITY CATEGORY Q2 29
10.1 Perimeter of application 29
10.2 RAMS 29
10.2.1 Safety 29
10.2.2 Dependability 29
10.3 Materials and processes 31
10.4 EEE components 31
10.5 Radiation 33
10.5.1 TID 33
10.5.2 TNID 33
10.5.3 SEE 34
10.6 EEE Procurement aspects 35
10.7 Application 36
10.7.1 De-rating rules 36
10.7.2 Worst case analysis 36
10.7.3 Mitigation techniques 37
10.7.3.1 Mitigation techniques at component level 37
10.7.3.1.1 General 37
10.7.3.1.2 Power discrete devices 37
10.7.3.1.3 Memories 38
10.7.3.1.4 FPGAs 39
10.7.3.1.5 Microprocessors 42
10.7.3.1.6 Microcontrollers 44
10.7.3.1.7 Programmable Systems-on-a-Chip (SoC) 46
10.7.3.2 Mitigation techniques at module/board level. 48
10.7.3.3 Mitigation techniques at system/subsystem level. 48
10.7.4 Reference application circuits 49
10.8 Modules 49
10.8.1 Data sheets 51
11 CRITICALITY CATEGORY Q1 52
11.1 Perimeter of application 52

11.2 RAMS 52
11.2.1 Safety 52
11.2.2 Dependability 52
11.3 Materials and processes 53
11.4 EEE components 54
11.5 Radiation 55
11.5.1TID and TNID 55
11.5.2 SEE 56
11.5.3 ERCB, Equipment Radiation Control Board 59
11.6 EEE Procurement aspects 60
11.7 Application 60
11.7.1Data sheets 60
11.7.2 De-rating rules 60
11.7.3 Worst case analysis 61
11.7.4 Mitigation techniques 61
11.7.4.1 Mitigation techniques at component level 61
11.7.4.1.1 General 61
11.7.4.1.2 Power discrete devices 62
11.7.4.1.3 Digital Components, general 62
11.7.4.1.4 Memories 62
11.7.4.1.5 FPGAs 63
11.7.4.1.6 Microprocessors 65
11.7.4.1.7 Microcontrollers 66
11.7.4.1.8 Programmable Systems-on-a-Chip (SoC) 67
11.7.4.2 Mitigation techniques at module/board level. 67
11.7.4.3 Mitigation techniques at system/subsystem level. 68
11.7.5 Reference application circuits 69
11.7.6 Modules 69
12 CRITICALITY CATEGORY Q0 71
12.1 Perimeter of Applications 71
12.2 RAMS 71
12.3 Materials and processes 71
12.4 EEE components 72
12.5 Radiation 72
12.6 EEE Procurement aspects 72
12.7 Application 72
12.7.1 Data sheets 72
12.7.2 De-rating rules 73
12.7.3 Worst case analysis 73
12.7.4 Mitigation techniques 73
12.7.5 Reference application circuits 74
12.7.6 Modules 74

13 HOW TO ATTRIBUTE CRITICALITY CATEGORY 75
13.1 Responsibilities 82
13.2 How to attribute criticality category, flow chart 83
14 GUIDELINES FOR EVALUATING LOT HOMOGENEITY 84
14.1 General 84
14.2 Radiation 84
15 FEEDBACK FROM SPACE APPLICATION 85
16 REVIEWS OF ITEMS CONTAINING COTS EEE COMPONENTS AND MODULES IN CATEGORY Q1 AND Q2 86
17 THE CONCEPT OF SAFETY BARRIER FOR EQUIPMENT OF HIGHER CRITICALITY CLASS 87
ANNEX 1, RECOMMENDED APPLICATION BOUNDARIES OF CRITICALITY CATEGORIES 89
ANNEX 2, RADIATION MITIGATION TECHNIQUES 90
A2.1 Potentially radiation sensitive EEE components 90
Table A2-1: EEE component families potentially sensitive to TID 90
Table A2-2: List of EEE component families potentially sensitive to TNID 91
Table A2-3: List of EEE component families potentially sensitive to SEE 92
A2.2 Generic radiation mitigation techniques, TID 93
A2.3 Generic radiation mitigation techniques, TNID 95
A2.4 Generic radiation mitigation techniques, SEE 96
A2.4.2.1.1 Spatial Redundancy Mitigation Techniques 98
A2.4.2.1.2 Temporal redundancy mitigation techniques 101
A2.4.2.2.1 Error Correcting Codes (ECC) 102
A2.4.2.2.2 Overview of ECC types 102
A2.4.2.3 SEE Mitigation per Memory Type 104
A2.4.2.4 Field Programmable Gate Arrays (FPGAs) 105
A2.4.2.4.1 SEE Mitigation for Flash-based FPGAs 107
A2.4.2.4.2 SEE Mitigation for SRAM-based FPGAs 108
A2.4.2.5 SEE Mitigation for Microprocessors 110
A2.4.2.6 SEE Mitigation Techniques for Microcontrollers 111
A2.4.2.7 SEE Mitigation Techniques for SoC FPGAs 112
A2.4.2.8 Bandgap references 113
A2.4.2.9 Operational amplifiers and comparators 113
A2.4.2.10 Microwave integrated circuits 113
A2.4.2.11 CMOS 113
A2.4.2.12 CCD, APS 113
A2.4.2.13 Opto devices 114
A2.4.2.14 MOSFET (Si NMOS and PMOS) 114
A2.4.2.15 HEMT (p-GaN and MISHEMT) 114
A2.4.2.16 Microwave transistors 114
A2.4.2.17 FET (N and P channel) 114
A2.4.2.18 Other components 114

ANNEX 3, CONSERVATIVE TID AND TNID RADIATION ENVIRONMENT MODELLING FOR Q1 AND Q2 CRITICALITY CATEGORIES 115
ANNEX 4, DETAILS ON Q2 AND Q1 RADIATION TESTS 116
ANNEX 5, RECOMMENDATIONS FOR PCBS FOR CATEGORY Q1 120
ANNEX 6, ADDITIONAL RECOMMENDATIONS FOR ASSEMBLY PROCESSES FOR Q1 AND Q0 CATEGORIES.. 122
ANNEX 7, ELECTRICAL SAFETY BARRIER EXAMPLES 126

1 INTRODUCTION

Space is becoming a more and more competitive sector, asking continuously for higher performance figures while reducing the overall cost from missions inception up to end of life decommissioning. Such a trend has consequences at all levels down to the selection and procurement of building blocks and components.

In parallel to the above-mentioned paradigm, EEE components designed for terrestrial application such as automotive and other industrial sectors show high reliability levels in the targeted applications when produced in massive quantities and while being the subject to ad-hoc qualification schemes (e.g. AEC-Q).

Although we could see a solution matching a need, there is still a big gap between space and terrestrial application of components, and proper methodologies have still to be developed and approved in order to allow a more systematic usage of Commercial Off The Shelf (COTS) components and modules for space applications.

2 SCOPE

The scope of this guideline is the following:

- *Perform the classification of the COTS component categories according to (applications) criticality categories;*
- *Identify procurement, screening, application and test methods for COTS components and modules in the different application criticality categories.*

The scope of these guidelines is limited to ESA missions only.

This document is intended as a guideline and not as a standard.

This document covers electrical, electronic and electromechanical (EEE) COTS components and modules for the space segment.

Coverage of software guidelines is not included in this document.

This document provides guidelines regarding the use of COTS components and modules in equipment, subsystem or system of defined criticality categories.

The ESA mission classification is not part of this document.

COTS components have been classified in different criticality categories.

As a first step, the criticality of the module, equipment, subsystem or system needs to be determined, which will then determine which set of guidelines should be used. The criticality classes are explained in chapter 10 (category Q_2), chapter 11 (category Q_1) and chapter 12 (category Q_0).

3 EXECUTIVE SUMMARY

The main reasons of using COTS components and modules in space are the following:

- **Performance advantage** if the performance is not obtainable by classical Hi-Rel components
- **Lack of Hi-Rel components** for performing that function
- **Availability of production capability of supply chain for terrestrial use** (in terms of modules)
- **Shorter lead times and lower risk of EEE components unavailability** (not necessarily true, depending on procurement scheme, taking into account the quick obsolescence cycle of COTS components and their limited shelf life). Also limited regulatory control might help shorter lead times.
- **Cost advantage**, only for large volumes or low reliability/low radiation application where important risks might be taken.

This document addresses the selection and use of COTS components and modules in modules, equipment, subsystems or systems of different criticality categories for ESA institutional missions.
This document contains a **set of guidelines** and not requirements.

Such criticality categories have been developed to support a rational approach for the selection of COTS, especially with regards to reliability and radiation performance.
The criticality categories are built according to a balanced scheme from higher to less risk taking, and allowing both an economic/experimental (but more risky) use of COTS for cost reduction reasons, and a reliable (but expensive) use of COTS for performance reasons.

Since ESA missions imply typically small procured lots of COTS components and modules, special care has been given to address the issue of unsure lot homogeneity, which has consequences for both reliability and radiation assurance aspects.
In fact, only with guaranteed lot homogeneity one can be sure that the test or evaluation sample is representative of the flight EEE components.

One of the major advantages to define different criticality categories for equipment or subsystem based on COTS components and modules is that on a given mission, different

criticality categories can appear, depending on the nature of the considered modules, equipment or subsystem.
For example, essential equipment for mission success can only be reasonably selected from criticality category with the lowest risk profile, while experimental or "expendable" payload might be developed from a criticality category with higher risk profile.

It is therefore important to remember that:

- the criticality categories are relevant to modules, equipment, subsystems and systems and not to the mission class;
- a mission of any class can employ modules, equipment, subsystems of any criticality categories, depending on the criticality of the considered function.

The identified criticality categories at modules, equipment or subsystem level are divided in two main groups: a **normative** ("green") area and an **informative** ("yellow") one. See Figure 1.

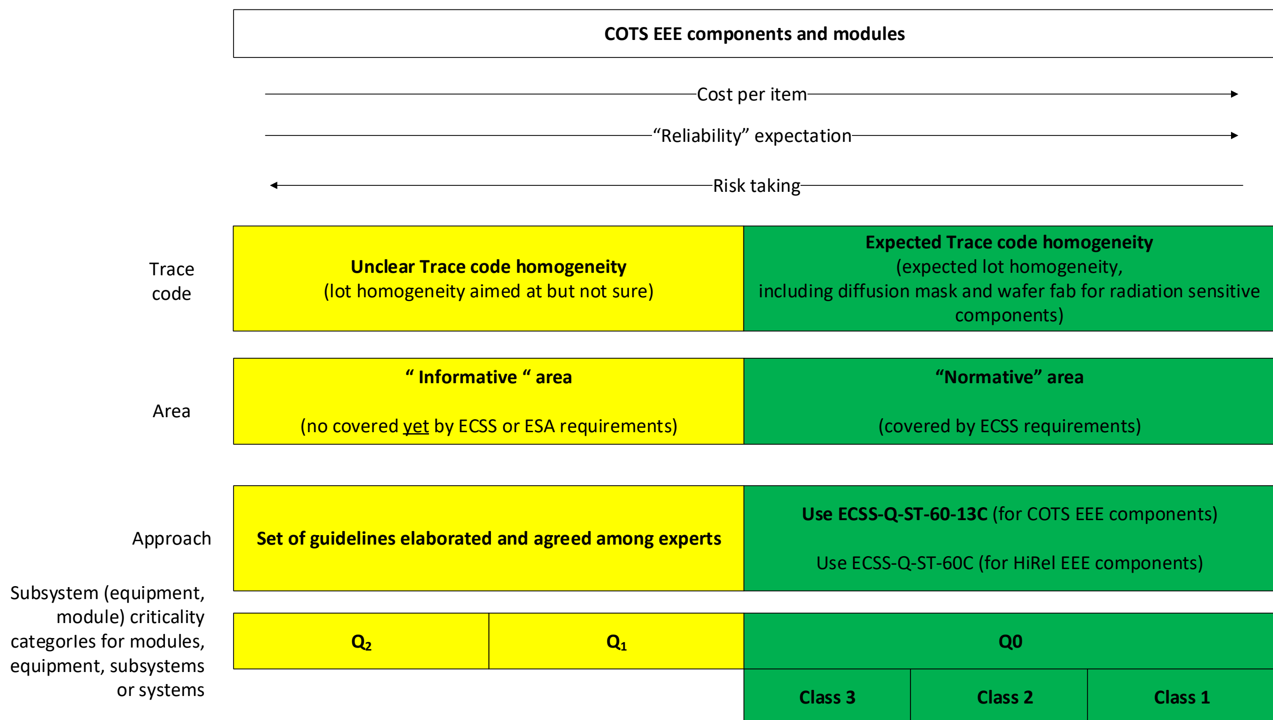


Figure 1, COTS, overall approach, versus Criticality Categories

The **normative** ("green") area addresses COTS components and modules for which all standard ECSS requirements apply, specifically for commercial components ECSS-Q-ST-

60-13 . The **relevant criticality category** is **Q_0**, and it is subdivided in three EEE components classes as shown in Figure 2.
In this case homogeneity of procurement lot is expected, making evaluation and lot acceptance activities fully representative of flight EEE components.

The **informative** ("yellow") area represents categories with lower requirements and where higher risk can be accepted.
COTS components and modules lot homogeneity is still aimed at but exceptions are still possible, in these cases tests are not guaranteed to be representative. In this case, the proposed approach identifies **two criticality categories:**

- **Q_2**, the most risky and economic;
- **Q_1,** less risky and more expensive than Q_2.

Q_2 application perimeter is defined by the following recommendations:

- The mission radiation exposure TIDL at component level should be limited to <5 krad(Si)
- The mission operational duration should be limited to few months, typically less than one year.

Q_1 application perimeter is defined by the following recommendations:

- The mission radiation environment (TIDL) limit is indicatively 10-15 krad(Si)
- The mission operational duration should be limited to few years, typically less than five years.

For both Q_2 and Q_1 **design mitigation techniques** and **reference designs** are highly recommended to minimise the failure probability especially related to radiation tolerance and random quality issues at EEE component level.

For additional details on the generic COTS approach, refer to section 9.

For more details on criticality categories, refer to section 10 (Q_2), 11 (Q_1), and 12 (Q_0).

For each criticality category the following aspects are addressed:

- *Perimeter of application (according to table in annex 1 with some more details)*

- *Recommended PA and engineering approach to*

    - *RAMS*
    - *Material and processes*

- *EEE components*
- *Radiation*
- *Procurement aspects*
- *Application, including*
  - *approaches for data sheets review*
  - *electrical analyses needs*
  - *mitigation techniques*
  - *reference application circuits*
  - *modules*

For details on how to attribute criticality categories, refer to section 13.

ECSS-Q-ST-60-13C
21 October 2013

Annex G (informative) Difference between the three classes

	CLASS 1	CLASS 2	CLASS 3
EVALUATION	COMPLETE - Construction analysis - Electrical charact. (3T+10°C margin) - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C + DPA - Precond + 500T/C -55°C/+125°C - Radiation evaluation (TID, SEE)	COMPLETE - Construction analysis - Electrical charact. (3T+10°C margin) - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C + DPA - Precond + 500T/C -55°C/+125°C - Radiation evaluation (TID, SEE)	LIMITED - Construction analysis - Radiation evaluation (TID, SEE)
JD (Justification Doc)	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and test - Lot acceptance tests - Radiation hardness data and RVT	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and test - Lot acceptance tests - Radiation hardness data and RVT DATA COLLECTED *(EFR, lifetest, thermal cycling)* used for screening reduction	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and tests - Lot acceptance tests - Radiation hardness data and RVT DATA COLLECTED *(lifetest, HAST, thermal cycling)* used for lot test reduction
CUSTOMER PRECAP	no	no	no
SCREENING	COMPLETE - X-rays - Serialisation - 10T/C -55°C/+125°C - PIND test (if applicable) - Initial electrical test @ 25°C - Dynamic burn-in 240h-125°C - Final electrical test @ 3T° - PDA (5%) - Hermeticity (if applicable) - External visual inspection	LIMITED (if data collected) - PIND test (if applicable) - Hermeticity (if applicable) + if no data collected (see JD) - Serialisation - 10T/C -55°C/+125°C - Initial electrical test @ 25°C - Dynamic burn-in 160h-125°C - Final electrical test @ 3T° - PDA (5%) - External visual inspection	LIMITED - PIND test (if applicable) - Hermeticity (if applicable)
LOT TEST (on screened parts) (when applicable)	COMPLETE - Construction analysis - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C - Precond + 100T/C -55°C/+125°C - RVT (Radiation Verification test)	COMPLETE (but LT 1000h) - Construction analysis - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 1000h-125°C - Precond + 100T/C -55°C/+125°C *(may be waived i.a.w. application)* - RVT (Radiation Verification test)	LIMITED (if data collected) - Construction analysis - RVT (Radiation Verification test) + if no data collected (see JD) - Precond + HAST 96h or THB 1000h - Lifetest 1000h-125°C - Precond + 100T/C -55°C/+125°C
CUSTOMER BUY-OFF	no (replaced by incoming)	no (replaced by incoming)	no (replaced by incoming)
INCOMING	yes	yes	yes

97

Figure 2, ECSS-Q-ST-60-13C, summary (annex G)

4 ACRONYMS

1D	One-Dimensional
2D	Two-Dimensional
AEC	Automotive Electronics Council
AEC-Q	The set of AEC automotive qualification standards
ADC	Analog to Digital Converter
ADS	Airbus Defence and Space
APS	Active Pixel Sensor
BCH	Bose-Chaudhuri codes
BiCMOS	Bipolar and CMOS
CD	Competence Domain
CDR	Critical Design Review
CoC	Certificate of Conformity
COTS	Commercial Off The Shelf (components and modules)
CPPA	Central Part Procurement Agency
CM	Clock generators/Managers
CMOS	Complementary Metal Oxide Semiconductor
CRC	Cyclic Redundancy Check
CSAM	C-Mode Scanning Acoustic Microscope
DAC	Digital to Analog Converter
DCL	Declared Components List
DD	Displacement Damage
DDC	Dose Depth Curve
DFF	D Flip Flops
DML	Declared Materials List
DMPL	Declared Materials and Processes List
DMR	Double Modular Redundancy
DPL	Declared Process List
DPA	Destructive Physical Analysis
DSP	Digital Signal Processor
DWC	Duplication with comparison
EDAC	Error Detection And Correction
ECC	Error Correcting Code
ERCB	Equipment Radiation Control Board
EPROM	Erasable Programmable Read-Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
EEE	Electrical, Electronic and Electromechanical
EPPL	European Preferred Parts List
EQSR	Equipment Qualification Status Review
FEC	Forward Error Correction

FET	Field Effect Transistor
FMECA	Failure Mode Effects and Criticality Analysis
FPGA	Field Programmable Gate Arrays
FSM	Finite State Machine
GaN	Gallium Nitride
GCR	Galactic Cosmic Rays
HALT	Highly Accelerated Life Test
HASS	Highly Accelerated Stress Screening
HCE	High Current Event
HEMT	High Electron Mobility Transistor
HW	Hardware
IPN	Internal Problem Notification
LAT	Lot Acceptance Test
LET	Linear Energy Transfer
LETth	LET threshold
LDPC	Low Density Parity Codes
MBU	Multiple Bit Upset
MISHEMT	Metal Insulator Semiconductor HEMT
MOSFET	Metal Oxide Semiconductor FET
MMIC	Microwave/Millimeter-wave Monolithic Integrated Circuit
OBC	On Board Computer
OS	Operating System
p-GaN	p-type layer gate GaN HEMT
PA	Product Assurance
PCB	Printed Circuit Board
PDR	Preliminary Design Review
PSA	Parts Stress Analysis
PWM	Pulse Width Modulation
RAMS	Reliability, Availability, Maintainability, Safety
R&D	Research and Development
RHA	Radiation Hardness Assurance
RS	Reed-Solomon
SEB	Single Event Burnout
SEC-DED	Single Error correction and Double Error Detection
SEDR	Single Effect Dielectric Rupture
SEE	Single Event Effects
SEFI	Single Event Functional Interrupt
SEGR	Single Event Gate Rupture
SEHE	Single Event Hard Error
SEL	Single Event Latch-up
SET	Single Event Transient
SEU	Single Event Upset
SIFT	Software-Implemented hardware Fault Tolerance

SoC	System on a Chip
SPF	Single Point Failure
SRAM	Static Random Access Memory
SW	Software
TAS	Thales Alenia Space
TBA	To Be Added
TBC	To Be Confirmed
TBD	To Be Defined
TDE	Technology Development Element (part of ESA budget line for generic R&D activities at low TRL)
TI EP	Texas Instrument Enhanced Plastic (components)
TID	Total Ionizing Dose
TIDL	Total Ionizing Dose Level
TIDS	Total Ionising Dose Sensitivity
TMR	Triple Modular Redundancy
TNID	Total Non Ionizing Dose
TNIDL	Total Non Ionizing Dose Level
TNIDS	Total Non Ionizing Dose Sensitivity
TRP	Technology Research Programme (obsolete ESA budget line for generic R&D activities at low TRL)
USA	United States of America
WBG	Wide Band Gap (semiconductor)
WCA	Worst Case Analysis
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (German Electrical and Electronic Manufacturers‘ Association) Electronic Components and Systems Division

5 DEFINITIONS

assembly

the act of combining components in manufacturing, or the resulting assemblage

component

set of materials, assembled according to defined and controlled processes, which cannot be disassembled without destroying its capability and which performs a simple function that can be evaluated against expected performance requirements

part

see "component"

module

assembly of interconnected EEE components

NOTE
A module can be verified independently.
Example of modules are assembled PCB, part of or full electronic unit.

board

module designating a PCB or substrate populated with components

hybrid

EEE component consisting of a substrate populated with components within a single package

NOTE
The electronic components of a hybrid are typically naked dice

COTS Components and Modules

An assembly, module or part designed for commercial applications for which the item manufacturer or vendor solely establishes and controls the specifications for performance, configuration, and reliability (including design, materials, processes, and testing) without additional requirements imposed by users and external organizations.

design mitigation (technique)

is typically a specific solution, a "trick" to address and resolve an environmental compatibility problem (usually, but not always, related to Single Event Effect – SEE-).
For example, the adoption of a RC filter after a comparator to avoid the effects of an output transient due to Single Event Transient (SET).

essential function (module, equipment, subsystem)

function without which the operator cannot recover the space vehicle (following any conceivable on-board or ground-based failure), the space vehicle cannot be commanded, the space vehicle permanently loses attitude and orbit control, the space vehicle consumables (e.g. fuel and energy) are depleted to such an extent that more than 10% of its lifetime is affected, or the safety of the crew is threatened (definition 3.2.19 according to ECSS-E-ST-20C, 31July2008, with "spacecraft" substituted with "space vehicle").

Essential functions may include means for safe passivation of the space vehicle (if passivation is required).

Essential item is intended considering the possible redundancies at space segment level (for example, a receiver equipment is essential for a mission with a single spacecraft, but it might be not essential for a constellation where the redundancy is at spacecraft level).

non Essential function (module, equipment, subsystem)

Contrary to essential function.

heritage

In the context of this document, heritage has to be considered in a wider meaning than is normally applied.
At EEE component level (COTS) it identifies EEE components that have been used in the past but for which in general there is no guarantee of performance in the future if trace code (plus diffusion lot and wafer fab) is not the same as the one used in the past.
At COTS module level, heritage identifies modules that have successfully been used in the past for space applications, but it does not guarantee per se success for future space applications if modules

cannot be demonstrated to have homogeneous performances including radiation in equivalent environmental conditions.
Heritage can also be referred to application circuits for a generic or specific part numbers, providing effective and documented mitigation techniques against for example radiation effects.

date code

code used by the EEE part manufacturer at assembly step that indicates the production date (from ECSS-Q-ST-60-14C Rev.1 Corr.1)

NOTE
Generally, four-figures codes two for the year and two for the week

NOTE
Special lot number can also identify the date code.

designed module

custom module designed for specific space application, manufactured using COTS or High-Rel components.

procured module

Market available modules originally designed for a non-space high-rel application (defence, aeronautics, medical…) using COTS or High Rel EEE components. Procurement is from a recurring serial production line with medium to large manufacturing volume. Availability of reliability data from manufacturing and field use is expected for these types of modules.

reference design

A reference design describes the circuital and applicative solutions that are built around a generic or specific component (in this context, a COTS component), addressing the required mitigation techniques to ensure that the expected functionality and performance is achieved to the applicable level of criticality.
Formally speaking, a reference design is configured with a customer approved set of documents.
A reference design contains all the necessary design mitigation techniques around a generic or specific component to allow its reliable

use in a (radiation) environment.
For example, an application board for COTS FPGAs with provision of a SET-free majority voter to have a reliable output not affected by SET.

TIDL, TNIDL

are, respectively, the Total Ionizing Dose and Total Non-Ionizing Dose levels received by a component/part. TIDL/TNIDL are estimated/calculated as described in Annex 3.

TIDS, TNIDS

are, respectively, the Ionizing Dose and Non ionizing dose levels for which the part/component reaches the maximum parameter drift acceptable for its given application. When TID/TNID test is performed at part level, parameter drift is equal to average drift +/- 3*standard deviation of drift among tested samples (5 samples minimum). When TID is evaluated at board level, TIDS, is the dose level for which the maximum parameter drift of the application is reached.

trace code

Trace code (or traceability information) is a unique identifier used by manufacturers to label and trace a quantity of components with a common manufacturing history and thereby common characteristics (from ECSS-Q-ST-60-13C).

6 REFERENCE DOCUMENTS

In the document, reference document xy is identified in brackets [xy].

01. Automotive Components Qualification, J.E.Le Calvé, Valeo, COMET, May 24th, 2018
02. Automotive grade capacitors & Space Applications, Joao Pedroso, KEMET, COMET, May 2018
03. The use of automotive components for space application, Vishay, COMET, May 2018
04. Reliability tests at board level, F. Vacher, CNES, COMET, May 24, 2018
05. How to Perform Representative Radiation Tests on Automotive Components, F. Bezerra, CNES, COMET, May 24, 2018
06. The selection, procurement and use of automotive components for space applications, Industrial (Prime) Point of View, M. Marin, A. Mouton, ADS, COMET, May 2018
07. The selection, procurement and use of automotive components for space applications, Industrial (Equipment Supplier) Point of View, G. Salvaterra, ADS, COMET, May 2018
08. AUTOMOTIVE EEE parts in SPACE applications, N. Jaussein, E. Marin, TAS, COMET, May 24, 2018
09. COTS in Space: Experience and lessons learned at ESA, K. Lundmark, ESA, SERESSA 2018
10. Texas Instruments HiRel ESA Update, TI presentation, Sep 2018
11. Decision Tree for Use of COTS Electronic Components -TR - HRE-IL - V1.2 - 2017_09_19
12. Counterfeit avoidance, CNES lessons learned and Policy, P. Lay, CNES, ESCCON, Mar 2013
13. Techniques for radiation effects mitigation in ASICs and FPGAs handbook, ECSS-Q-HB-60-02A, Sep 2016
14. Single Event Effects Mitigation Techniques Report, DOT/FAA/TC-15/62, FAA, Feb 2016
15. IGLOO2 and SmartFusion2 65nm Commercial Flash FPGAs, Interim Summary of Radiation Test Results, Microsemi, Oct 2014
16. TR0011, Test Report, Radiation-Tolerant ProASIC3 Single-Event Latch-Up, Microsemi, May 2017
17. Radiation Effects on CMOS Active Pixel Image Sensors, V. Goiffon, ISAE-SUPAERO, Nov 2015
18. Response Variability in Commercial MOSFET SEE Qualification, J. S. George and others, IEEE transactions on nuclear science, Vol. 64, no. 1, January 2017
19. A Bayesian Approach for Total Ionizing Dose Hardness Assurance, R. Ladbury, B. Triggs, IEEE transactions on Nuclear Science, Vol. 58, no.6, Dec 2011

20. Statistical Modeling for Radiation Hardness, towards bigger data, R. Ladbury, M.J. Campola, IEEE transactions on Nuclear science Vol. 62, no.5, Oct 2005
21. FPGA Mitigation Strategies for Critical Applications, M. Berg, SERESSA 2018, ESTEC/ESA, November 2018
22. 2017 Compendium of Recent Test Results of SEE Conducted by the JPL Radiation Effect Group, G.R. Allen and others, JPL, 2017
23. What's My Prior - Baby steps towards big data, R. Ladbury, J.M Lauenstein, JPL, 2019
24. Angular Dependence of Heavy-Ion Induced Errors in Floating Gate Memories, S. Gerardin & al., IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 58, NO. 6, DECEMBER 2011
25. Probing SET Sensitive Volumes in Linear Devices Using Focused Laser Beam at different wavelengths, C. Weulersse, & al., Proceeding of RADECS Conference, 2006
26. Critical Charge for Single-Event Transients (SETs)in Bipolar Linear Circuits, R. L. Pease, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 48, NO. 6, DECEMBER 2001.
27. New Reliability Prediction Aimed at Space Applications, ESA contract number 4000121065/0/0/0.
28. Single-Event Upsets Characterization of the 28nm Kintex-7-based Programmable Logic of Xilinx Zynq-7000 FPGA, University of Pyraeus, July 2019
29. Single-Event Upsets Characterization of the 28nm Artix-7-based Programmable Logic of Xilinx Zynq-7000 FPGA, University of Pyraeus, July 2019
30. Guidelines for electrical design and interface requirements for power supply, ECSS-E-HB-20-20A, 15 April 2016
31. Radiation-Tolerant ProASIC3 Single-Event Latch-Up, Test Report, TR001, Microsemi, 2017. https://www.microsemi.com/document-portal/doc_download/131375-tr0011-radiation-tolerant-proasic3-single-event-latch-up-test-report
32. Calculation of radiation and its effects and margin policy handbook, ECSS-E-HB-10-12A, 17 December 2010

7 REFERENCE STANDARDS

In the document, reference standard xy is identified in brackets [Sxy].

01. ECSS-Q-ST-60C-Rev.2, EEE components, 21 October 2013
02. ECSS-Q-ST-60-13C, Commercial EEE components, 21 October 2013
03. ECSS-Q-ST-60-15C, Space product assurance, Radiation hardness assurance - EEE components, 1 Oct 2012
04. GEIA-STD-0005-2_REVA_Draft 110105, Standard for Mitigating the Effects of Tin Whiskers in Aerospace and HP El Systems
05. IPC-6012E(L), Qualification and Performance Specification for Rigid Printed Boards, Mar 2021
06. IPC-6012ES(L), Space and Mil Avionics Application Addendum to IPC-6012E, Apr 2020
07. IPC-A-600K(L), Acceptability of Printed Boards, Jul 2020
08. IPC_J-STD-001H_EN, Requirements for Soldered Electrical and Electronic Assemblies, Sept 2020
09. IPC_J-STD-001GS, Space and Military Applications Electronic Hardware addendum to IPC J-STD-001G, Mar 2018
10. ESCC basic specification No.25100, Single Event Effects test method and guidelines, issue 2, October 2014
11. ECSS-Q-ST-70-38C Rev.1, Corrigendum 1, High-reliability soldering for surface-mount and mixed technology, 12 September 2018
12. ECSS-ST-Q-70C Rev.2, Material, mechanical parts and processes, 15 Oct 2019
13. ECSS-ST-Q-70-01C, Contamination and cleanliness control, 15 Nov 2008
14. ECSS-ST-Q-70-08C, Manual soldering of high reliability soldering connections, 6 Mar 2009
15. ECSS-Q-ST-70-12C, Design rules for printed circuit boards, 14 Jul 2014
16. ECSS-Q-ST-70-60C (corrigendum 1), Qualification and procurement of printed circuit boards, 1 Mar 2019
17. ECSS-Q-ST-70-02C, Thermal vacuum outgassing test for the screening of space materials, 15 Nov 2008
18. ESCC Basic Specification No. 22900, issue 5, Total Dose Steady-State Irradiation test method, June 2016
19. ESCC Basic Specification No. 22500, issue 1, Guidelines for displacement damage irradiation testing, November 2019
20. ECSS-Q-ST-60-02C, ASIC and FPGA development, 31 July 2008
21. ECSS-E-ST-20-20C, Electrical design and interface requirements for power supply, 15 April 2016
22. AEC-Q100, Failure Mechanism Based Stress Test Qualification For Integrated Circuits (set of standards), see http://www.aecouncil.com/

23. AEC-Q101, Failure Mechanism Based Stress Test Qualification For Discrete Semiconductors (set of standards), see http://www.aecouncil.com/
24. AEC-Q102, Failure Mechanism Based Stress Test Qualification for Discrete Optoelectronic Semiconductors in Automotive Applications (set of standards), see http://www.aecouncil.com/
25. AEC-Q103, Failure Mechanism Based Stress Test Qualification for Sensors in Automotive Applications (set of standards), see http://www.aecouncil.com/
26. AEC-Q104, Failure Mechanism Based Stress Test Qualification For Multichip Modules (MCM) In Automotive Applications (set of standards), see http://www.aecouncil.com/
27. AEC-Q200, Stress Test Qualification For Passive Components (set of standards), see http://www.aecouncil.com/
28. ECSS-E-ST-10-12C, Method for the calculation of radiation received and its effects, and a policy for design margins, 15 November 2008
29. ECSS-E-ST-10-04C Rev.1, Space environment, Space environment

8 FIRST IMPORTANT REMARKS

This is a short synthesis of the reference material provided in section 6 and 7.

- For high reliability application, the burden of evaluation/suitability check is suggesting that the COTS approach is only affordable for some large procurement. For example, EEE components used by major companies for constellations or launchers, were thoroughly tested/verified and many lots/references were rejected during these investigations. It appears that one can only afford such cautious approach, and such preliminary expenses, if there is a substantial production volume afterwards (importance of "economy of scale" in relation to procurement aspects - [1], [2], [3], [4], [5]. [6], [7], [8], 15], [9]).
- It may be difficult to know traceability of active commercial and automotive EEE components, hence to know actual flight model radiation capabilities ([6], [7]).
- For COTS components and modules, it seems that there are fast obsolescence issues ([7]).
- There is a clever move from manufacturers to offer intermediate quality levels, including lot/dies traceability (see for example Microchip COTS+ [06] or TI's EP [10]).
- ECSS-Q-ST-60-13C has been updated to consider specific evaluation and acceptance requirements for AEC-Q EEE components [S22…S27], and to include provision for the procurement of commercial passive components in three different classes. See also [6], [7], [8].
- There is a proposed decision tree for use of COTS electronic components in support of general discussion in HRE [11].
- Counterfeit avoidance is a big issue: recommendations to minimize the risk of counterfeit components should be followed [12].

9 GENERAL APPROACH TO COTS COMPONENTS AND MODULES

The general approach for the use of COTS components and modules is summarised in Figure 3.

Area	Criticality Category	TIDL limit	*Recommended Mission Application*	*Time limit*
Normative	**Q0**	n/a	*All*	*N/A*
Informative	**Q1**	10-15 Krad (just indicative, see note)	All, **but** depending on the SEE test and validation performed (heavy ions, protons or both depending on the mission)	up to 5 years
	Q2	5 Krad (just indicative, see note)	Low LEO orbits (typically <1000Km), if availability is not required through South Atlantic Anomaly and poles (e.g. the equipment can be switched OFF there) Outer space regions far from stars and radiative planets (e.g. Jupiter) if the equipment is switched ON for reduced time (esp. to reduce the risk of destructive events due to heavy ions or protons)	up to 1 year

- The TIDL limit for class Q2 is not arbitrary, but it derives from the simple consideration that many of the common EEE technologies (apart from a few cases such as electro-optical, bipolar, BiCMOS ,ADCs, DACs, voltage regulators, power MOSFET, flash memories) are able to withstand a radiation level of 5Krad without major degradation impairing their use . For details, refer to section 10.5.1.
- The TIDL limit for Q1 is only indicative, it depends on the individual mission radiation environment and equipment analysis. considering that homogeneity of the procured lot in Q1 is not certain. The TIDL limit is formulated to keep risk under reasonable control under these circumstances. Higher TIDL limits can be pursued in Q1, but considering that despite the recommended radiation testing there is still the risk to fly something different than what was tested on ground. For details, refer to section 10.5.1.
- Most of the limitations for Q2 and Q1 derive from environmental considerations relative to SEE (heavy ions and protons), especially of destructive nature (SEL with destructive effects, SEGR, SEB).
- Even if parts are switched off, they will still receive a radiation dose (TIDL) that may affect their operation.
- Recommended time limit are based on the uncertainty in correlating the results of Tin whiskers susceptibility test (JSD201) and the lifetime of the application.
- Most of anomalies in space equipment induced by radiation are due to destructive heavy ion effects, and it may be far more critical than TID or TNID effects for short missions.

Figure 3, Criticality classes and applications

Figure 3 identifies specific criticality categories for COTS components and modules and gives the relevant recommended mission application boundaries.

The table provided in Figure 3 identifies two main areas, one called “Normative area” and another one called “Informative area”.

For the COTS components belonging to the “Normative area”, identifying the lower criticality category Q_0, it is possible to follow specific control, procurement, screening and test requirements in accordance to the ECSS-Q-ST-60-13C and/or ECSS-Q-ST-60C. Note that it does not make sense to identify measures to cover COTS “modules” in criticality category Q_0, because the relevant space conformity is indeed evaluated at (EEE) component level.

For the COTS components and modules belonging to the “Informative area” it is not possible to refer to specific control, procurement, screening and test requirements according to a defined standard, but it is possible to confirm adherence to best practises and mitigation techniques as defined in this document.

One difference between “Informative” and “Normative” area is linked to the traceability information (or trace code, according to the definition 3.2.1 of ECSS-Q-ST-60-13). If the same trace code can be guaranteed between the EEE COTS components subject to evaluation/lot acceptance test, and the ones that will actually be used for flight, requirements of the normative area can be fully applied, and we can be sure of consistent functionality and performance in flight with respect to the test performed on ground.

If the same trace code cannot be guaranteed, there is no possibility to have this certainty (without extensive additional testing), and this is addressed in the informative area.

While it is still possible to take counter-measures against radiation to decrease the probability of mission failure (by circuit/system design, redundancy schemes, reduction of utilisation factors – voltage, current, power, temperature – versus absolute maximum ratings), there is no guarantee that the EEE COTS components subject to space conditions will behave in the same way of the ones that have been characterised, tested or screened on ground.

Note also that for full consistency of radiation performances, it is in general not enough to only ensure the same trace code. A trace code may include EEE components from several wafer fabs and several diffusion lots [6].

Additionally, it should be taken into account that burn-in test (that is usually performed as screening test on flight EEE components to remove infant mortality failures) can affect a component response to TID, and in some cases, even SEE (see [18]).

The identified criticality categories (Q_0 to Q_2) are applied for functions at subsystem, equipment or module level. A given mission can include systems, subsystems, equipment or modules of different criticality categories.

In general, it is not possible to ascertain the criticality category of a function included in a module, equipment or subsystem from the criticality category of the components thereby included, but it is necessary to evaluate the relevant risk profile in relation to the mission and its objectives.

For example, we could use in a high profile mission (using Q_0 elements for its most critical EEE components) a commercial camera of criticality category Q_2 for visualising the separation from the launcher and the spectacular deployment of the solar array and the other appendages.
In fact, the camera required lifetime is very low, the accumulated radiation level is negligible, and the overall camera reliability is expected not to be of particular concern.

The following sections are meant to identify the programmatic and technological answers to the initial logical questions for COTS in space applications, for each criticality category Q_0 to Q_2, with the identification of activities and actions to be followed up to get a satisfactory answer to each issue.

The content (per criticality category) is the following:

- *Perimeter of application (according to table in annex 1 with some more details)*

- *Methods to address the critical points relevant to*
    - *RAMS*
    - *Material and processes*
    - *EEE components general issues*
    - *Radiation*
    - *EEE Procurement aspects*
    - *Application, including*
        - *approaches for data sheets review*
        - *electrical analyses needs*
        - *mitigation techniques*
        - *reference application circuits*
        - *modules*

      The nature of the mitigation techniques provided for each criticality category refer to design and circuit solutions to overcome radiation and random quality issues at EEE component level.

10 CRITICALITY CATEGORY Q2

Equipment, subsystem or system of criticality category Q_2 normally rely on precedent history and heritage.

10.1 Perimeter of application

a. The mission radiation exposure TIDL at component level should be limited to <5 Krad(Si).
b. The mission operational duration should be limited to few months, typically less than one year.

NOTE
It is assumed that conventional qualification and acceptance campaigns are conducted at module, equipment, subsystem and system level according to project specific requirements.

10.2 RAMS

10.2.1 Safety

a. COTS components and modules involved in safety related functions should provide the same design features and qualification evidence required to category Q_0 components and modules according to the safety requirements defined by relevant Safety Launch Authority during launch phase and by national laws and regulations during AIT operations.

10.2.2 Dependability

a. No reliability quantitative requirement are specified for items (modules, equipment, subsystem) belonging to criticality category Q_2.

NOTE
The lack of reliability data does imply that compliancy to several requirements related to sustainability (i.e. successful disposal probability, collision impact probability) is not verifiable.

It is suggested to avoid the use of COTS module or equipment class Q_2 in

critical or essential mission functions (for example related to re-entry, docking or landing on a planetary surface).

b. COTS components and modules failures of higher criticality category should not propagate to interfacing module, equipment and subsystem functions.

NOTE
For power interfaces, it is assumed that over-current protection is provided by the power source contained in power distribution (by latching current limiter, fuse or electronic fuse) in order to limit electrical but also thermal failure propagation.

Design of overcurrent protection should be done with care to avoid problems. For example, if there is not sufficient granularity, all the current may be "steered" through a latched component that provides a low-resistance path to ground while other functions shut down from lack of current. The result is that one could see the latched component fail even though the total current flowing doesn't change (or even decreases).

NOTE
For signal interfaces, it is assumed that fault voltage and current emission are consistently respected from transmitter and receiver side.

NOTE
As an example, an equipment Q2 should not be susceptible to damage the satellite during the assembly due to low quality connectors.

c. FMECA should demonstrate absence of failure propagation.

d. For recommendations on design analyses, see application chapter 10.7.

e. A minimum set of telemetries should be provided to guarantee the required level of failure observability at system level.

f. The outage budget should be set considering the unavailability of the module, equipment or subsystem due to RHA limitations.

g. Since autonomous recovery is expected to be very limited, availability requirement should be set considering that recovery (for example from SEFI or SEL) is mainly implemented by telecommands.

10.3 Materials and processes

a. For the selection and use of material and processes of COTS components and modules, the principle should be not to harm the hosting satellite
b. For pure Sn finished EEE components the relevant mitigation strategy should be defined on the basis of GEIA-STD-0005-02 [S04] level 1
c. Outgassing should be evaluated if camera or other sensitive equipment is on the same space vehicle, according to ECSS-Q-ST-70-02C
d. If outgassing is a concern,

  - the declared material list should be provided for review together with the amount of the critical outgassing materials, and
  - outgassing tests should be performed on flight representative equipment

e. Soldering profiles recommended by COTS EEE components manufacturers should be respected
f. For PCBs, class 2 may be used as per IPC-6012E ([S05], Procurement per class 3 or higher is recommended.
g. For soldering, the requirements of IPC-J-STD-001 class 2 maybe be used [S08], application of class 3 requirements is recommended.
h. With respect to health and safety, beryllium oxide (except if identified in the procurement specification), cadmium, lithium, magnesium, mercury, zinc, radioactive material and all material which can cause safety hazard should not be used.
i. A material list should be provided.

NOTE
The importance of this recommendation is to ensure that no risky materials are present in the equipment under consideration.

10.4 EEE components

a. AEC-Q components [S22…S27] are preferred.

b. COTS components should preferably be selected among the ones having manufacturer's recommended operating temperature range from -40degC to +85degC or wider.

c. The supplier should ensure that non-hermetically sealed materials of components meet the requirements of ECSS-Q-ST-70 regarding off-gassing, out-gassing (if it is a concern), flammability, toxicity and any other criteria specified for the intended use.

d. With respect to health and safety, beryllium oxide (except if identified in the procurement specification), cadmium, lithium, magnesium, mercury, zinc, radioactive material and all material which can cause safety hazard should not be used.

e. For limited life duration, known instability, safety hazards or reliability risk reasons, the EEE components listed below should not be used:

1. Hollow core resistors
2. Potentiometers (except for mechanism position monitoring)
3. Wet slug tantalum capacitors other than capacitor construction using double seals and a tantalum case
4. Wire link fuses
5. Commercial relays and switches (including RF EEE components)
6. Thyristors

f. For limited life duration, known instability, safety hazards or reliability risk reasons, EEE components listed below shall not be used for new designs:

1. RNC90 > 100 kΩ

g. The Declared Component List should be provided, with content that can be relaxed compared to ECSS-Q-ST-60 requirements to minimum:

- Component number (commercial equivalent designation)
- Family (ESCC group code)
- Package
- Value or range of values
- Component manufacturer (name, country)
- Quality level
- Name of the procurement agents (CPPA, supplier, distributor)
- Change identification between each DCL issue

h. For high voltage (higher than typically 200V) and also high power microwave EEE components the compatibility with operation in vacuum should be addressed.

10.5 Radiation

For Q2 criticality category, the radiation hardness is assessed by the following measures.

a. A radiation analysis should be provided.

10.5.1 TID

a. The calculated TIDL received at component level should be less than 5 krad(Si).

> NOTE
> TID limit for recommending no test it is only indicative since some technologies are sensitive at lower radiation level (bipolar and BiCMOS contained in ADCs, DACs, voltage regulators, power MOSFET, flash memories).
> Some examples:
> - A digital to analog converter was found exceeding specification limits at 1 krad (DAC8800).
> - A voltage comparator showed input bias current doubled after 5 krad (LM111).
> - An operational amplifier (OP296, BiCMOS) failed parametrically at 0.8 krad(Si) and functionally at 1.8 krad(Si).

b. When calculating the TIDL, considering the 5krad(Si) limit for untested COTS, the modelling approach described in annex 3 should be used.

c. If TIDL < 5krad(Si) then untested COTS components may be used.

d. The target design should be robust to possible TID parameter drifts of the component in excess of its original datasheet.

> NOTE
> For example, the component is not subjected to additional stress conditions that might impair its functionality in the required lifetime.

See Annex 2 for typical parameters affected by radiation for each technology type.

10.5.2 TNID

a. The TNIDL should be calculated for optoelectronic devices.

b. TNIDL calculations should be performed using the same modelling approach as described in annex 3.

NOTE
A 50MeV equivalent proton fluence <2E11 p/cm2 should be normally encountered in the environment where the TID threshold is the specified one (5Krad).

c. For optoelectronic components flying in a proton rich environment radiation verification testing is strongly advised and/or selection of known radiation tested lots procured.

NOTE
See Annex 2 for typical parameters affected by radiation for each technology type.

10.5.3 SEE

a. SEE experimental test verification is highly recommended, e.g. with high energy protons, but not required. However it should be assumed that SEEs will occur and their mitigation by robust design should be implemented at component, module/board and system level.

NOTE
Refer to annex 4 for SEE test verification

NOTE
For mitigation techniques, see section 10.7.3 and Annex 2.

NOTE
Mitigations without testing cannot guarantee insensitivity to SEE including destructive SEE.

NOTE
When large procurement quantities are foreseen (for example for components used in a data recorder or readout of a complex detector array), the logical choice would be to follow the prescribing requirements of class Q0, because the large procurement lot size would likely justify the cost of screening and test.

10.6 EEE Procurement aspects

a. EEE components should be procured from official distributors

b. If it is possible, EEE components should be procured directly from the relevant manufacturers.

c. To achieve the maximum possible level of homogeneity, complete reels of components should be procured.

d. For COTS components and module, manufacturer's storage conditions should be followed.

10.7 Application

10.7.1 De-rating rules

a. For EEE components, the same or higher derating margins should be applied as defined in the ECSS-Q-ST-30-11and ECSS-Q-ST-60-13.

b. If complete modules are procured, the relevant application ratings (temperature, power, voltage, current) should be respected with margins to be agreed with the customer.

c. PSA document may not be delivered.

10.7.2 Worst case analysis

a. No WCA document is required, but WCA should be performed without considering ageing on the parameters.

NOTE
As basis for WCA, use data sheet information and known radiation drifts (see annex 2 and follow up recommendation in section 16). In case important parameters drifts are not available, get information about their variability by testing a representative set of samples.

b. Margin on component max/min ratings and performances should be considered in the design to account for component parametric drift due to radiation.

NOTE
See Annex 2 for typical parameters affected by radiation for each technology type.

c. The design should be robust against alleged tolerances

10.7.3 Mitigation techniques

In this section, design and application mitigation techniques to overcome degradation at component level due to radiation or to random failures are explained, at component, module/board and system/subsystem level.
For generic mitigation techniques description and explanation, see Annex 2.

10.7.3.1 Mitigation techniques at component level

10.7.3.1.1 General

a. Filtering of SET (transients) should be performed according to the Worst-case SET templates provided in ECSS-Q-ST-60-15C (table 5-4).

b. Effects of SEL should be taken into account for all devices based on CMOS and BiCMOS technology, including memories.

c. Power cycling should be implemented to mitigate SEL risk in all cases at board or unit level.

NOTE
The effectiveness of power cycling is subject to reference designs where mitigation techniques are adopted and validated. The heritage applies more to the reference design than on the specific component or module.

NOTE
For specific devices, other mitigation techniques can be implemented as explained in the relevant sub-sections of section 10.7.3.1.

10.7.3.1.2 Power discrete devices

a. The voltage application of power components (silicon MOSFET) should be de-rated to:

- MOSFETs BVDSS rated more than 200V should not be used
- maximum 30% of the datasheet value on the drain voltage
- less than 50% of absolute maximum rating voltage value on the gate (ON state)
- Do not apply negative gate to source voltages to n-channel MOSFET, or positive gate to source voltages to p-channel MOSFET (OFF state).

NOTE
One possible mitigation against SEB is to add a current limiting device for transient events (either resistance or inductance) in the drain path if this is compatible with device operation.

NOTE
The gate de-rating recommendation is provided in attempt to decrease the probability of SEGR (gate rupture), which cannot be mitigated by any other technique than decreasing the gate voltage in addition to the decrease of drain voltage.

b. For power WBG EEE components SEE test is recommended.

NOTE
The SEE test is specifically recommended for SiC.

10.7.3.1.3 Memories

a. Robust error detection and correction methods (e.g. Reed Solomon) should be used according to the memory type (SRAM, SDRAM, Flash, etc) to mitigate single and multiple upsets (SEU/MBU).

NOTE
The effectiveness of mitigation depends on the memory organization and multi-bit/multi-cell upset behaviour.

b. Hamming ECC can be used for SRAM.

c. Reed-Solomon, or even BCH, ECC may be used for SDRAM, due to the nature of the faults encountered in those memories (SEFI, burst errors).

NOTE
A critical distinction is whether a SEFI requires a power cycle for recovery or whether recovery can be carried out by a reset/reload of mode registers. If power is cycled, all memory contents for die (or module) are lost. This is a distinction between volatile and non-volatile memories.

d. For SRAM/SDRAM memory arrays, scrubbing (periodic refreshing of memory contents) should also be used, to avoid accumulation of errors that could render the ECC algorithms ineffective.

NOTE
Scrubbing is more critical for more "static" data. If the memory data are

refreshed more dynamically from the application, and with expected refresh rates higher than the anticipated error rates (based on particle flux) then scrubbing may not be necessary.

e. CRC may be used for EEPROMs.

NOTE
EEPROMs are commonly used for storage or software images, or parameter sets.
With CRC data can be read back immediately after writing to confirm correct completion of write operations.
In case of errors detected at read-back, the write operations may just be repeated.

f. Wear levelling should be considered for Flash memories.
g. If not already implemented in the embedded Flash memories control logic, wear levelling should be handled by the end user.

10.7.3.1.4 FPGAs

a. For SRAM-based and Flash-based FPGAs spatial redundancy techniques may be utilized for mitigation against radiation induced SEE in the combinatorial and sequential logic.

NOTE
Local TMR can yield acceptable upset rates when used in Flash-based FPGAs, but is not recommended for SRAM FPGAs as the upset rates may even be worse than with no mitigation in those devices.

Full (or Global) TMR is the strongest method of SEU mitigation for SRAM-based FPGAs, but the skew between the triplicated clocks may be a challenge to manage, and it can reduce the effectiveness of the mitigation.

Distributed TMR is a good compromise between SEU mitigation strength, implementation complexity, and area overheads, and is the recommended TMR scheme for SRAM based FPGAs.

Designers should try to select the most suitable TMR scheme to meet the error rate requirements in their projects, while keeping effort and area overheads to minimum. (see section A.2.4.2.1.1)

b. Hamming-3 encoding and "safe FSM" options may be used for Finite State Machines, in addition to the TMR used for state vector registers.

c. Depending on the acceptable error rate for the on-chip memories, EDAC may also be used for the on-chip RAM blocks.

d. The configuration memory of SRAM FPGAs should be protected by scrubbing and EDAC: periodic scan and correction of the active configuration memory. Scrubbing can be either :

   (i) "blind scrubbing", in which case the complete configuration memory is periodically refreshed without applying EDAC, or

   (ii) "readback scrubbing", where the configuration memory is periodically compared with an externally stored "golden reference" version, corrected from of possible errors and the corrected results are written back into the configuration memory. EDAC schemes may also be employed with read-back scrubbing, such as CRC checks.

NOTE
The need for scrubbing is due to the sensitivity of the configuration memory of SRAM FPGAs to SEUs.

NOTE
A configuration-bit SEU in SRAM FPGAs may also alter the functional flow of the circuit and the design functionality. In that case, either configuration memory scrubbing and circuit reset, or a full reconfiguration, will need to be applied.

NOTE
For some FPGA memory configuration, upset conditions following SEE may require power recycle, or a full reconfiguration, because read-back and scrubbing is not always possible.

NOTE
The user will need to confirm whether the required functionality (external readback, scrubbing and reconfiguration) is supported, and can be safely applied, for the target FPGA. Possible limitations include the following cases:

- No support for external readback of the configuration memory (e.g. Intel Stratix), or the internal scrubber being sensitive to SEE.
- Partial reconfiguration process prone to failures due to SEE, in which case the device gets blocked and the process needs to be restarted (and the device reset). E.g. Xilinx Kintex-7 FPGAs

NOTE
MBUs even up to 16 bits have been observed in the configuration memory of certain SRAM FPGAs under radiation (e.g. Xilinx Artix-7, Kintex-7). In such cases the on-chip EDAC algorithm would not be able to correct the configuration frames during scrubbing. The user will need to implement an external configuration memory EDAC mechanism for such cases. [28, 29]

NOTE
The way that scrubbing and TMR are implemented for FPGAs can have a critical influence on error/outage rates, hence the importance of using a validated approach. Note that a bad mitigation technique can deliver worse results than no mitigation at all, especially if there is no validation by test.

e. An external latch-up protection mechanism should be employed for SRAM FPGAs: detection of current draw above a certain limit, and automatic power cycling.

NOTE
The reason is that some COTS SRAM FPGAs are susceptible to SEL.

f. Depending on the technology, Flash FPGAs may be susceptible to SEL (TBC by the user, info available from FPGA manufacturer), in which case an external latch-up protection mechanism should be used.

NOTE
As examples, the Microsemi SmartFusion2 and IGLOO2 Flash FPGAs are SEL sensitive at heavy ion energy levels ≥24 MeV*cm²/mg [15], but the (RT)-ProASIC3 Flash FPGAs do not experience SEL below 60 MeV*cm²/mg [16].

NOTE
The configuration memory of Flash-based FPGAs is immune to SEE.
In Flash-based FPGAs, the memory cells that keep the configuration information (routing and LE/tiles configuration), are Flash based, so they are inherently not susceptible to SEUs/bit flips.
This provides a good level of radiation tolerance, since only the logic (sequential and combinational) and the on-chip memories need to be mitigated.

10.7.3.1.5 Microprocessors

Microprocessors can be susceptible to SEU for their internal memories, SEFI for the on-chip functional units (processor core/s), and SEL.

a. The on-chip memories may be protected by ECC, by software generated CRC, parity for register files and caches if supported).

b. External memories may be protected by dedicated ECC (see recommendation 10.7.3.1.3 b).

c. Watchdogs may be utilised to monitor and detect SEFI.

d. Most COTS microprocessors are susceptible to SEL, so an external latch-up protection mechanism should be used, with detection of current draw above a certain limit, and automatic power cycling.

e. SEL protection logic needs to be activated in a prompt manner (typically within 1ms) after appearance of overcurrent condition to avoid damages to the component.

   NOTE
   The response time should be sufficient to discharge the energy contained in the relevant decoupling capacitors (typically 10's or 100's of ms).
   A generic approach for SEL protections is shown in Figure 4.

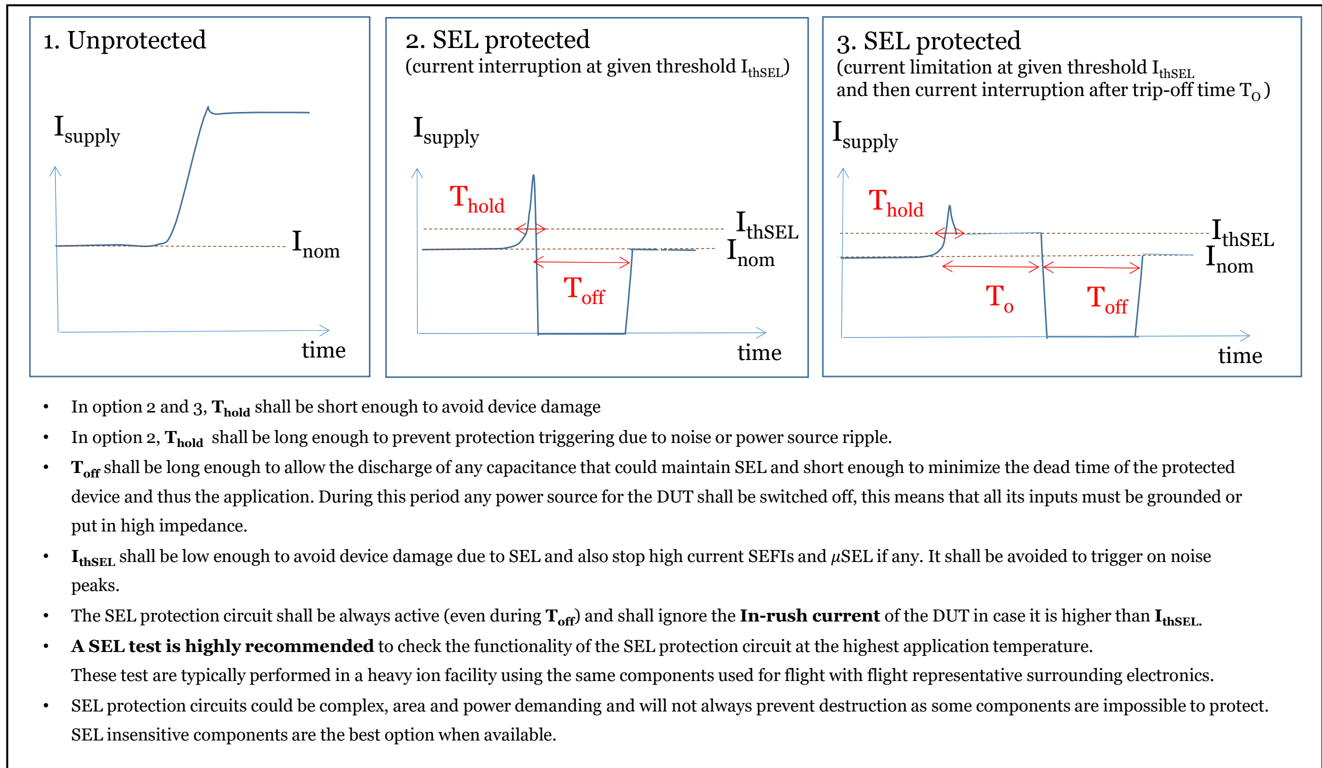


Figure 4, Different SEL protection approaches

For resolution of SEFI two alternative approaches are recommended: one utilising a watchdog timer (recommendations f to h) or a simpler method based on periodical reset or power cycle (recommendation i).

f. A watchdog timer should be used to detect SEFIs or deadlock situations, where the normal execution flow of the processor is interrupted.

g. The watchdog should be periodically refreshed by the user application.

h. If the watchdog expires, an interrupt should be raised and the device should be reset.

> NOTE
> The watchdog expiration condition may also be managed by an external supervisor, responsible for resetting or power cycling the device. This may also be the responsibility of the main platform controller (e.g. OBC).

i. To resolve SEFI (and possibly SEL) a microprocessor may be periodically reset, or power cycled.

NOTE
Periodic reset can help avoid deadlocks due to SEFI, and periodic power cycling may help control SEL effects.
However, this cannot be considered as a reliable SEL protection mechanism: SEL can be a destructive event, and the SEL protection logic need to respond in a prompt manner after detection of the overcurrent condition to avoid damage to the component.
Periodic power cycling may not be of sufficiently high frequency to guarantee proper protection.
On the other hand, a high power cycling frequency would not be practical and might have too high an impact on system availability.

j. To control destructive effects of SEL, local overcurrent protection mechanisms should be used if repetition frequency of periodic power cycling cannot be made fast enough to avoid destructive effects.

   For Q_2, “remote” SEL mitigation, consisting in current sensing of power supply rails to the module from OBC platform, with power cycling if current spikes are detected, may replace recommendation j.

10.7.3.1.6 Microcontrollers

Microcontrollers tend not to have caches (e.g. for more deterministic behaviour), but they do integrate analogue functions such as ADC/DAC, PWM controllers, etc, which will need to be considered accordingly.
See relevant sections on analogue components/modules in this document as well standard [S03].

As is the case for microprocessors, microcontrollers can also be susceptible to SEU for their internal memories, SEFI for the on-chip functional units (processor core/s), and SEL. However, they tend to be used for simpler applications compared to microprocessors, so their SEE mitigation requirements may be adapted accordingly.

a. The on-chip SRAM is usually very sensitive to SEU, so the designer should assess the “criticality” of the application data and apply ECC as needed to protect the on-chip volatile memory blocks.

Program code is usually stored in Flash or EEPROM, either on-chip or externally, which should already provide sufficient SEU tolerance for the requirements of Q2 category applications.

b. A CRC may still be used for these memories, especially if the program memory is to be updated at later points (patched).

NOTE
Some microcontrollers support program execution directly from Non Volatile Memory. In other cases, the program image needs to be copied to on-chip SRAM first. In that case, recommendation a above also applies.

c. Watchdogs may be utilised to monitor and detect SEFI.

d. Most COTS microcontrollers are susceptible to SEL, so a SEL mitigation mechanism may be implemented for the detection of current draw exceeding a certain limit, and power cycling as a result.

NOTE
The SEL mitigation can either be in the form of a dedicated SEL protection circuitry, or as an automatic periodic power cycling controlled by an external source (supervisor). In this second case, a rather simplified current limiting device (for example, a resistor) can be used to ensure that the SEL is not destructive.

e. SEL protection logic needs to respond in a prompt manner (in TBD ms) after detection of the overcurrent condition to avoid damage to the component.

SEFI may be mitigated either by a watchdog timer mechanism (recommendations f to h below), or by automatic, unconditional, periodic reset or power cycling, controlled by an external source (supervisor) (recommendation i below).

f. A watchdog timer may be used to detect SEFIs or deadlock situations, where the normal execution flow of the processor is interrupted.

g. The watchdog should be periodically refreshed by the user application.

h. If the watchdog expires, an interrupt should be raised and the device should be reset.

NOTE
The watchdog expiration condition may also be managed by an external supervisor, responsible for resetting or power cycling the device. This may also be the responsibility of the main platform controller (e.g. OBC).

i. To resolve SEFI (and possibly SEL) a microcontroller may be periodically reset, or power cycled, by an external source.

NOTE
Periodic reset can help avoid deadlocks due to SEFI, and periodic power cycling may

help control SEL effects.
However, this cannot be considered as a reliable SEL protection mechanism: SEL can be a destructive event, and the SEL protection logic need to respond in a prompt manner after detection of the overcurrent condition to avoid damage to the component.
Periodic power cycling may not be of sufficiently high frequency to guarantee proper SEL protection.
On the other hand, a high power-cycling frequency would not be practical and might have too high an impact on system availability.

j. To control destructive effects of SEL, local overcurrent protection mechanisms may be used if repetition rate of automatic periodic power cycling cannot be made fast enough to avoid destructive effects.

10.7.3.1.7 Programmable Systems-on-a-Chip (SoC)

Since SoC are a combination of FPGAs with embedded microprocessors, the recommended SEE mitigation techniques to be applied are a combination of the recommendations on FPGAs (according to FPGA type, SRAM or Flash), microprocessors and memories (see para 10.7.3.1.3, 10.7.3.1.4, 10.7.3.1.5 and also A2.4.2.7).

A simple form of error mitigation at software level is duplication the execution of certain instructions and compare the results. If a discrepancy is detected between the results, an exception may be raised and the program backtracked to a previous check-point.

Table 1, Possible SEE as a function of component technology and family

Component Type	Technology	Family	Function	SEL	SESB	SEGR	SEB	SEU	MCU/SM	SEDR	SEHE	SEFI	SET	HCE
Transistors	Power MOS					X	X							
ICs	CMOS or BiCMOS or SOI	Digital	SRAM	X*				X	X		X			X**
			DRAM/SDRAM	X*	X			X	X		X	X		X**
			FPGA	X*				X		X		X		X**
			EEPROM/ Flash EEPROM	X*		X				X		X		X**
			µP/ µcontroller	X*		X		X		X	X	X		X**
		Mixed Signal	ADC	X*				X		X		X	X	X**
			DAC	X*				X		X		X	X	X**
		Linear		X*						X			X	
	Bipolar	Digital						X					X	X**
		Linear						X					X	
Opto-electronics			Opto-couplers										X	
			CCD	X									X	
			APS (CMOS)	X								X	X	

*except SOI
**TBC for SOI

NOTE: On the basis of recent experience, also Si and SiC diodes should be added the table.

NOTE: SET is only mentioned for analogue or mixed analogue/digital components

To give an idea,

- about 50% of CMOS EEE components are SEL susceptible, and in about 50% of those, SEL is destructive.
- SDRAMs have not been observed to latch since about 2010. Flash memories still latch, but only about 25% of them do.
- ADCs and DACs--about 72% of commercial ADCs and DACs are susceptible to SEL.

As a reference, see [22] and [23].

10.7.3.2 Mitigation techniques at module/board level.

a. Power cycling provisions to any complex digital circuit to resolve SEL and SEFI should be provided.

b. Error detection and correction provisions should be provided in memories against SET, SEU.

c. Current limitation, detection and power reset provisions should be used to survive SEL (latch-up) in EEE components/boards, especially when including SRAM memories.

d. For effective SEL mitigation the response time for SEL protection should be limited, due to the potentially destructive nature of the latch-up event.

    NOTE
    There are a few devices where SEL happens too rapidly for any protection circuit to kick in.
    Also, the more rapid the response, the more likely it is to suffer false resets due to transients.

e. To increase SEL protection levels the SEL protection should be implemented locally within the module hosting the SEL sensitive part(s), to reduce latency in the detection and management of the SEL (latch-up event detection and power cycling).

f. Critical functions should be provided with redundancy and voting.

g. If voters are used, they should be inherently robust to SEE.

10.7.3.3 Mitigation techniques at system/subsystem level.

It is important to provide as much in-flight feedback as possible for each mission, for COTS-based components/modules/systems where ground radiation verification, testing and qualification has not been performed.

a. In case of redundant systems, provide timely switching from main to redundant back-up systems in order to meet availability requirements.

b. At system level measure, monitor, management approach should be used using radiation effect sensors and relevant telemetry channels.

If the use of (“direct”) radiation monitors is not feasible, indirect methods of radiation performance characterization might be used, such as “radiation-induced error logging methods”, e.g. counting of EDAC instances in memories, SEFIs (and resets) in processors, SEL detected and mitigated events, performance derating due to TID etc. would be very useful, combined with relevant telemetry channels.

NOTE
This allows in-flight environment data to be recorded in order to build up in-flight component/module/system heritage and provide real-time spacecraft radiation ‘health’ data (much like temperature sensors are used to track thermal aspects).
It is also important for establishment of validation procedures.
If something goes wrong the actual reason can be determined, and lessons learned can be created and fed back into the RHA approach for the next mission.
If the spacecraft receives less radiation than designed for, the lifetime may be extended.

10.7.4 Reference application circuits

Activities are recommended to identify, collect and maintain reference application circuits for specific EEE components, so as to have a clear and unambiguous reference for radiation tests including design mitigation techniques at circuit level if applicable.

a. If available, reference application circuits should be applied.

10.8 Modules

a. Modules should not contain components or materials from forbidden lists (see section 10.3).

b. Absence of forbidden components and materials should be assured through review of parts and material lists.

c. Modules can contain design mitigation provisions as per section 10.7.3.

d. Modules should use reference circuits around specific EEE components, as indicated in section 10.7.4.

e. For procured modules and boards, radiation verification with high energy protons should be performed if radiation data is not already available.

NOTE
See annex 4.
Aim at testing the same module as the flight board (same procurement batch, same manufacturer, possibly same date code, same design).

f. Power supply modules not designed for space, and specifically commercial power supply modules (black box approach) should not be used.

g. For modules, CoC should be provided.

NOTE
Typically, a CoC would cover

1. Title including references to identify the product and the relevant applicable documents
2. Reference of conformity, calling for example the following documents:
   - Business agreement requirements: reference number of design specification, ICD or other contractual documents
   - Operational documents: reference number of drawings, procedures, and electrical schematics
   - Deliverable documents: reference number of EIDP, logbooks, and manuals
3. Statement of conformity
4. List of waivers or deviations or other remarks

10.8.1 Data sheets

a. COTS components and module performances declared in the relevant datasheets and critical for the intended design application should be subject to verification by test.

NOTE
The reason for recommendation derives from the typical disclaimers in the datasheets, stating that data and specifications are subject to change without notice. A datasheet is not as reliable as a procurement specification!

11 CRITICALITY CATEGORY Q1

Module, equipment, subsystem or system of criticality category Q_1 strongly rely on precedent history and heritage.

11.1 Perimeter of application

a. The mission radiation environment (TIDL) limit is indicatively 10-15 krad(Si).

NOTE
The TIDL limit for Q1 is only indicative, considering that homogeneity of the procured lot in Q1 is not certain.
The TIDL limit is formulated to keep risk under reasonable control under these circumstances. Higher TIDL limits can be pursued in Q1 but considering that despite the recommended radiation testing there is still the risk to fly something different than what was tested on ground.

b. The mission operational duration should be limited to few years, typically less than five years.

NOTE
It is assumed that conventional qualification and acceptance campaigns are conducted at module, equipment, subsystem and system level according to project specific requirements.

11.2 RAMS

11.2.1 Safety

a. COTS components and modules involved in safety related functions should provide the same design features and qualification evidence required to category Q0 components and modules according to the safety requirements defined by relevant Safety Launch Authority during launch phase and by national laws and regulations during AIT operations.

11.2.2 Dependability

a. Reliability quantitative requirement at system level might be specified.

b. Reliability prediction may be done using FIDES approach.

NOTE
Additional guidance is provided by the study "New Reliability Prediction Aimed at Space Applications", [27]

Testing activity should be focused to reliability growth (e.g. aimed at the identification of all possible failure modes).

c. COTS components and modules failures of higher criticality category should not propagate to interfacing module, equipment and subsystem functions.

NOTE
For power interfaces, it is assumed that over-current protection is provided by the power source (by latching current limiter, fuse or electronic fuse) in order to limit electrical but also thermal failure propagation.

For signal interfaces, it is assumed that fault voltage and current emission are consistently respected from transmitter and receiver side.

d. FMECA should demonstrate absence of failure propagation and failure prevention and compensation.

e. For recommendations on design analyses, see application chapter 11.7

f. A minimum set of telemetries should be provided to guarantee the required level of failure observability at system level.

g. At system level, autonomous recovery should be exploited as possible.

h. At system level, robust FDIR should be designed and implemented.

11.3 Materials and processes

a. For the selection and use of material and processes of COTS components and modules, the principle should be not to harm the hosting satellite.

b. For pure Sn finished EEE components classification of the risk and relevant mitigation strategy should be defined based on the approach defined in GEIA-STD-0005-02 ([S04]). If the analysis of the determination of the risk level is not performed, the application of the Control Level2B is recommended.

c. Outgassing should be evaluated if camera or other sensitive equipment is on the same space vehicle, according to ECSS-Q-ST-70-02C.

d. If outgassing is a concern,
   - the declared material list should be provided for review together with the amount of the critical outgassing materials, and
   - outgassing tests should be performed on flight representative equipment.

e. Soldering profiles recommended by COTS EEE components manufacturers should be respected.

f. The full set of additional recommendations for PCBs is given in annex 5.

g. The full set of additional recommendations for soldering verification is given in annex 6.

   NOTE
   The present recommendations do not cover lead free soldering.

h. DML, DPL and DMPL should be provided.

i. With respect to health and safety, beryllium oxide (except if identified in the procurement specification), cadmium, lithium, magnesium, mercury, zinc, radioactive material and all material which can cause safety hazard should not be used

11.4 EEE components

a. AEC-Q components [S22…S27] are not mandatory but they are preferred.

b. COTS components should only be used with recommended operating temperature range from -40degC to +85degC or wider.

c. A justification document should be provided in accordance to ECSS-Q-60-13, annex F.

d. For EEE components Class 3 (Paragraph 6) of ECSS-Q-ST-60-13 should be followed with following possible differences:
   - Constructional analysis and radiation tests (6.2.3.1 d) are not required on each lot when justification can be provided (for example high radiation margin, heritage or AEC-Q qualification to be reported in the justification document,).
   - Justification documents (6.2.2.1 e) can be combined to one per part family.

- DCL in accordance with ECSS-Q-ST-60C is required.
- Additional component families are allowed.

e. Prohibited/restricted components should be as per section 10.4 plus

- Aluminium liquid electrolytic capacitors
- PVC insulated wires and cables
- Feedthrough filter in commercial grade
- Connectors with less than 0,7µm gold plating contact in commercial grade.

f. For high voltage (higher than typically 200V) and also high power microwave EEE components the compatibility with operation in vacuum should be addressed.

11.5 Radiation

For equipment, subsystem and system belonging to the Q_1 criticality category, the radiation hardness is assessed, in addition to the measures valid for Q_2, by the following measures.

a. A radiation analysis should be provided.

11.5.1 TID and TNID

a. The radiation test at component level is recommended for TID and TNID Q_1 criticality category. unless substantial margins (3x or more) are demonstrated at board or module level. No margin is required when TIDS and TNIDS are determined by a test at component level on a sufficient number of samples (see annex 4 for details).

NOTE
The reason of this recommendation is that, in spite of aiming to it, we are not sure of homogeneity of EEE components mounted on boards.
Because of that, one cannot be sure that non- linear / saturation effects at component level are avoided that would cause as a functional failure of the board or module if a slightly different component would be used.

b. If boards or modules are procured, the margin should be demonstrated by the relevant manufacturer and not by the user.

c. If the calculated TIDL received at component level is higher than 5 krad(Si), the component should be tested according to ESCC22900 [S18] ("procedure for testing

outside of an ESCC context", section 7).

d. If the calculated TNIDL received at component level is higher than 2E11 p/cm2 50 MeV equivalent proton fluence, bipolar components should be tested to TNID according to ESCC22500 [S19].

e. Optoelectronic components (imagers, optocouplers, etc) should be tested to TNID according to ESCC22500 [S19] regardless of TNIDL, or a selection of known radiation hardened lots should be procured.

f. The detailed approach provided in Annex 4 should be applied to TID and TNID Q_1 tests.

g. For ERCB (see section 11.5.3) a detailed radiation test plan should be prepared to be agreed with the customer together a final test report deliverable to the customer.

11.5.2 SEE

a. If the EEE components can be delidded and the chip exposed, SEE heavy ion test should be performed.

NOTE
Heavy ion test results are used to measure the device cross-section sensitivity versus LET (MeVcm2/mg) and to estimate the SEE rate in-flight.

NOTE
Focused pulsed laser can be used to experimentally simulate heavy ion strike, if the semiconductor is accessible (front side or back side), for example to detect potential latch-up sensitivity (SRAM memories), or measure single event transients (SETs) amplitude and width in linear components (operational amplifier, voltage reference, etc).

NOTE
Focused pulsed laser cannot replace heavy ion irradiation. The equivalence between laser pulse energy depends on the laser parameters and the device technology and sample preparation.

NOTE
If the device cannot be delidded, the heavy ion energy (i.e. ion beam range) provided by most ground test facilities will be insufficient to reach the sensitive active part of the device.

NOTE
If the die is flip-chip mounted it is unlikely that the ions used will have the penetration range required to get through the substrate to the active regions.
Extra processing of the die (i.e. thinning) is then required, or alternatively recommendation 11.5.2.b. may be used.

b. If the EEE components cannot be delidded, heavy ion tests should be performed with very high-energy (e.g. GSI FAIR) or ultra-high energy (e.g. CERN) heavy ion facilities.

c. If it is not possible to test with very high-energies or ultra-high energies, and in agreement with Customer, test with high energy protons should at least be performed.

d. The SEE test verification should be performed at component or board level.

NOTE
Both at board and component level, the SEE assessment provides information on the devices response, which can be used to calculate mission SEE rate. In addition, the test at board level provides the response to check whether the mitigation techniques are effective.

NOTE
Heavy-ion testing usually uses focused beam. The beam characteristics are checked with the facility and included in the test plan as recommended in [S10] (Annex 4).
For board testing, mainly under proton, enough observability points (voltage, current test points) should be considered to understand correctly the board response in order to maximize the outcome of the test campaign.

e. A SEE test plan should be discussed and submitted to the customer defining the test conditions.

f. Board level SEE testing is significantly more complex than at component level. The validation of the test setup in a detailed dry run at least 1 month prior to the SEE test campaign is highly recommended.

g. Tests should be performed according to the detailed information provided in annex 4.

h. The following SEE LET threshold (LETth) acceptance levels should be applied:

1) For any SEE effects (destructive and non-destructive):

   LETth > 38 MeV.cm^2/mg: EEE components or board is accepted

2) For destructive effects with no mitigation possible (inclusive destructive SEL):

   LETth =< 38 MeV.cm^2/mg: EEE component or board should not be used

3) For non-destructive effects (inclusive non-destructive SEL):

   LETth =< 38 MeV.cm^2/mg:
   component or board accepted with mitigation implemented and tested - (see NOTE below), and SEE analysis should be performed for GCR & solar heavy-ions

   LETth < 15 MeV.cm^2/mg:
   Proton test should be performed and additional SEE analysis should be performed for trapped & solar protons.

   NOTE
   When mitigation is implemented, it is recommended to ensure:
   - the good functionality of the mitigation system through SEE testing (e.g. in-the-loop testing during irradiation)
   - as well as demonstrating no loss of functionality of the protected component or module after a large/sufficient number of SEE occurrences.

   NOTE
   SEL can only be considered non-destructive after a SEL test triggering a sufficient number of SEL occurrences and demonstrating full electrical recoverability each time.
   Otherwise SEL is always considered as destructive. It is often not possible to mitigate SEL.
   SEL may also generate latent defects which may potentially degrade the component's reliability.

   NOTE
   The LETth of 15 MeVcm2/mg for performing proton SEE tests is an indicative value.

i. The LETth levels as described in 11.5.2 h. should be revised for EEE components made of a material other than Silicon (i.e. GaAs, GaN, SiC, ...)

j. The effectiveness of any SEL mitigation should be demonstrated during irradiation tests.

11.5.3 ERCB, Equipment Radiation Control Board

a. A specific review, Equipment Radiation Control Board (ERCB), should be implemented before PDR and again before CDR, or in any case as part of EQSR.

b. The ERCB should be held with Space environment, Radiation effects, Design and Systems experts.

c. The documentation expected for the ERCB as a minimum should be
   - information on traceability of components (e.g. a EEE components list or DCL, with all information about radiation sensitivity),
   - evidence of discussions among the experts regarding radiation and design mitigation aspects (this could be tracked on the components list), and
   - circuit design schematics.

d. The ERCB review between the Prime, the Customer and the (sub)contractor should be held at the (sub)contractor premises.

11.6 EEE Procurement aspects

a. EEE components should be procured from official distributors.

b. If it is possible, EEE components should be procured directly from the relevant manufacturers.

c. To achieve the maximum possible level of homogeneity, complete reels of components should be procured.

d. All provisions necessary to determine homogeneity of the procured lots should be practised, e.g.

- Check components marking,
- Check uniformity of visual appearance of packaged components,
- Perform if possible and needed X-ray imaging,
- Perform sample electrical measurements.

e. For COTS components and modules, manufacturers storage conditions should be followed.

f. For COTS EEE components re-lifing, the requirements as per ECSS-Q-ST-60-14 should be followed.

11.7 Application

11.7.1 Data sheets

a. COTS components and module performances declared in the relevant datasheets and critical for the intended design application should be subject to verification by test.

NOTE
The reason for recommendation derives from the typical disclaimers in the datasheets, stating that data and specifications are subject to change without notice. A datasheet is not as reliable as a procurement specification!

11.7.2 De-rating rules

a. For EEE components, the same or higher derating margins should be applied as defined in the ECSS-Q-ST-30-11 and ECSS-Q-ST-60-13.

b. If complete modules are procured, the relevant application ratings (temperature, power, voltage, current) should be respected with margins to be agreed with the customer.

c. PSA is a deliverable document.

11.7.3 Worst case analysis

a. WCA should be a deliverable document, to include components parametric variation with respect to temperature, radiation and ageing.

NOTE
As basis for WCA, use data sheet information and known radiation drifts (see annex 2). In case important parameters drifts are not available, derive them by test on a representative set of samples.

b. Margin on component max/min ratings and performances should be considered in the design in order to account for component parametric drift due to radiation.

NOTE
See Annex 2 for typical parameters affected by radiation for each technology type.

11.7.4 Mitigation techniques

In this section, design and application mitigation techniques to overcome degradation at component level due to radiation or to random failures are explained, at component, module/board and system/subsystem level.

11.7.4.1 Mitigation techniques at component level

11.7.4.1.1 General

a. Filtering of SET (transients) should be performed according to the Worst-case SET templates provided in ECSS-Q-ST-60-15C (table 5-4).

b. Effects of SEL should be taken into account for all devices based on CMOS and BiCMOS technology, including memories.

c. Power cycling should be implemented to mitigate SEL risk in all cases at board or unit level.

NOTE
The effectiveness of power cycling is subject to reference designs where mitigation techniques are adopted and validated. The heritage applies more to the reference design than on the specific component or module.

NOTE
For specific devices, other mitigation techniques can be implemented as explained in section 11.7.4.1.

11.7.4.1.2 Power discrete devices

a. In case power components (silicon MOSFET) are not tested in radiation, the relevant voltage application of should be de-rated as explained in recommendation 10.7.3.1.2.a.

11.7.4.1.3 Digital Components, general

a. For digital components, the mitigation techniques explained in annex 2 should be extensively applied.

11.7.4.1.4 Memories

a. Robust error detection and correction methods (e.g. Reed Solomon) should be used according to the memory type (SRAM, SDRAM, Flash, etc) to mitigate single and multiple upsets (SEU/MBU).

NOTE
The effectiveness of mitigation depends on the memory organization and multi-bit/multi-cell upset behaviour.

b. Hamming ECC should be used for SRAM.

c. Reed-Solomon, or even BCH, ECC should be used for SDRAM, due to the nature of the faults encountered in those memories (SEFI, burst errors).

NOTE
A critical distinction is whether a SEFI requires a power cycle for recovery or whether recovery can be carried out by a reset/reload of mode registers. If power is cycled, all memory contents for die (or module) are lost. This is a distinction between SDRAM and FLASH memories

d. For SRAM memory arrays, scrubbing (periodic refreshing of memory contents) may also be used, to avoid accumulation of errors that could render the ECC algorithms ineffective.

NOTE
The scrubbing period should be adjusted according to the radiation profile of the mission, and the target error rates.

e. CRC should be used for EEPROMs.

NOTE
EEPROMs are commonly used for storage or software images, or parameter sets. With CRC data can be read back immediately after writing to confirm correct completion of write operations. In case of errors detected at read-back, the write operations may just be repeated.

f. Wear levelling should be considered for Flash memories.

NOTE
If not already implemented in the embedded Flash memories control logic, wear levelling should be handled by the end user.

11.7.4.1.5 FPGAs

a. For SRAM-based and Flash-based FPGAs spatial redundancy techniques should be utilized for mitigation against radiation induced SEE in the combinatorial and sequential logic.

NOTE
Local TMR can yield acceptable upset rates when used in Flash-based FPGAs, but is not recommended for SRAM FPGAs as the upset rates may even be worse than with no mitigation in those devices.

Full (or Global) TMR is the strongest method of SEU mitigation for SRAM-based FPGAs, but the skew between the triplicated clocks may be a challenge to manage, and it can reduce the effectiveness of the mitigation.

Distributed TMR is a good compromise between SEU mitigation strength, implementation complexity, and area overheads, and is the recommended TMR scheme for SRAM-based FPGAs.

Designers should try to select the most suitable TMR scheme to meet the error rate requirements in their projects, while keeping effort and area overheads to

minimum (see section A.2.4.2.1.1).

b. Hamming-3 encoding and "safe FSM" options should be used for Finite State Machines, in addition to the TMR used for state vector registers.

c. Depending on the acceptable error rate for the on-chip memories, EDAC should also be used for the on-chip RAM blocks (parity, Hamming, CRC, etc).

d. The configuration memory of SRAM FPGAs should be protected by scrubbing and EDAC: periodic scan and correction of the active configuration memory. Scrubbing can be either

(i) "blind scrubbing", in which case the configuration memory is periodically refreshed without applying EDAC, or

(ii) "readback scrubbing", where the configuration memory is periodically compared with an externally stored "golden reference" version, corrected from possible errors and the corrected results are written back into the configuration memory.

NOTE
The reason is that the configuration memory of SRAM FPGAs is sensitive to SEE.

NOTE
The way that scrubbing and TMR are implemented for FPGAs can have a critical influence on error/outage rates, hence the importance of using a validated approach. Note that a bad mitigation technique can deliver worse results than no mitigation at all, especially if there is no validation by test.

e. An external latch-up protection mechanism should be employed for SRAM FPGAs: detection of current draw above a certain limit, and automatic power cycling.

NOTE
The reason is that most COTS SRAM FPGAs are susceptible to SEL.

f. Depending on the technology, Flash FPGAs may be susceptible to SEL (TBC by the user, info available from FPGA manufacturer), in which case an external latch-up protection mechanism should be used.

NOTE
As examples, the Microsemi SmartFusion2 and IGLOO2 Flash FPGAs are SEL sensitive at heavy ion energy levels ≥24 MeV*cm2/mg [17], but the (RT)-ProASIC3 Flash FPGAs do not experience SEL below 60 MeV*cm2/mg [16].

NOTE
The configuration memory of Flash-based FPGAs is immune to SEE. In Flash-based FPGAs, the memory cells that keep the configuration information (routing and LE/tiles configuration), are Flash based, so they are inherently not susceptible to SEUs/bit flips. This provides a good level of radiation tolerance, since only the logic (sequential and combinational) and the on-chip memories need to be mitigated.

11.7.4.1.6 Microprocessors

Microprocessors can be susceptible to SEU for their internal memories, SEFI for the on-chip functional units (processor core/s), and SEL.

a. The on-chip memories should be protected by ECC: Hamming, CRC for memory blocks (either SW or HW generated, if supported), parity for register files and caches (if supported).

b. External memories should be protected by dedicated ECC (see recommendation 10.7.3.1.3 b).

c. Watchdog timers should be utilised to monitor and detect SEFI, or processor deadlocks.

d. Most COTS microprocessors are susceptible to SEL, so an external latch-up protection mechanism should be used, with detection of current draw above a certain limit, and automatic power cycling.

e. SEL protection logic need to respond in a prompt manner (in TBD ms) after detection of the overcurrent condition to avoid damage to the component.

For resolution of SEFI two alternative approaches are recommended: one utilising a watchdog timer (recommendations f to h), or a simpler method based on periodic reset or power cycling (recommendation i).

f. A watchdog timer should be used to detect SEFIs or deadlock situations, where the normal execution flow of the processor is interrupted.

g. The watchdog should be periodically refreshed by the user application.

h. If the watchdog expires, an interrupt is raised and the device is reset.

> NOTE
> The watchdog expiration condition may also be managed by an external supervisor, responsible for resetting or power cycling the device. This may also be the responsibility of the main platform controller (e.g. OBC).

i. To resolve SEFI (and possibly SEL) a microprocessor may be periodically reset, or power cycled.

> NOTE
> Periodic reset can help avoid deadlocks due to SEFI, and periodic power cycling may help control SEL effects. However, this cannot be considered as a reliable SEL protection mechanism: SEL can be a destructive event, and the SEL protection logic need to respond in a prompt manner after detection of the overcurrent condition to avoid damage to the component (as mentioned in recommendation 11.7.4.1.6.h). Periodic power cycling may not be of sufficiently high frequency to guarantee proper protection. On the other hand, a high power-cycling frequency would not be practical and might have too high an impact on system availability.
> This SEL/SEFI mitigation option is assessed on a mission basis by the designer, based on availability, reliability, and power consumption requirements.

j. To control destructive effects of SEL, local overcurrent protection mechanisms should be used if repetition frequency of periodic power cycling cannot be made fast enough to avoid destructive effects.

11.7.4.1.7 Microcontrollers

For microcontrollers used in module, equipment, subsystem or system of criticality category Q_1, the recommendations listed in section 10.7.3.1.6 apply, but the recommendations mentioned as optional ("may") should be considered as fully applicable, even as major

(“should”).

11.7.4.1.8 Programmable Systems-on-a-Chip (SoC)

Since SoC are a combination of FPGAs with embedded microprocessors, the recommended SEE mitigation techniques to be applied are a combination of the recommendations on FPGAs (according to FPGA type, SRAM or Flash), microprocessors and memories (see sections 10.7.3.1.3, 10.7.3.1.4, 10.7.3.1.5, and also A2.4.2.6).

A simple form of error mitigation at software level is duplication the execution of certain instructions and compare the results. If a discrepancy is detected between the results, an exception may be raised and the program backtracked to a previous check-point.

11.7.4.2 Mitigation techniques at module/board level.

a. The same mitigation techniques should be applied that have been presented for category Q2 (see para 10.7.3.2) with the following differences and additions.

b. Additional localised shielding may be utilized at module level to provide increase protection of specific, radiation sensitive components.

c. For modules and boards equipped with digital components, the mitigation techniques explained in annex 2 should be extensively applied.

d. Power cycling provisions to any complex digital circuit to resolve SEL and SEFI should be provided.

e. Error detection and correction provisions should be provided in memories against SET, SEU.

f. Current limitation, detection and power reset provisions should be used to survive SEL (latch-up) in EEE components/boards, especially when including SRAM memories.

g. For effective SEL mitigation the response time for SEL detection should be limited, due to the potentially destructive nature of the latch-up event.

    NOTE
    There are a few devices where SEL happens too rapidly for any protection circuit to kick in.

Also, the more rapid the response, the more likely it is to suffer false resets due to transients.

h. To increase SEL protection levels the SEL protection mechanisms should be implemented locally within the module hosting the SEL sensitive part(s), to reduce latency in the detection and management of the SEL (latch-up event detection and power cycling).

i. Critical functions should be provided with redundancy and voting.

j. If voters are used, they should be inherently robust to SEE.

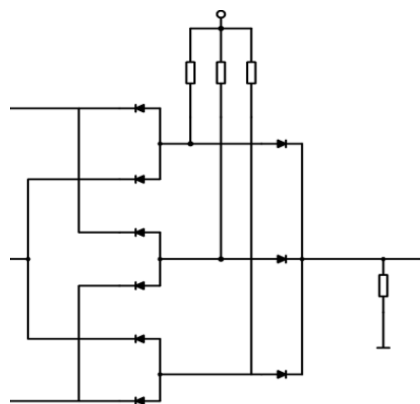


Figure 5, reliable TMR voter by diodes

11.7.4.3 Mitigation techniques at system/subsystem level.

a. The same mitigation techniques should be applied that have been presented for category Q2 (see para 10.7.3.3) with the following differences and additions.

b. For systems and subsystems equipped with digital components, the mitigation techniques explained in annex 2 should be extensively applied.

c. In case of redundant systems, provide timely switching from main to redundant back-up systems in order to meet availability requirements.

It is important to collect as much in-flight feedback as possible for each mission, for COTS-based components/modules/systems where ground radiation verification, testing and qualification has not been performed.

d. A measure, monitor, management approach should be used using radiation monitors and relevant telemetry channels.

NOTE
Compliance to recommendation d allows in-flight environment data to be recorded in order to build up in-flight component/module/system heritage and provide real-time spacecraft radiation 'health' data (much like temperature sensors use used to track thermal aspects).).
It is also important for establishment of heritage and validation of test and qualification procedures.
If something goes wrong the actual reason can be determined, and lessons learned can be created and fed back into the RHA approach for the next mission.
If the spacecraft receives less radiation than designed for, the lifetime may be extended.

11.7.5 Reference application circuits

It is recommended to identify, collect and maintain reference application circuits for specific EEE components, to have a clear and unambiguous reference for radiation tests including design mitigation techniques at circuit level if applicable.

a. If available, reference application circuits should be applied.

11.7.6 Modules

a. Modules should not contain components or materials from forbidden lists (see section 11.3).

b. Absence of forbidden components and materials should be assured through review of parts and material lists, or by confirmation from supplier supported by visual inspection.

c. Modules should contain design mitigation provisions as per section 11.7.4.

d. Modules should use reference circuits around specific EEE components, as indicated in section 11.7.5.

e. For modules and boards, radiation verification is recommended as per section 11.5.

NOTE
See annex 4.

Aim at testing the same module as the flight board (same procurement batch, same manufacturer, possibly same date code, same design).

f. Any power supply module, and specifically commercial power supply modules (black box approach) should not be used.

g. For modules, CoC should be provided.

h. Screening provisions to ensure modules reliability (thermal cycling, burn in), LAT endurance (life test), and LAT thermo-mechanical tests should be implemented.

NOTE
An approach based on HALT and HASS may be proposed.

Also for modules a distinction has to be made between designed and procured ones.

12 CRITICALITY CATEGORY Q0

12.1 Perimeter of Applications

All space applications.

12.2 RAMS

a. Safety should be ensured according to the ECSS-Q-ST-40.

b. Dependability should be ensured according to the ECSS-Q-ST-30.

c. Failure modes, effects, (and criticality analysis) should be conducted according to ECSS-Q-ST-30-02.

d. Availability should be ensured according to ECSS-Q-ST-30-09.

12.3 Materials and processes

a. Materials, mechanical parts and processes should comply with ECSS-Q-ST-70 [S12] including all lower level standards [S13], [S14], [S15], [S16] (as tailored in the applicable PA requirements).

b. Management of the risk associated with the use of pure Sn finishes should comply to GEIA-STD-0005-02 [S04] level 2C.

c. Contamination and cleanliness control should comply with ECSS-Q-ST-70-01C [S13].

d. Outgassing control should comply with ECSS-Q-ST-70-02 [S17].

e. PCB design should comply to ECSS-Q-ST-70-12C [S15].

f. Qualification and procurement of PCBs should comply to ECSS-Q-ST-70-60C [S16].

g. In case of non-compliance to ECSS-Q-ST-70-60 [S16] or in case of procurement as per IPC-6012ES [S06], PCBs should be project qualified under RFA as per chapter 7.7.2 of ECSS-Q-ST-70-60 [S16].

NOTE
This approach is used for High Density Interconnect technology that is typically needed for COTS Area Array Devices, among others.

h. Assembly processes for Q0 should comply to ECSS-Q-ST-70-38C [S11].

i. Assembly processes verification for Q0 class 3 should comply with the approaches defined in Annex 6.

12.4 EEE components

a. ECSS-Q-ST-60 should apply (Class defined in PA requirements), including lower-level standards as for example:
   1. Commercial electrical, electronic and electromechanical (EEE) components should comply with ECSS-Q-ST-60-13.
   2. Re-lifing should comply with ECSS-Q-ST-60-14.

12.5 Radiation

a. The radiation hardness assurance should be conducted according to the ECSS-Q-ST-60-15.

12.6 EEE Procurement aspects

a. Traceability of EEE components should be ensured between the components subjected to evaluation, screening and lot tests on ground and the ones that are used for flight purposes.

12.7 Application

12.7.1 Data sheets

a. COTS components and module performances declared in the relevant datasheets and critical for the intended design application should be subject to verification by test.

NOTE
The reason for recommendation derives from the typical disclaimers in the datasheets, stating that data and specifications are subject to change without notice. A datasheet is not as reliable as a procurement specification!

12.7.2 De-rating rules

a. For EEE components, the same or higher derating margins should be applied as defined in the ECSS-Q-ST-30-11 and ECSS-Q-ST-60-13.

b. PSA is a deliverable document.

12.7.3 Worst case analysis

a. WCA should comply with the recommendations provided in ECSS-Q-HB-30-01.

b. WCA should be a deliverable document, to include components parametric variation with respect to temperature, radiation and ageing.

NOTE
As basis for WCA, use data sheet information and known radiation drifts (see annex 2). In case important parameters drifts are not available, derive them by test on a representative set of samples.

c. Margin on component max/min ratings and performances should be considered in the design in order to account for component parametric drift due to radiation.

NOTE
See Annex 2 for typical parameters affected by radiation for each technology type.

12.7.4 Mitigation techniques

a. Design and application mitigation techniques to overcome degradation at component level due to radiation or to random failures should be implemented as generally explained in annex 2, at component, module/board and system/subsystem level.

b. For Flash-based FPGAs: reprogramming should be avoided during flight, due to the possible probability of failures and errors from radiation induced SEE in the programming logic.

NOTE
Refer to section A2.4.2.4.1.

12.7.5 Reference application circuits

It is recommended to identify, collect and maintain reference application circuits for specific EEE components, so as to have a clear and unambiguous reference for radiation tests including design mitigation techniques at circuit level if applicable.

a. If available, reference application circuits should be applied.

12.7.6 Modules

In criticality category Q0, the adoption of COTS EEE components is controlled at EEE components only and complete ECSS standards envelope applies.

NOTE
The qualification or acceptance of COTS "black box" modules or boards, without qualification or acceptance of their constituent parts (EEE components), is not allowed in Q0.

13 HOW TO ATTRIBUTE CRITICALITY CATEGORY

Let us start from the definition of COTS components and modules.
We are considering commercial electronic **components and modules** readily available and not manufactured, inspected or tested in accordance with military or space standards: they are typically manufactured, inspected and tested according to either internal manufacturers rules, or to standards (for example, AEC-Q ones) that have not been drafted specifically to cover space applications.

While MIL and ECSS specifications focus on EEE components testing, COTS quality is based on the application of Statistical Process Control (SPC). SPC is typically suited to large production volumes. COTS components and modules get continuous improvement thanks to SPC, but on the other side SPC, as applied for mass production of terrestrial components, gives no guarantees against radiation performance.

COTS components and modules may or may not be suitable to space environment, space conditions and requested lifetime: even in case they have been developed, manufactured and qualified with stringent terrestrial specifications, they might not comply with the global, minimum space requirements relevant to:

- radiation (which is not tested for terrestrial application and probably the main failure mode of EEE components).
- thermal and mechanical environmental conditions, which is tested for in terrestrial applications but not necessarily enveloping the environment of space applications.
- acceptance criteria (workmanship and after test), which are equally specified in terrestrial conditions, but which may show significant relaxation of quality with respect to space standards.
- electrical reliability. Continuity and insulation tests are routinely performed on terrestrial applications. The COTS space approach should ensure that these tests are implemented in the (procurement or qualification) specifications.
- Outgassing.
- Forbidden and not allowed materials.

It is clear that the assessment of their suitability for space use will imply a dedicated evaluation, a possible screening, and acceptance test at lot level.

This is in fact the prescription provided by ECSS-Q-ST-60-13, the relevant (summarizing) annex G being provided in Figure 6.

ECSS-Q-ST-60-13C
21 October 2013

Annex G (informative) Difference between the three classes

	CLASS 1	CLASS 2	CLASS 3
EVALUATION	COMPLETE - Construction analysis - Electrical charact. (3T+10°C margin) - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C + DPA - Precond + 500T/C -55°C/+125°C - Radiation evaluation (TID, SEE)	COMPLETE - Construction analysis - Electrical charact. (3T+10°C margin) - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C + DPA - Precond + 500T/C -55°C/+125°C - Radiation evaluation (TID, SEE)	LIMITED - Construction analysis - Radiation evaluation (TID, SEE)
JD (Justification Doc)	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and test - Lot acceptance tests - Radiation hardness data and RVT	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and test - Lot acceptance tests - Radiation hardness data and RVT DATA COLLECTED *(EFR, lifetest, thermal cycling)* used for screening reduction	DATA COLLECTION - Component manufacturer data - Approval status - Evaluation tests - Procurement inspection and tests - Lot acceptance tests - Radiation hardness data and RVT DATA COLLECTED *(lifetest, HAST, thermal cycling)* used for lot test reduction
CUSTOMER PRECAP	no	no	no
SCREENING	COMPLETE - X-rays - Serialisation - 10T/C -55°C/+125°C - PIND test (if applicable) - Initial electrical test @ 25°C - Dynamic burn-in 240h-125°C - Final electrical test @ 3T° - PDA (5%) - Hermeticity (if applicable) - External visual inspection	LIMITED (if data collected) - PIND test (if applicable) - Hermeticity (if applicable) + If no data collected (see JD) - Serialisation - 10T/C -55°C/+125°C - Initial electrical test @ 25°C - Dynamic burn-in 160h-125°C - Final electrical test @ 3T° - PDA (5%) - External visual inspection	LIMITED - PIND test (if applicable) - Hermeticity (if applicable)
LOT TEST (on screened parts) (when applicable)	COMPLETE - Construction analysis - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 2000h-125°C - Precond + 100T/C -55°C/+125°C - RVT (Radiation Verification test)	COMPLETE (but LT 1000h) - Construction analysis - Meca shocks + Vib. + Const. Acc. *(for cavity package)* - Precond + HAST 96h or THB 1000h - Lifetest 1000h-125°C - Precond + 100T/C -55°C/+125°C *(may be waived i.a.w. application)* - RVT (Radiation Verification test)	LIMITED (if data collected) - Construction analysis - RVT (Radiation Verification test) + If no data collected (see JD) - Precond + HAST 96h or THB 1000h - Lifetest 1000h-125°C - Precond + 100T/C -55°C/+125°C
CUSTOMER BUY-OFF	no (replaced by incoming)	no (replaced by incoming)	no (replaced by incoming)
INCOMING	yes	yes	yes

97

Figure 6, ECSS-Q-ST-60-13C, summary (annex G)

The approach provided in Figure 6 implicitly relies on a substantial homogeneity of the COTS components that are subjected to evaluation, screening and (lot) test: if such

homogeneity cannot be reasonably postulated, it does not make too much sense to spend such effort, because it will not guarantee that what flies is the same component that passed the evaluation, screening or test.

The important remark at this point is of practical nature: in absence of large procurement lots of COTS components it might not be possible to count on their homogeneity in spite of aiming at it. This might be the most common case for a components or modules procurement if it is limited to a single mission, where components might just be procured through distributors and not through direct contact with the relevant manufacturers. Additionally, guaranteeing lot homogeneity for small procurement lots is in contradiction with the cost advantage of the COTS solution, and it should only be pursued if COTS components and modules are used instead of hi-rel ones for performances improvement.

The implications of (alleged) lot uniformity suggest the use in two main application fields (see Figure 7).

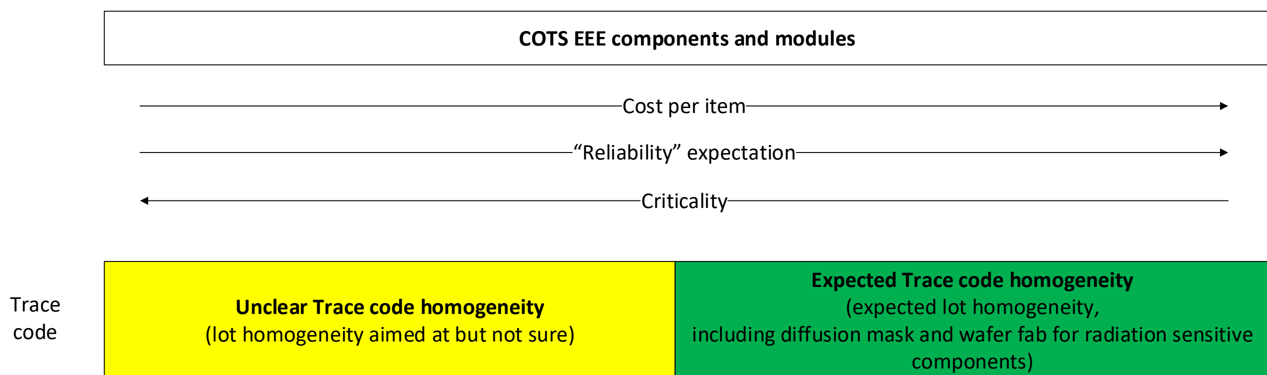


Figure 7, COTS & homogeneity of the procured lot

On the right-hand side, the **green** application field identifies the situation for those COTS components where the procured lot is expected to be homogeneous (same expected behavior from components tested on ground and used for flight).
Such area is already provided with a relevant set of consistent requirements for the maximum expected reliability (chances of success in space).
We might define it as "*normative*" area: the requirements are the ones laid down in the ECSS-Q-ST-60-13 or in equivalent standards.

On the left-hand side, the **yellow** application field identifies the situation for those COTS components for which it is unclear if the procured lot is homogeneous, and therefore the components used for flight might not behave as the ones tested on ground.

In any case, the possible traceability/homogeneity difference between Normative and Informative area are definitively driven by budget constraints: the inspiring principle is

that traceability/homogeneity is always aimed at, within the cost constraints of the relevant development.

In spite of the expected higher criticality and reduced certified reliability, there are at least a couple of reasons to identify a possible yellow environment besides the green one.
A first reason to enter the yellow environment is **cost convenience**: it is clear that the expected reliability is not the same as the one provided by the green area, but the cost per component is expected to be far lower (due to the savings on full evaluation, screening, lot acceptance and the avoidance of lot rejections).
The second reason is that **it allows the evaluation of different and promising technologies at different integration level** (from material and processes to system level through equipment, subsystem, system) **in the relevant environment**.

It allows wide scale learning and progress, at the price of a more remarked risk-taking attitude: at the moment is not the subject of a prescriptive set of requirements but more reasonably of a set of guidelines, elaborated by each domain expert.

Clearly, the lack of complete “knowledge” at component level is partially resolved by adoption of relevant and effective mitigation techniques as described in the other sections of this document.

We can conveniently refer the yellow area as “informative” due to the present lack of normative coverage for it: it is clear that standard requirement might in future be defined for it, possibly based on the present guideline.

The approach as discussed so far is summarized in Figure 8.

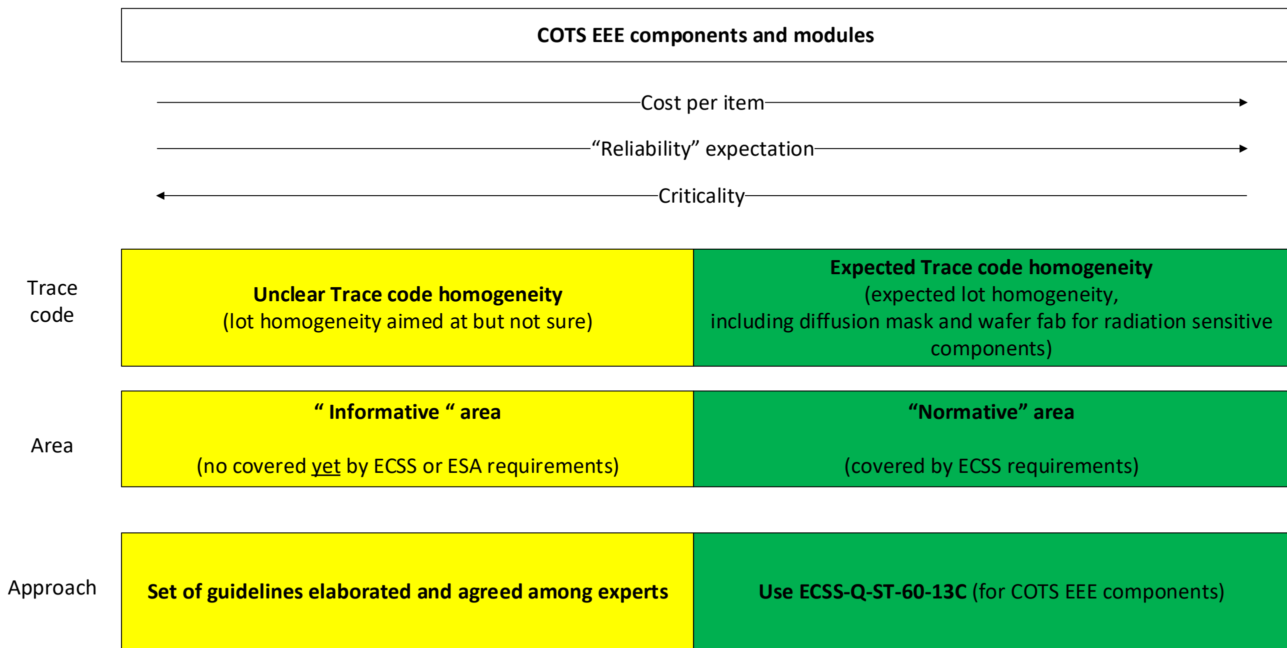


Figure 8, COTS, lot homogeneity & areas

It should be clear that for cost advantage purposes (linked or not to performance advantages or lack of Hi-Rel options) it is more effective to enter the yellow area, while for performance advantages or lack of Hi-Rel options (with no cost advantage objectives) the green area is most suited.

It is convenient to define "minimum effort" guidelines for evaluating lot homogeneity, such to define the best "entry" point into the proposed approach (see section 14).

Note that lot homogeneity seems definitively easier to achieve for large, single procurement that on smaller ones, especially because it might enable a privileged relationship to specific manufacturers according to the mentioned "economy of scale".

At this point, the different criticality categories can be identified. To this purpose, see Figure 9.

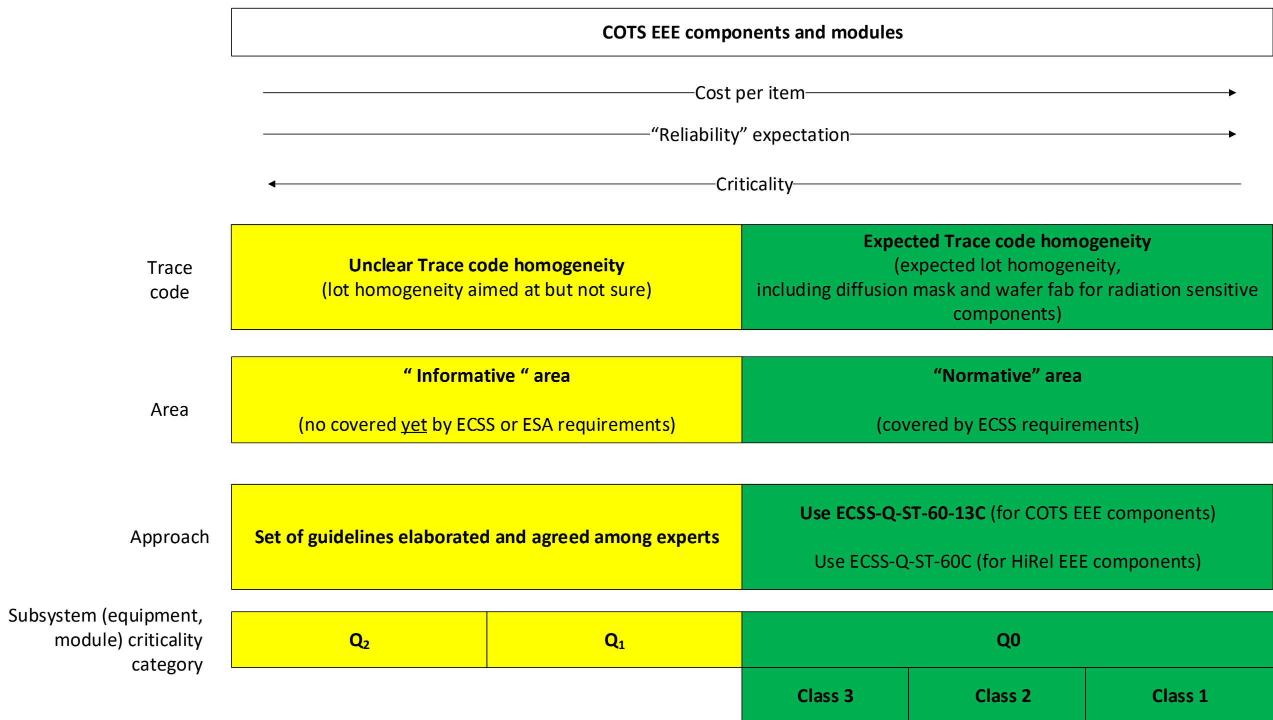


Figure 9, COTS, overall approach

It is important to remember that

- the criticality categories are relevant to modules, equipment, subsystems and not to the mission;
- that a mission of any criticality can embark modules, equipment, subsystems of any criticality category, depending on the criticality of such item.

The relevant criticality categories are described in the previous sections 10 to 12, in order of decreasing risk profile.

The perimeter (boundaries) of application of each criticality category are provided in the relevant sub-sections (10.1, 11.1, and 12.1).

Class Q_2 is suitable for items (module, equipment, subsystem, system) for which the highest risk of failure can be accepted.
It is suitable for applications where very minor total radiation dose is expected (<5Krad) and for exposure to space conditions for less than few months, typically one year maximum.

Class Q_1 is suitable for items (module, equipment, subsystem, system) for which medium failure probability can be accepted.
It is suitable for applications where intermediate levels of total radiation dose is expected (indicatively up to 10-15 Krad) and for exposure to space conditions for less than 5 years.

For class Q_0, the ECSS-Q-ST-60-13 identifies three (sub) EEE classes, 1 to 3 in order of increasing risk taking and decreasing assurance.

The differentiation of (sub)classes within class Q_0, is explained with the reason of giving three options allowing the most suitable balance between failure probability and cost to the possible user.
The environmental perimeter of application does not change among the three options (no prescribed limits for radiation), so the selection is purely determined on the basis of risk taking and budget constraints.

- For modules, equipment, subsystems of major ESA missions, class 1 components are mostly used, even though higher risk options (including yellow area ones) might be adopted for modules, equipment, subsystems of less essential nature according to mission objectives.

- For modules, equipment, subsystems of medium-profile ESA missions, class 2 components are mostly used, even though higher risk options (including yellow area ones) might be adopted for modules, equipment, subsystems of less essential nature according to mission objectives.

- For modules, equipment, subsystems of low-profile ESA missions, class 3 components are mostly used, even though higher risk options (including yellow area ones) might be adopted for modules, equipment, subsystems of less essential nature according to mission objectives.

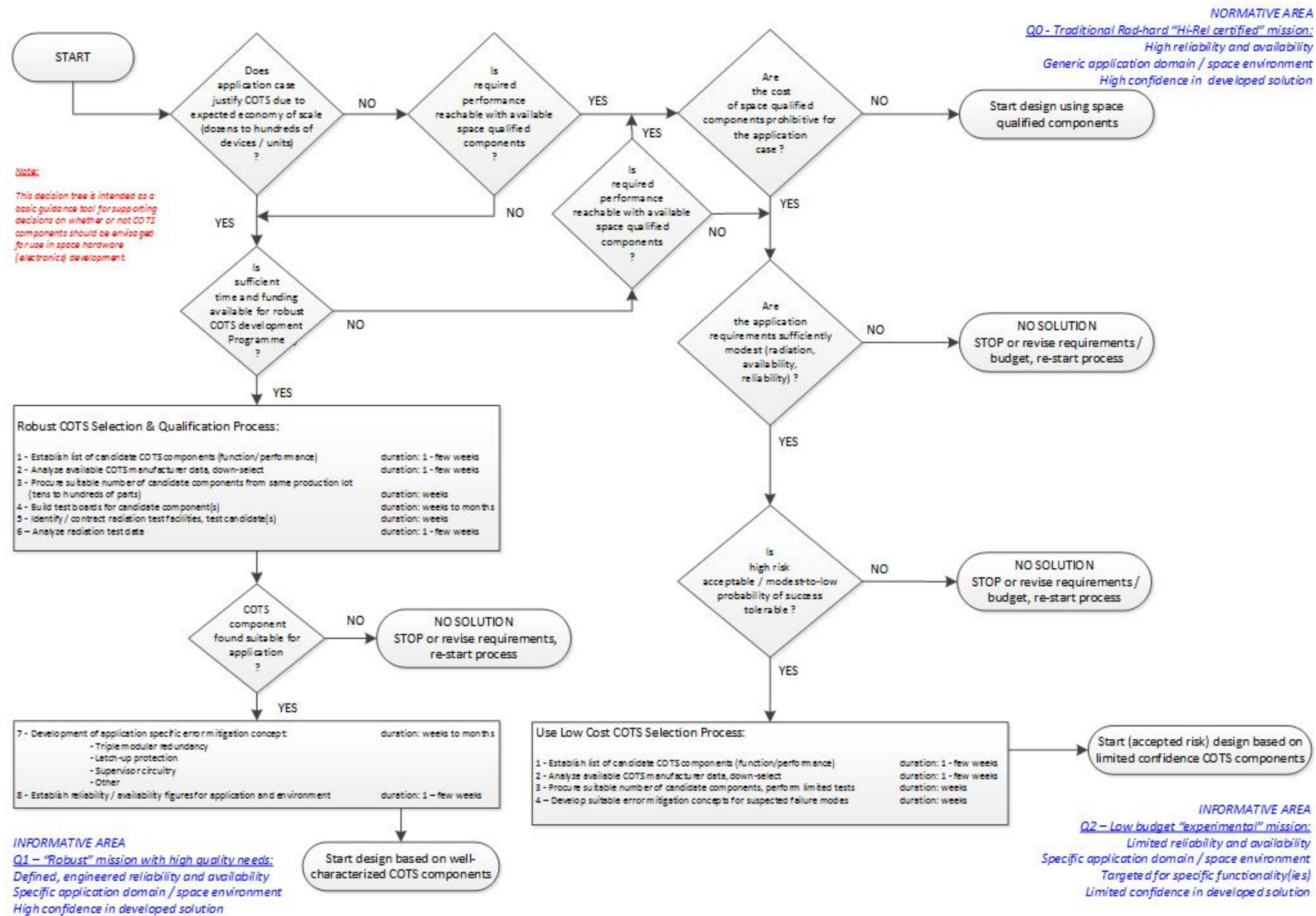
Generally speaking, note that

- the criticality of an equipment is defined by the lowest class of the components, or modules, used in it;
- an equipment of a given criticality class can employ components and modules of higher classes.

13.1 Responsibilities

The attribution of minimum criticality category to modules, equipment, subsystems for a given mission is the outcome of an agreement between the Agency Program Management and the relevant contractor.

13.2 How to attribute criticality category, flow chart



14 GUIDELINES FOR EVALUATING LOT HOMOGENEITY

14.1 General

a. From general point of view, the homogeneity of the procured lot should aim at determining (as applicable) data code, die revision, wafer lot, wafer fab, assembly location.

b. The homogeneity of the procured lot can be evaluated performing

- Documentation and supplier check
- Inspection (marking, appearance, other)
- Construction analysis and/or DPA (for die revision and overall construction)
- Radiography

NOTE
Consider that the measures provided in the recommendation 14.1b might still not be sufficient for radiation tolerance purposes.

14.2 Radiation

a. Statistical checks should be performed on samples of the procured lot depending on its size if homogeneity cannot be confirmed.

NOTE
As an indication, at least 10% of the procured lot component should be tested in total dose, with a minimum of 30 pieces. For more details, see [19], [20].

15 FEEDBACK FROM SPACE APPLICATION

It is of high importance to get application feedback from mission operation to improve

- actual behavior of COTS EEE components in actual environment (especially in case no radiation campaign has been performed on ground);
- understanding that correct mitigation measures have been implemented (validation of mitigation measures and improvement of their "heritage" status);
- understanding if the recommended quality class (for PCB and assembly) is fit for purpose.

To get such feedback it is important to be sure of the environment actually encountered, so it is of paramount importance to use radiation monitors, to ensure sufficient telemetry channels are provided and the relevant data are actually analysed.

NOTE
Especially for SEE, flight data on one or a few EEE components may not give statistically significant results. For example, no SEL on one EEE components for several years does not give a large guarantee.

NOTE
Note that each environment (GEO, polar LEO, etc.) pose different level of risk with respect to cosmic rays.

16 REVIEWS OF ITEMS CONTAINING COTS EEE COMPONENTS AND MODULES IN CATEGORY Q1 AND Q2

This section applies only to items containing EEE components and modules of criticality category Q_2 and Q_1.

a. Items containing COTS EEE components and modules should be matter of detailed expert review on the basis of application perimeter (function and relevant criticality, type of mission, environmental and RAMS requirements).

b. Such review should be based on

- Parts Approval Document and Justification Document as applicable
- Declared Component List
- Declared Materials and Processes lists
- Detailed Circuit Diagrams and Parts Lists
- Details on used mitigation techniques (HW and SW)
- Applicable analyses (radiation, FMECA, PSA, WCA if available)

according to the details provided for each criticality category.

c. To have the most efficient and reliable outcome of the COTS EEE components and module review, such review should be conducted as a concurrent engineering effort among the different experts involved (components, material and processes, electrical, RAMS, radiation) and as a peer-to-peer review.

d. The review of recurrent items containing COTS EEE components and modules might be lighter after the first use, especially if there is evidence of the effectiveness of reference designs and relevant mitigation techniques with respect to flight operation under same or similar environment.

e. An information tool should be conveniently used to store and then access and use information on COTS components and modules, possibly arranged as a real database (with searchable fields and tags) in order to get quick and relevant response.

NOTE
Such tool can allow easy and wide access to COTS components databases of CPPAs run by ESA.

17 THE CONCEPT OF SAFETY BARRIER FOR EQUIPMENT OF HIGHER CRITICALITY CLASS

One interesting option to use COTS EEE components in space is to allow their use in equipment of more experimental or innovative nature within a space vehicle that is generally providing a more reliable platform.
For example, to use an equipment of criticality class Q_2 (or Q_1) within a satellite of general criticality class Q_0 (based on COTS or even on conventional space grade components).

Such an opportunity seems very interesting because it allows to use of the dependable telemetry chains of higher mission classes to have reliable information on COTS-based designs functionality and performance, and at the same time the expansion of the possibility to use and fly promising COTS component and modules with limited budget and time impacts.

From the other point of view, it is anyhow necessary to ensure that the presence of such equipment does not jeopardize the reliability of the hosting platform, hence it is a general recommendation and a wise choice to adopt a "safety barrier" interface between the platform and the said equipment (see Figure 10).

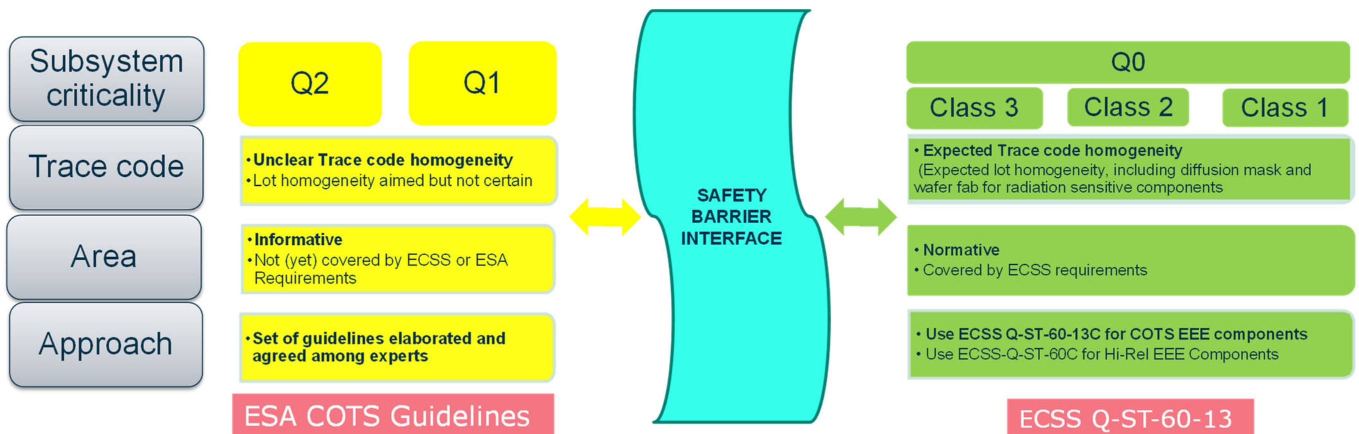


Figure 10, Safety barrier interface

Such safety barrier implements the so called do not harm principle: it consists of a reliable, well designed and validated set of (electrical, mechanical or thermal) provisions in the interface between equipment of criticality classes Q_2 or Q_1 and of Q_0.
Its scope is to avoid that any type of failure can propagate from the item of criticality class Q_2 or Q_1 to any equipment of criticality class Q_0 (through power, signal lines, thermal or mechanical interfaces).

From electrical standpoint the safety measures entail the adoption of fault emission and fault tolerance of the interfaces.

Fault emission and fault tolerance are properties of the interface, affecting voltage and/or current in abnormal (failure) conditions: the fault tolerance of the connected interface shall always be equal or exceed the fault emission of the interface itself (see Figure 12 and Figure 11).

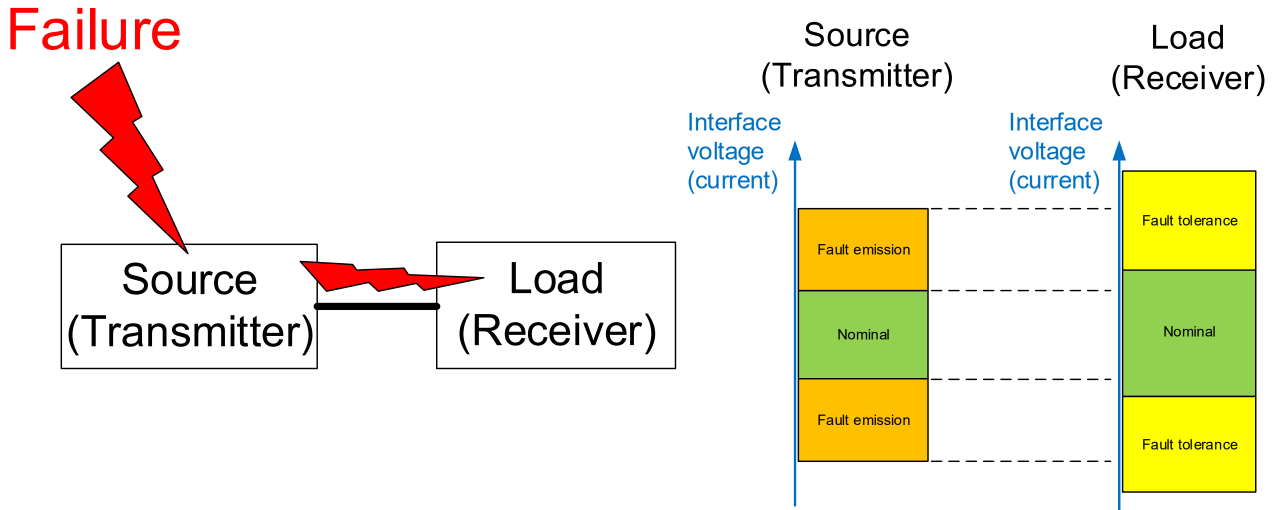


Figure 12, Fault emission and fault tolerance (following failure on the source or transmitter)

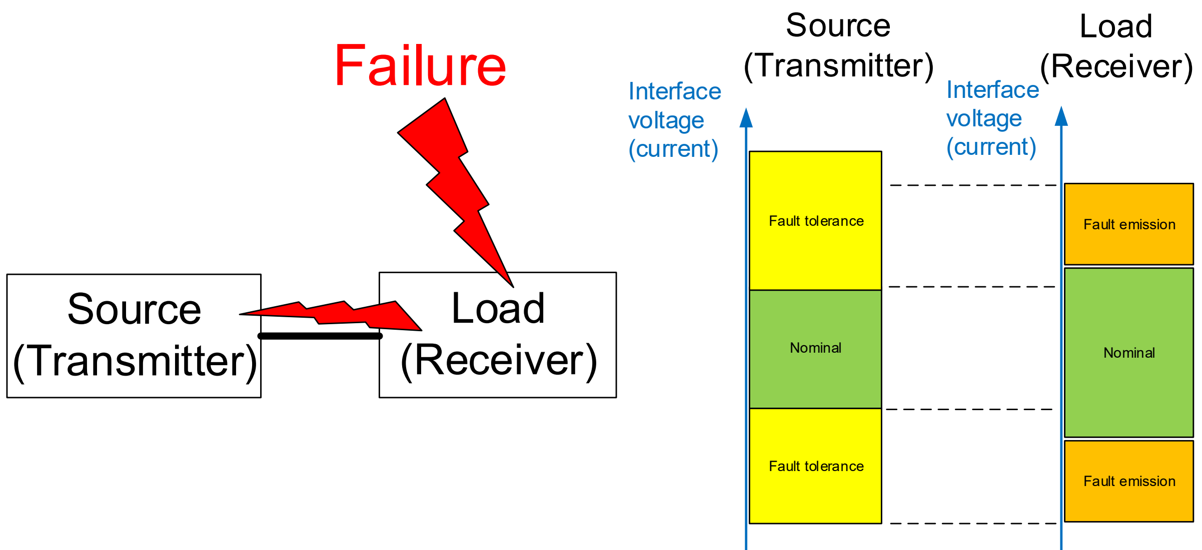


Figure 11, Fault emission and fault tolerance (following failure on the load or receiver)

Some examples of electrical safety barrier provisions for power and signal lines are provided in Annex 7.
Note that some electrical provision (like the distribution of power lines by latching current limiters) can also take care of potential thermal failure propagation patterns. For more details on power distribution based on latching current limiters, see [30] and [S21].

ANNEX 1, RECOMMENDED APPLICATION BOUNDARIES OF CRITICALITY CATEGORIES

Area	Criticality Category	TIDL limit	*Recommended Mission Application*	*Time limit*
Normative	**Q0**	n/a	*All*	*N/A*
Informative	**Q1**	10-15 Krad (just indicative, see note)	All, **but** depending on the SEE test and validation performed (heavy ions, protons or both depending on the mission)	up to 5 years
	Q2	5 Krad (just indicative, see note)	Low LEO orbits (typically <1000Km), if availability is not required through South Atlantic Anomaly and poles (e.g. the equipment can be switched OFF there) Outer space regions far from stars and radiative planets (e.g. Jupiter) if the equipment is switched ON for reduced time (esp. to reduce the risk of destructive events due to heavy ions or protons)	up to 1 year

- The TIDL limit for class Q2 is not arbitrary, but it derives from the simple consideration that many of the common EEE technologies (apart few cases such as electro-optical, bipolar, BiCMOS,ADCs, DACs, voltage regulators, power MOSFET, flash memories) are able to withstand a radiation level of 5Krad without major degradation impairing their use. For details, refer to section 10.5.1.
- The TIDL limit for Q1 is only indicative, it depends on the individual mission radiation environment and equipment analysis.considering that homogeneity of the procured lot in Q1 is not certain. The TIDL limit is formulated to keep risk under reasonable control under these circumstances. Higher TIDL limits can be pursued in Q1 but considering that despite the recommended radiation testing there is still the risk to fly something different than what was tested on ground. For details, refer to section 10.5.1.
- Most of the limitations for Q2 and Q1 derive from environmental considerations relative to SEE (heavy ions and protons), especially of destructive nature (SEL with destructive effects, SEGR, SEB).
- Even if parts are switched off, they will still receive a radiation dose (TIDL) that may affect their operation.
- Recommended time limit are based on the uncertainty in correlating the results of Tin whiskers susceptibility test (JSD201) and the lifetime of the application.
- Most of anomalies in space equipment induced by radiation are due to destructive heavy ion effects, and it may be far more critical than TID or TNID effects for short missions

ANNEX 2, RADIATION MITIGATION TECHNIQUES

Note that the mitigation techniques explained in this annex
1. are not necessarily exhaustive, and
2. are generally valid for all criticality categories.

A2.1 Potentially radiation sensitive EEE components

- For TID, see table 5-1 of ECSS-Q-ST-60-15C:

Table A2-1: EEE component families potentially sensitive to TID

EEE component family	Sub family	TIDL
Diodes	Voltage reference, Zener	all
	Switching, rectifier, Schottky	> 300 krad-Si eq.
Diodes microwave		> 300 krad-Si eq.
Integrated Circuits		all
GaAs Integrated Circuits		> 300 krad-Si eq.
Oscillators (hybrids)		all
Charge Coupled devices (CCD)		all
Opto discrete devices, Photodiodes, LED, Phototransistors, Opto couplers		all
Transistors	Bipolar	all
	MOSFET (including Si NMOS, Si PMOS)	all
	HEMT (including p-GaN HEMT and GaN MISHEMT): threshold voltage, drain leakage, gate leakage and ON serial resistance	all
GaAs Transistors		> 300 krad-Si eq.
Hybrids containing active EEE components		all

- For TNID, see table 5-2 of ECSS-Q-ST-60-15C.

Table A2-2: List of EEE component families potentially sensitive to TNID

Family	Sub-Family	TNIDL
CCD, CMOS APS, opto discrete devices	all	all
Integrated circuits	Silicon monolithic bipolar or BiCMOS	> $2x10^{11}$ p/cm² 50 MeV equivalent proton fluence
Diodes	Zener Low leakage Voltage reference	> $2x10^{11}$ p/cm² 50 MeV equivalent proton fluence
Transistor	Low power NPN Low power PNP High power NPN High power PNP	> $2x10^{11}$ p/cm² 50 MeV equivalent proton fluence
	HEMT (including p-GaN HEMT and GaN MISHEMT): SEB, SEGR, gate leakage	TBD

- For SEE, see table 5-3 of ECSS-Q-ST-60-15C.

Table A2-3: List of EEE component families potentially sensitive to SEE

Family	Sub-family
Integrated Circuits	all
Integrated Circuits Microwave	all
Transistors	MOSFET (including Si NMOS, Si PMOS)
	HEMT (including primarily MISHEMT and possibly p-GaN HEMT): SEB, SEGR, gate leakage
	TBD
Transistors Microwave	all
CCD, CMOS APS, opto discrete devices	all

On the basis of recent experience, also Si and SiC diodes should be added to table A2-3.

For possible single event effects as a function of component technology and family, see Table 1 at p.47.

A2.2 Generic radiation mitigation techniques, TID

A2.2.1 Diodes

- Only potential issue for high accuracy (Vz < 1%) reference/Zener diodes exposed to high doses > 100krad(Si).

A2.2.2 Integrated circuits

A2.2.2.1 Digital logic

- Take into account of additional increase in supply current
- Consider minor additional drifts on input voltage high and low threshold levels
- Consider medium additional drifts on output voltage high and low drive levels
- Consider major additional drifts on output source and sink currents
- Consider major additional drifts on input/output delays and rise and fall times

A2.2.2.2 FPGAs

TID performance of Flash FPGAs (e.g. Microchip ProASIC3) can be increased via reprogramming. After an exposure to a total dose of up to 20 Krad, it was demonstrated that the device was “annealed” to a certain extent after one reprogramming cycle. In essence the effective TID performance of a ProASIC3 FPGA could be nearly doubled, from 20Krad to nearly 40Krad, after 1 or 2 reprogramming cycles.
Reprogramming in flight could be an attractive solution for these components, however the sensitivity of the programming circuitry (charge pump) during programming should also be taken into account: a destructive SEE in the charge pump could disable the reprogrammability of the FPGA.

Microchip FPGA design tools enable the designer to enter TID levels as design parameters. The design and timing analysis reports are then automatically adjusted accordingly. If the FPGA vendors tools do not provide this feature (timing derating analysis based on TID levels), a timing margin of 15-20% is applied during the synthesis and place-and-route phases should provide sufficient margin to cover possible TID performance derating of the device.

A2.2.2.3 Memories (SRAM, SDRAM, NAND-FLASH, EEPROM)

- Consider additional degradation of retention time (due to increase of leakage current in the memory cells)
- For Flash memories: power down redundant banks to to reduce degradation in the control circuitry and charge pump.
- For SDRAM, there is minimal impact of TID for the target applications (for radiation levels approximately to 10Krad).
- Higher dosages may result in stuck-bits and higher power consumption (TBC).

Annealing effects are expected when components are unbiased.

A2.2.2.4 Bandgap references

- Consider additional degradation of regulated voltage
- Consider that commercial voltage references may work well in Electron induced TID but drastically degrade if TNID is also present

A2.2.2.5 Operational amplifiers and comparators

- Consider additional increase of input offset voltage, input bias and offset currents
- To reduce effects of input bias current, make such that resistance seen from the inverting and non-inverting inputs is almost equal
- To reduce effects of input offset current, make such that resistance seen from the inverting and non-inverting inputs is small
- To reduce the effects of input offset voltage, use the operational amplifier only with low amplification factor
- Consider additional drifts of output high and low voltage levels
- Consider additional increase of supply current
- Consider potential decrease of open loop gain and of gain-bandwidth product
- Consider potential worsening of Power Supply Rejection Ratio (PSRR)

A2.2.2.6 CCD/APS

- Commercial CCDs are likely extremely sensitive to TID/TNID.
- Commercial CMOS sensors are typically sensitive but possible to use when low radiation tolerance needed.
- Effects:
    - Dark current increases
    - Read-out noise increases
    - Hot pixels increase (permanently damaged)
    - Random Telegraph Signal (RTS) – gate oxide becomes damaged in a way that charge is trapped there. After some time the trapped charge is released, giving the effect of blinking pixels
    - Flat-band voltage shifts (charging of oxide layers and structures)
    - Charge Transfer Inefficiency (CTI) is degraded
    - Increased power consumption
- Design/Operation pointers:
    - To mitigate flat-band voltage shifts:
        - Use a thin-gate technology, which limits the amount of voltage shift per unit of radiation
        - Design electronics such that operating voltages are adjustable
    - To mitigate CTI optimise the combination of operating temperature and clocking speed (read-out electronics). This would have to be adjustable throughout the mission or properly chosen in the beginning, considering radiation induced effects (i.e. if temperature is reduced to mitigate dark current then adjustments need to be made accordingly). Note that there is a sweet spot for CTI – the lowest temperature is not the best solution.
    - Dark current and CTI can be helped by annealing (increasing the temperature to room temperature for days to weeks, then then bringing back down to operating temperature)

A2.2.3 Opto devices

- For optocouplers, design conservatively to cover additional degradation of current transfer ratio
- For laser diodes and LED, consider additional degradation of emitted light
- For photodiodes, consider additional degradation of the dark current
- For phototransistor, consider additional degradation of collector current versus light input
- For fiberoptics, consider photo-bleaching of damage as a possible mitigation

A2.2.4 Bipolar transistors

- Design conservatively to cover Hfe additional degradation.
- Design conservatively to take into account of the additional increase of base and collector leakage currents

Note that normal heritage LEO design base on bipolar technology might not work in MEO, especially when TID effects are combined with TNID ones, and due to additional degradation of Hfe and base and collector leakage currents.

A2.2.5 MOSFETS (Si NMOS and PMOS)

- Design conservatively to cover additional trans-conductance degradation
- Design conservatively to take into account of the additional increase of gate and drain leakage currents

A2.2.6 p-GaN HEMT (and MISHEMT)

- Typical GaN HEMT RF show very little drift (< 12%) on threshold voltage and transconductance up to 1MRad
- Similar results are obtained for power GaN HEMT.

A.2.2.7 Other components

- For other integrated components not appearing in the list (for example DAC, ADC, linear regulators, etc) consider the radiation sensitivity of their constituent parts.

A2.3 Generic radiation mitigation techniques, TNID

A2.3.1 CCD, CMOS APS, opto discrete devices

- Effects:
    - Dark current increases
    - Read-out noise increases
    - Hot pixels increase (permanently damaged)
    - Random Telegraph Signal (RTS) – gate oxide becomes damaged in a way that charge is trapped there. After some time, the trapped charge is released, giving the effect of blinking pixels
    - Charge Transfer Inefficiency (CTI) is degraded
    - Increased power consumption
    - For photodiodes consider an increase of the dark current and additional degradation for InGaAs material compared to Silicon material (3 orders of magnitude)
- Design/Operation pointers:
    - Dark current and CTI can be helped by annealing (increasing the temperature to room temperature for days to weeks, then then bringing back down to operating temperature). Thus, should the design include the capacity to heat the CCD, then high temperature annealing may repair up to 80% of the damage

- Fill the charge traps before taking an image

A2.3.10 Other components

- For other integrated components not appearing in the list (for example DAC, ADC, linear regulators, etc) consider the radiation sensitivity of their constituent parts.
- Take into account that combined TID & TNID effects can greatly reduce the specified limits for operational amplifiers, voltage comparators and other analogue ICs. Especially ICs based on bipolar technologies can be a lot more affected by TID if it is combines with TNID.
- Consider that commercial voltage references may work well in Electron induced TID but drastically degrade if TNID is also present.

A2.4 Generic radiation mitigation techniques, SEE

A2.4.1 Diodes

- High voltage schottky rectifiers (especially SiC diodes) show increased leakage current in reverse bias conditions after SEE.
- Schottky diodes biased with more than 50% of rated reverse voltage may suffer destructive SEE.

A2.4.2 Integrated circuits

A2.4.2.1 Digital Logic, general

Digital electronics components are susceptible to various types of radiation induced SEE. Therefore, different types of mitigation techniques are required per each EEE component type, and often the best solution to protect digital circuits is to use a combination of error mitigation techniques. An overview of SEE, and their applicability to EEE components is shown in Table A2.4-1.

Table A2.4-1: Overview of SEE in EEE components

SEE type	Acronym	Effect	Affected electronics
SEU	Single Event Upset	Corruption of the information stored in a memory content	Memories, latches in logic devices
MBU	Multiple Bit Upset	Corruption of several memory elements in a single hit	Memories, latches in logic devices
SEFI	Single Event Functional Interrupt	Loss of normal operation	Complex devices with built-in state/control sections
SET	Single Event Transient	Impulse response of certain amplitude and duration	Analog and mixed-signal circuits, photonics
SED	Single Effect Disturb	Momentary corruption of the information stored in a bit	Combinatorial logic, latches in logic devices
SEL	Single Event Latch-up	High current conditions	CMOS, BiCMOS devices
SESB	Single Event Snapback	Device snapback, with transition from high voltage-low current to low voltage high current; high current conditions	N-Channel MOSFET
SEB	Single Event Burnout	Destructive burn-out	Bipolar junction transistors, N-Channel power MOSFET
SEGR	Single Event Gate Rupture	Rupture of gate dielectric	Power MOSFET
SEDR	Single Effect Dielectric Rupture	Rupture of dielectric	Non volatile NMOS structures, FPGA, linear devices
HCE	High Current Event	High current conditions	Digital devices
SEHE (SEH, SHE)	Single Event Hard Error	Irreversible change in operation typically associated with permanent damage to one or more elements of a device (e.g., gate oxide rupture)	Memories, latches in logic devices

In this section overview of SEE mitigation techniques are presented, as applicable to each different digital EEE component types. For more details, see [13] and [14]. The techniques presented hereafter cover:

- *Spatial redundancy, temporal redundancy* or a combination of both.
  In *spatial* redundancy, the logic resources are replicated in order to process the same task in parallel. The results from each replicated path are majority voted to detect and correct possible errors.
  In *temporal* redundancy signals are sampled (or full functions are executed) in varying time instances, and then majority voted to filter out SET and SEU.

- *Mitigation techniques specifically addressing Finite State Machines (FSM)*
  Specific FSM state coding and deadlock-recovery logic can be used to protect FSMs.

- *Error mitigation methods applied for memory arrays*
  Information redundancy methods are employed, using error detection and correction (EDAC) codes to protect data in memory arrays. Spatial redundancy can also be used, where the memory blocks are replicated and majority voted.

The following main digital electronic component category types will be considered:

- FPGAs
- Memories
- Microcontrollers
- Microprocessors
- Programmable Systems-on-a-Chip

A2.4.2.1.1 Spatial Redundancy Mitigation Techniques

a) Triple Modular Redundancy (TMR):

Different types of TMR can be used:

- ***Local TMR***
Only the sequential elements (D Flip Flops) in the circuit are triplicated and voted by a single voter (see Fig. A2-1). The voter is SET-free.

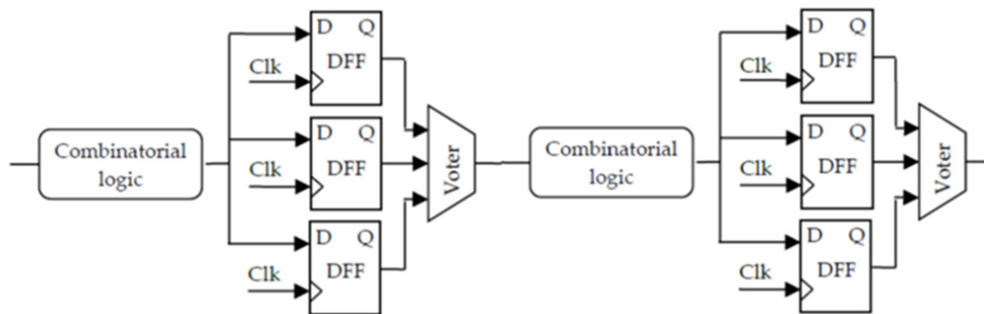


Figure A2-1: Local TMR

Local TMR is a good option for Flash-based FPGAs, providing acceptable upset rates with minimal area overheads. However, Local TMR is not a good option for SRAM-based FPGAs and should be avoided: upset rates with Local TMR are actually similar or worse than without mitigation. [21]

- ***Distributed TMR***
The complete computation paths are triplicated, including combinational logic, sequential elements, and voters (see Fig. A2-2). Single voters clock and reset lines are used.

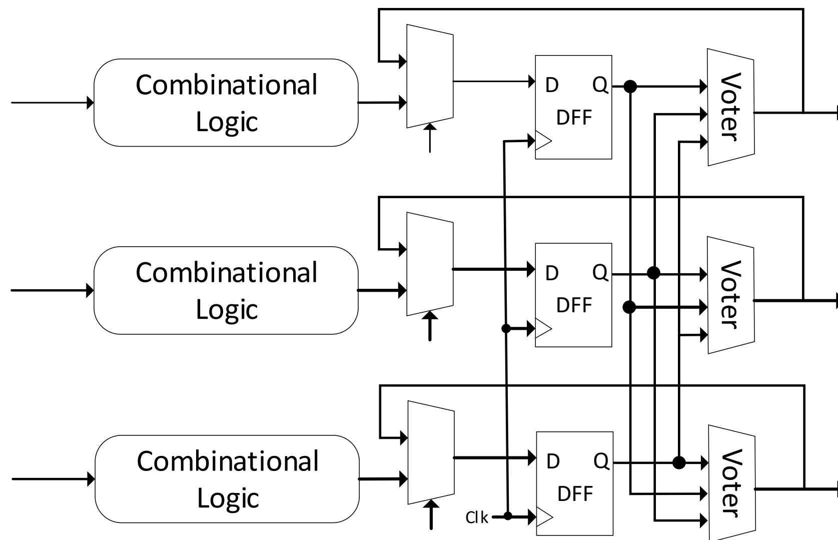


Figure A2-2: Distributed TMR

Distributed TMR is a good compromise between SEU mitigation strength, implementation complexity, and area overheads, and it is the recommended TMR scheme for SRAM FPGAs.

- ***Full or global TMR***
  All circuit elements, including DFF, combinational logic and TMR voters are triplicated. The clock trees are also triplicated, as shown in Fig. A2-3. Triplicating the clock trees also gives protection against SETs in the clock generation logic (clock tree).
  Full TMR should be in principle the strongest TMR method for SEU mitigation in SRAM FPGAs. However, skew among the triplicated clock trees introduces further design challenges, and may reduce mitigation strength.
  In addition, the additional circuit area required by the Full TMR scheme may even result in an actual increase on the error cross section of the circuit.
  The designer should confirm that the design tools properly support this TMR option and can manage the timing challenges, before using it. [21]
  Overall, considering the implementation challenges and the possible adverse effects on the error cross section, the Full or Global TMR is not one of the recommended TMR schemes for FPGA designs.

In all TMR cases, it is preferred to feedback the voted result back to the inputs of the sequential elements to update and correct the data and avoid accumulation of errors, as also shown in Fig. A2-3.

It should also be noted that as the transistor feature sizes decrease, especially in the Ultra Deep Submicron (UDSM) VLSI technologies in which the latest generation of FPGAs are manufactured, the probability of a single particle upsetting (SEU) more than one of the adjacent DFF in a TMR set increases. In such an event the TMR voting will fail, as 2 out of the 3 voted DFFs will have an erroneous value. This condition can be mitigated by physically distancing the DFFs of each TMR set on the FPGA area. This is a recommended solution for Local and Distributed TMR implementations, if the FPGA design tools used support it as an option (the synthesis and place-and-route tools).

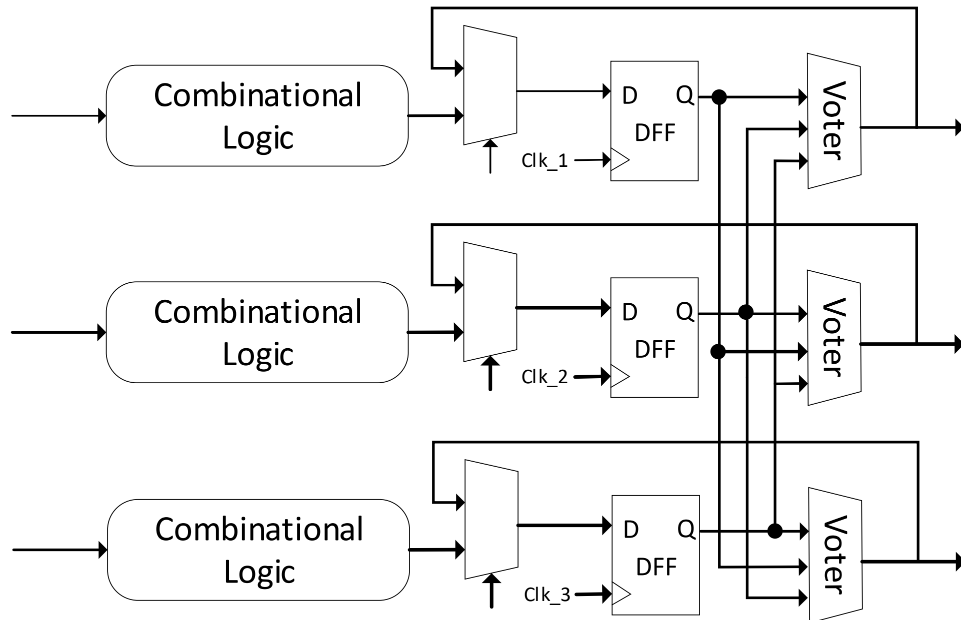


Figure A2-3: Full or Global TMR

b) Double Modular Redundancy (DMR), or Duplication with comparison (DWC)

When there is a need to reduce the TMR-induced overhead while still complying with reliability requirements, DMR with self-voting, duplication with comparison (DWC), or double-triple modular redundancy (DTMR) techniques can be used. Duplex architectures can only detect errors, but not correct them. An example of a DMR architecture in action is shown in Fig. A2-4.

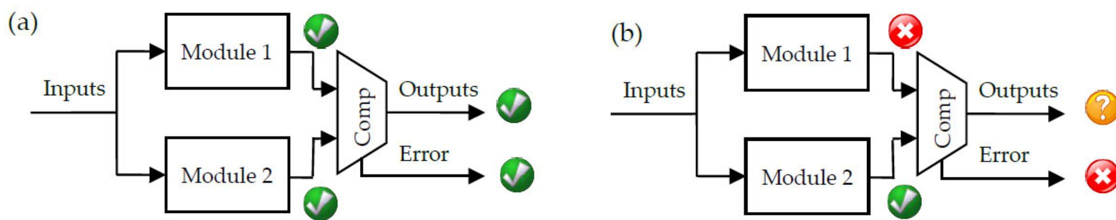


Figure A2-4: Fault detection in a Duplex Architecture

A2.4.2.1.2 Temporal redundancy mitigation techniques

a) TMR with triplicated clocks

If the technology used supports it, it is better to use three separate clock generators/managers (CM) on-chip for full TMR. If using a single CM to generate the clocks for all 3 paths, any SEE in the CM would essentially propagate through all three TMR paths. This technique was presented in the section "Full or Global TMR" above, and in Fig. A2-3.

b) SET filtering in TMR

Note*: this technique is mainly targeted at ASIC implementations. It is very challenging to implement temporal redundancy of this kind in FPGAs. It is mentioned here for reference and completeness, mainly.*

If only a single clock manager/generator is to be used, TMR can be complemented by triple skewed clocks. In this case varying delays are introduced in each sequential path to effectively filter out possible transients in the clock lines, as shown in Fig. A2-5. This technique has been successfully applied in the design of the LEON2-FT microprocessor, for example.

One of the main drawbacks of this mitigation technique is the intrinsic implementation difficulty, and in particular in timing closure of the mitigated design due to possible hold violations. The other drawback is the increase of the minimum clock period (reduction of max frequency) of the circuit by 2δ, where δ is the delay time in each clock path.

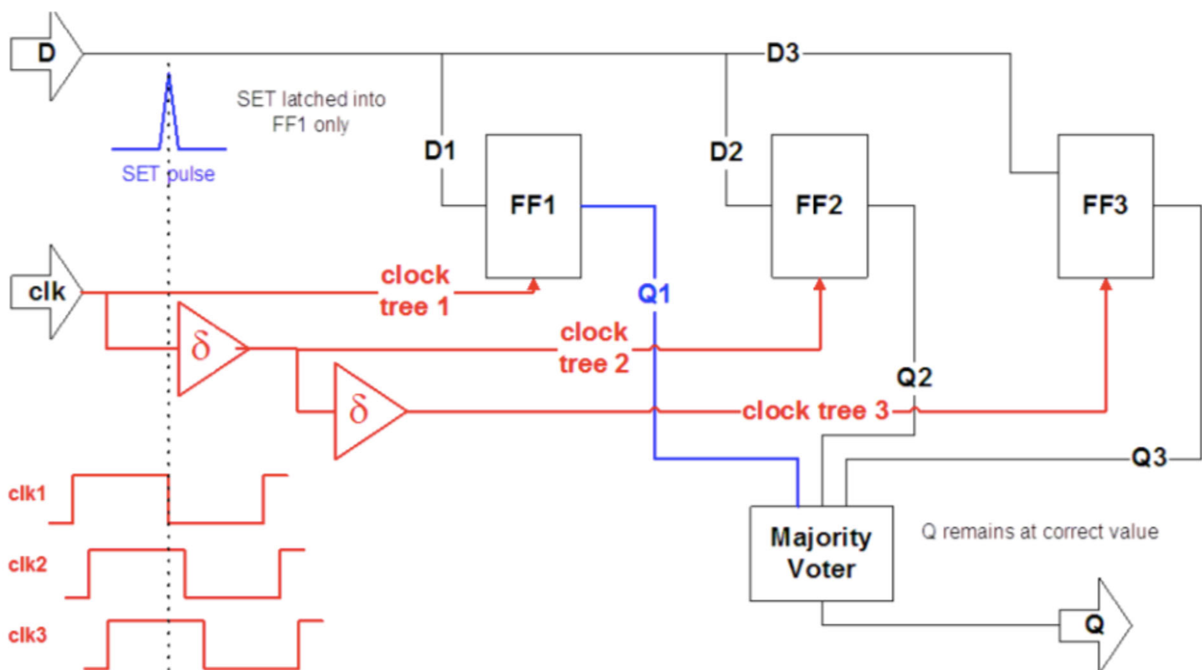


Figure A2-5: Skewed TMR Implementation

A2.4.2.1.3 SEU mitigation methods for Finite State Machines (FSMs):

FSMs are control circuits in integrated circuits, so radiation induced SEE in FSMs can have severe consequences in the operation of the circuit which the FSM is controlling.

For an FSM with N states, at least $\log_2(N)$ bits (rounded up to next integer) are used to store the state vector. Unless N is a power of two, the total number possible states will be greater than the number of valid or "legal" states. "Illegal states" are those in which the FSM is not supposed to enter during its intended normal operation.

For instance, an FSM with 6 valid states would need at least 3 bits to store the state vector, hence 2 out of the possible 8 states in the state vector will be invalid, or "illegal".

Possible issues in FSMs include transitions into illegal states, or illegal transitions (possibly even into legal states). The results from these effects can be either malfunctions in the controlled circuits, before the FSM recovers to a correct state, or a persistent "deadlock" condition where the FSM is stuck in an invalid state.

Mitigation against these faults include the following provisions. Note that all these mitigation techniques can be applied automatically by the FPGA EDA design tools (synthesis tools).

a) **Protection of FSMs by "safe" logic (automatic recovery to default state).**
Additional circuitry is introduced to detect a transition to an invalid state, and to automatically recover back to a default, pre-defined state.

Warning: "Safe" logic recovers from transitions to invalid states, but does not mitigate invalid transitions themselves, even if they are to valid states. These invalid transitions also need to be considered, and possibly mitigated via other means, even at a higher (system) level if necessary.

b) **Hamming-3 state encoding.**
The FSM states are encoded using a minimum of Hamming-3 distance, to reduce the possibility of invalid state transitions.

Warning: Hamming-3 may be more susceptible to SETs due to the increased combinational area footprint.

c) **TMR of state vector**
Of course the flip-flops used to store the state vector may also be protected by TMR, as an extra measure.

A2.4.2.2 SEU mitigations in Memory Arrays

A2.4.2.2.1 Error Correcting Codes (ECC)

Memory arrays can be protected against Single and Multiple Error Upsets (SEUs/MBUs) via the following methods:

- **EDAC**: An error detection and correction (EDAC) function can be used to correct errors in each memory block. These are usually in the form of Error Correction Code (ECC) algorithms.

- **Block TMR**: The memory blocks are triplicated, and their outputs are triple majority voted. However, this strategy is not well suited for large memory arrays due to the large area overheads incurred.

- **Bit-interleaving (or data scrambling):** Interleaving of memory cells within the memories blocks also helps compensating for MBUs. With interleaving the error-correcting code words are formulated from physically dispersed locations in the memory array. This results in errors in adjacent memory cells due to a particle hit to appear as multiple single errors instead of single MBUs, and therefore being easier to correct using EDAC algorithms.

A2.4.2.2.2 Overview of ECC types

The main error mitigation method applied to most types of memories is the EDAC (Error Detection and Correction) function. This is usually implemented using an Error Correcting Code (ECC) or Forward Error Correction (FEC).
ECC algorithms add redundant data or parity data to the original data, enabling the detection and correction of errors that may have been introduced during the transmission or storage of this original data.

There are several types of ECC, each one with each own characteristics and EDAC capabilities. Because of this, it is up to the designer to select the most suitable ECC for use taking into account the requirements and needs of each specific application. An overview of different ECC is given in Table A2.4-2.

Table A2.4-2: EDAC capability of different ECC

ECC	Error Detection	Error Correction
Parity check	X	
Cyclic Redundancy Check (CRC)	X	
BCH codes	X	X
Hamming codes	X	X
Reed-Solomon codes	X	X
Low Density Parity Codes (LDPC)	X	X

- **Parity** is the simplest form of error detection mechanism: an extra bit is appended in the data word to indicate the overall number of 1's in the word (including the parity bit), either ODD or EVEN. A possible data corruption might alter the total number of 1's, causing a discrepancy versus the indicated parity bit, and flagging a corrupted data word.

- **Cyclic Redundancy Check (CRC)** is an-error-detecting (not correcting) cyclic code and non-secure hash function designed to detect errors in computer network communications. It is characterized by specification of a so-called generator polynomial, which is used as the divisor in a polynomial long division over a finite field, taking the input data as the dividend, and where the remainder becomes the result. Cyclic codes have favourable properties as they are well suited for detecting burst errors (continuous sequences of data containing errors). CRCs are particularly easy to implement in hardware, and are therefore commonly used in digital network communications, and in data storage devices.

- **BCH (Bose-Chaudhuri) codes** form a class of parameterized error-correcting codes which have been the subject of much academic attention in the last fifty years. Reed-Solomon codes are a special case of BCH codes.
  The principal advantage of BCH codes is the ease with which they can be decoded, via an elegant algebraic method known as syndrome decoding (syndrome decoding is a highly efficient method of decoding a linear code over a noisy channel). This allows small and power- efficient hardware implementations of the decoding logic.

- **Hamming codes** add additional check bits to the data to be protected, enabling single error correction and multiple (usually double) error detection (SEC-DED). A common example is Hamming (7, 4), where 4 bits are encoded into 7-bits by adding 3-parity bits, hence enabling SEC-DED. Hamming codes are effective for transmission mediums where burst errors are not likely to occur.

- **Reed-Solomon (RS) codes** are non-binary cyclic error-correcting codes, capable of detecting and correcting multiple random errors. They are a form of BCH (see above), where encoding symbols are derived from the coefficients of a polynomial constructed by multiplying $p(x)$ with a cyclic generator polynomial. By adding t check symbols to the data, an RS code can detect any combination of up to t erroneous symbols and correct up to $t/2$ symbols. Furthermore, RS codes are suitable as multiple-burst bit-error correcting codes, since a sequence of $b+1$ consecutive bit errors can affect at most two symbols of size b. The choice of t is up to the designer of the code and can be selected within wide limits.

- **Low Density Parity Codes (LDPC)** can provide high error correction capabilities, compared to e.g. Hamming ECC. An advantage of LDPC when compared to other high (error correction) performance codes

such as Reed-Solomon or BCH is their simpler algebraic principles, making them easier to implement in programmable logic arrays (e.g. FPGA) and requiring less computation time, therefore being well suited as an EDAC strategy for high speed memories.

A2.4.2.3 SEE Mitigation per Memory Type

Each different memory type needs different kinds of SEE mitigation methods to be applied.

a) SRAM

- The ECC methods commonly used for SRAM memories are Hamming code ECC, parity, and CRC.
- Scrubbing can also be utilized: the data words in the memory are periodically read and either corrected from possible errors using an ECC algorithm or compared with a "golden reference" data set. The corrected data words are then written back into the memory. The scrubbing period needs to be adjusted according to the anticipated error rate of the specific application, to avoid accumulation of errors that might render the EDAC method used insufficient.
- SRAM can be susceptible to latch-up, so the use of an external latch-up protection circuit (current limiter) is recommended.

b) SDRAM

SEE in SDRAM are either SEU - bit flips directly in memory cells - or SEFI, due to transient errors in the control logic of the memory, causing burst errors while reading/writing the memory. The following mitigation methods are recommended for SDRAM applications:

- Reed-Solomon ECC
  The main EDAC algorithm commonly used for SDRAMs is Reed-Solomon (RS).
  RS is preferred because it suits better the types of errors incurred in SDRAMs, which are burst errors due to SEFI in their control registers/logic.

  The RS based ECC most used in 32-bit SDRAMs can detect and correct SEUs in at least one nibble per word. I.e. up to 4-bit errors can be detected and corrected per word as long as they are within the same nibble. Such ECC may also detect, but not correct, multiple errors in different nibbles within the word.
- Interleaving of memory cells within the memory blocks also helps compensate for MBUs. With bit-interleaving the error-correcting codewords are formulated from physically dispersed locations in the memory array. This results in errors in adjacent memory cells due to a particle hit to appear as multiple single errors instead of single MBUs, and therefore easier to correct.
  SEFI can result from particle hits affecting the SDRAM control logic or mode register. Clearing and re-loading of the mode register can clear the row SEFI. If not, the same procedure may be repeated after stopping the refreshing operation.
- Board-level redundancy:
  Redundancy and fault tolerance can also be implemented at board level. For example, assuming a (40,32,8) RS ECC code, if 4-bit SDRAM chips were used, the RS ECC scheme used would enable a board level redundancy of 1 SDRAM chip/bank. Since each memory chip would implement a nibble, it would still be possible to recover the full 32-bit word even in case of destructive (and not only transient) failure in one memory chip/bank (assuming that the ECC bank would remain intact).

- While in SDRAM produced until about 2005 SEL was a major issue, SDRAM produced as from 2010 do not show susceptibility to SEL.
  https://ieeexplore.ieee.org/document/7336713
  https://escies.org/download/webDocumentFile?id=63077

c) EEPROM

- Memory cells are not sensitive to radiation induced SEE. Only the control register (read/write buffer) is susceptible to SEU/SET, so memory is only sensitive during read/write cycles. A system-level mitigation can be applied, e.g. reading back the data after writing to confirm correctness.
- Use of CRC protection recommended.
- EEPROM memories readout registry may be activated from Hi-energy protons and not only by heavy ions.

d) Flash

- Memory banks in Flash memory arrays can be powered down to reduce TID accumulation effects.
- Flash memories, and EEPROM, are more sensitive in Write and Read modes than in Static mode, especially to SEFIs.
- Flash memories readout registry may be activated from Hi-energy protons and not only by heavy ions.

A2.4.2.4 Field Programmable Gate Arrays (FPGAs)

FPGAs are integrated circuits designed to be configured by the end user (hence the term “field programmable”), rather than the manufacturer or semiconductor fab factory.
FPGAs consist of an array of programmable logic blocks and a hierarchy of reconfigurable interconnects that allow these logic blocks to be connected in different configurations. Logic blocks can be configured to perform combinational functions, or used as sequential elements (flip flops), or simple memory blocks. FPGAs also contain larger memory blocks, different types of configurable I/O, and even more complex processing elements such DSPs or even embedded processor cores. Overall, FPGAs provide the functionality to implement different complex logic functions, and flexible reconfigurable computing applications.

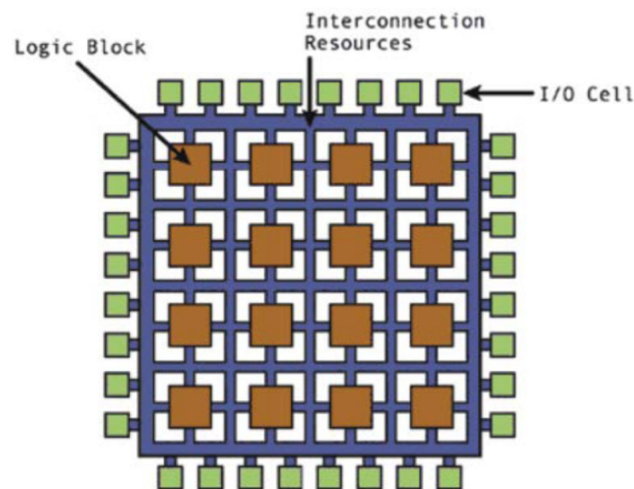


Figure A2-6: High level overview of FPGA structure

There are several different FPGA types, according to their underlying manufacture process technology. The most commonly used ones are the following:

- **SRAM-based FPGAs**
  Based on static memory (SRAM) CMOS technology. They can be programmed in-system and are reprogrammable. SRAM cells are volatile, so these FPGAs require external boot devices, to contain their configuration bitstreams and control their programming.

  They can be sensitive to radiation, in particular their configuration memory cells. Bit-flips occurring in the configuration memory can have an impact on the application behavior in case the perturbed bit is used, altering the circuit configuration. In such a case, even a reset of the application would not recover to the normal operation, and an FPGA reconfiguration would be necessary to recover the nominal configuration.

  Notable SRAM FPGA manufacturers are:

  - Xilinx:
    https://www.xilinx.com/products/silicon-devices/fpga.html

  - Intel (ex Altera):
    https://www.intel.com/content/www/us/en/products/programmable/fpga.html

  - NanoXplore (eFPGA technology):
    http://www.nanoxplore.com/categories/17-efpga.html

  - Lattice (ECPx families, Ice40, LatticeXP)
    http://www.latticesemi.com/Products.aspx#_D5A173024E414501B36997F26E842A31

- **Flash-based FPGAs**
  Based on Flash-erase CMOS EPROM technology. They can be erased and reprogrammed. Most Flash-based FPGAs can be in-system reprogrammed. They are more power efficient than SRAM FPGAs, and have better radiation tolerance.
  The most commonly used Flash FPGAs are from Microsemi (now Microchip), e.g. ProASIC3, IGLOO2, SmartFusion2, PolarFire, Fusion etc:
  https://www.microsemi.com/product-directory/fpga-soc/1638-fpgas

- **Antifuse-based FPGAs**
  The basic structural element of these devices is the antifuse, which starts with a high resistance, and forms a permanent electrically conductive path during programming when a current through the antifuse exceeds a certain level.
  These FPGAs are one-time programmable devices. They have very good radiation tolerance, and lower power consumption. Notable manufacturers of antifuse FPGAs are:

  - Microchip (ex Microsemi)
    https://www.microsemi.com/product-directory/fpga-soc/1641-antifuse-fpgas

  - QuickLogic
    https://www.quicklogic.com/products/fpga/fpgas-antifuse/

Configuration memory type	Antifuse	Flash	SRAM
Characteristics	a.Electrically programmable switch which forms a low resistance path between two metal layers b.Configuration is NON-volatile c. One-time programmable (OTP)	a.Electrically programmable Flash cells (transistors) hold the configuration that controls a pass transistor or multiplexer connected to predefined metal layers. b.Configuration is NON-volatile c. Re-programmable	a.The state of a static latch controls a transistor or multiplexer connected to predefined metal layers. b.Configuration is volatile c.Re-programmable
Manufacturers	Cobham (ex-Aeroflex) Microchip (ex-Microsemi) QuickLogic	Microchip (ex-Microsemi)	Xilinx Microchip (ex-Atmel) NanoXplore

Table A2.4-3: Types of FPGAs

A2.4.2.4.1 SEE Mitigation for Flash-based FPGAs

Flash based FPGAs, such as Microchip ProASIC3, SmartFusion2, or PolarFire require SEE mitigation for their sequential and combinational logic, for their on-chip memories and if applicable to their I/O as well. The configuration memory of these FPGAs is not susceptible to SEUs. The following mitigation techniques can be applied:

- TMR for sequential elements: local TMR can yield acceptable upset rates when used in Flash-based FPGAs and is the recommended scheme for those FPGAs.

- FSM protection: (a) Hamming-3 FSM state encoding and (b) “Safe” FSM implementation. This is additional circuitry that detects transitions to invalid states, and automatically recovers the FSM to a default known state, to avoid deadlock. . The FSM state vectors registers will also be protected by the TMR applied globally within the FPGA.

- Memory EDAC: Depending on the application needs, any type of ECC listed in section A2.4.2.2.2 can be used: Hamming, CRC, parity, RS. Block TMR can also be considered for the on-chip memories, depending on the area utilization margins.

- TMR for Outputs: the final outputs of an internal TMR set, driving external output pins, can be voted outside the FPGA on the board using the diode-based voter shown in section 11.7.4.2).
  If applicable in the target FPGA technology, another approach can be to use Minority Voters to control the tri-state logic of the output buffers, as documented in the following application note:
  https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf
  The main advantage of such an approach is that no external devices are required to implement the triple redundant voting.

Most of these mitigation techniques can be implemented automatically by the FPGA design tools.

The SEL sensitivity of Flash FPGAs varies depending on their specific manufacture technology, so it is recommended to assess their SEL immunity on a case by case basis, based on existing radiation performance data. See also section f10.7.3.1.4-f. [31]

While Flash-based FPGAs are re-programmable, reprogramming them during flight in a radiation environment presents certain risks mainly due to the higher voltages utilized for programming the Flash configuration cells (up to 17.5V). The risks can be either due to TID effects in the configuration logic, or to SEEs in the internal charge pump used for the generation of the programming voltages. Experimental data have shown that failed reconfiguration cycles may be successfully repeated several days later. These mechanisms have been attributed to micro dosage mechanisms and annealing effects. Since these effects, and the success of reprogramming under irradiation, are not deterministic, it is recommended to avoid reprogramming of Flash FPGAs for higher criticality missions: definitely not for Q0, better to be avoided for Q1, can be considered for Q2 based on the mission requirements.

https://ieeexplore.ieee.org/document/6062510

A2.4.2.4.2 SEE Mitigation for SRAM-based FPGAs

In SRAM-based FPGAs, both the programmable logic fabric – flip flops, look-up tables (LUTs), combinational logic, etc – the on-chip memory blocks, the I/O banks, as well as the configuration memory are susceptible to SEE.
The following mitigation methods are recommended:

- TMR for sequential elements: local TMR is not recommended for SRAM FPGAs as the upset rates may even be worse than with no mitigation in those devices. Distributed TMR is a good compromise between SEU mitigation strength, implementation complexity and area overheads, and it is the recommended TMR scheme for SRAM based FPGAs.

- FSM protection: (a) Hamming-3 FSM state encoding, and (b) "Safe" FSM implementation. This is additional circuitry that detects transitions to invalid states, and automatically recovers the FSM to a default known state, to avoid deadlock. The FSM state vectors registers will also be protected by the TMR applied globally within the FPGA.

- Memory EDAC: Depending on the application needs, any type of ECC listed in section A2.4.2.2.2 can be used: Hamming, CRC, parity, RS. Block TMR can also be considered for the on-chip memories, depending on the area utilization margins.

- TMR for Outputs: The final outputs of an internal TMR set, driving external output pins, can be voted outside the FPGA on the board using the diode-based voter shown in section 11.7.4.2).
  Another approach is to use Minority Voters to control the tri-state logic of output buffers, as documented in the following application note: https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf
  The main advantage of such an approach is that no external devices are required to implement the triple redundant voting.

- FPGA configuration memory: the configuration memory of an SRAM FPGA needs to be periodically refreshed and "scrubbed", i.e. corrected from potential errors to avoid accumulation. The active configuration memory area is scanned sequentially and periodically, and each memory word is either "blindly" refreshed from a externally referenced version of the data, or it is checked and if necessary corrected either using an ECC algorithm or via comparison with an externally stored reference version of the data, and then written back. The scrubbing period needs to be adjusted taking into account the radiation profile and SEU error rates for the specific mission, to avoid accumulation of errors that might also not be correctable by the ECC algorithm used. Xilinx already has provisions for supporting this mechanism both in hardware, via a dedicated, on-chip configuration memory scrubber block (SEM), and in their design software tools.
  https://www.xilinx.com/products/intellectual-property/sem.html

- SRAM FPGAs can be susceptible to SEL, and unless it is confirmed otherwise, they should be used with external latch-up protection circuitry. The SEL susceptibility levels of each device can also be assessed against the specific application requirements, and the designer may decide whether the SEL thresholds of the device require actual latch-up protection at board level.

- If a SRAM FPGA is to be reprogrammed/reconfigured in-flight, either fully or partially, it is recommended to use a radiation tolerant "supervisor" (e.g. a processor or radiation tolerant FPGA) to control, initiate and execute the reconfiguration procedure, if possible.

- SRAM FPGAs support different configuration options, or methods of loading a configuration file (bitfile):
  (1) The FPGA can load the bitfile itself directly from an external, directly connected serial non-volatile memory, or
  (2) The FPGA can be configured "remotely", where the bitfile is loaded by an external "intelligent agent" such as a processor, microcontroller, DSP etc. The advantages in this in this case is that (a) a parallel interface can be used for the configuration, hence significantly reducing configuration times, especially for larger FPGAs, and (b) the configuration bitstream can reside anywhere in the system and can even by loaded from ground.

  These factors should be considered when designing with SRAM-based FPGAs, in conjunction with the radiation profile of the mission and the specific reliability/availability requirements. E.g. radiation tolerant serial NVMs (Non Volatile Memories) should be used, or "reliable" (radiation tolerant) configuration supervisors.

A2.4.2.5 SEE Mitigation for Microprocessors

Microprocessors can be susceptible to several SEE, including SEU/MBU in the register files and memories, SEFI during program execution, and SEL. Therefore a combination of mitigation methods is required to address all possible types of errors:

- Watchdog timer(s)
  A continuous timer can be set to count down from a predefined value, during program execution. The SW will need to refresh the counter periodically during normal application execution, as a "program health check". If a radiation-induced SEE affects normal program execution, or completely freezes the processor, the watchdog will not be refreshed, and will eventually timeout. A watchdog time-out event causes an automatic processor reset and is used as a straightforward means of automatic recovery from SEFI.

- Software-level mitigation of errors
  Software-Implemented hardware Fault Tolerance (SIFT) refers to a set of techniques that allows a piece of software to detect and possibly to correct faults affecting the hardware on which the software is running. SIFT can be applied to Commercial-Off-The-Shelf (COTS) processors, or to Intellectual Property (IP) processors embedded in ASICs or FPGAs, which either do not include any mitigation techniques for the radiation effects faults of concern or where not enough mitigation can be implemented in the hardware due to system requirements (e.g. power consumption or chip area occupation).

  In all SIFT techniques redundant instructions are inserted in the original program code, to enable fault detection. Instructions in this context can be either individual instructions, groups or blocks of instructions. Since transients and upsets are the main types of faults considered, redundancy is obtained by selectively duplicating computations and by inserting consistency checks to detect differences among the computations. Duplication can be performed at different levels of granularity: at instruction level, at task-level, or at application level.
  Software-level mitigation techniques are applied at a high level of abstraction, and therefore they cannot determine the source the errors (SEUs or SETs), but only detect their impact on the computation. Section 14 of ECSS-Q-HB-60-02A provides a more detailed overview of SIFT techniques.

- Memories and register files
  Register files can be protected by CRC or other ECC (see also para A2.4.2.2.2), on chip memories by Hamming ECC, or CRC if suitable. The on-chip busses can be protected by extra parity bits: if a parity error is detected during a transaction, a flag can be raised and the transaction repeated by the application SW.

In the case of multicore microprocessors, another possible SEE mitigation technique is dual-lockstepped operation. In dual lock-stepped operation, each instruction is duplicated and executed in parallel in more than one cores, and the results compared or voted. There are two types of lock-stepped operation:

a. Fine grain lock-stepping:
   The two cores are running in full synchronization, with the intermediate results (or register files, caches, etc) compared and voted in every execution cycle. In case of discrepancy, instruction execution is backtracked to a previous execution checkpoint.

b. Coarse-grain lock-stepping:
   The processor cores are run independently, interrupted in periodic intervals to synchronize execution and compare/vote their intermediate results (or register files, caches, etc). In case of discrepancy, instruction execution is backtracked to a previous execution checkpoint.

In both cases, the checker/voter can be implemented in either SW or in HW. A HW implementation allows for more robustness, since the checker/voter can be radiation hardened as well. A SW voter would also be susceptible to SEE. [ECSS-Q-HB-60-02A, section 15.2.5]

- COTS microprocessors can be susceptible to SEL, so an external latch-up protection mechanism is required.

A2.4.2.6 SEE Mitigation Techniques for Microcontrollers

Some of the considerations and techniques mentioned for the microprocessors above may also be applicable for microcontrollers, although the (usually) reduced complexity of the component and of the target application probably doesn't justify their use. For instance, microcontrollers don't usually have caches, for more deterministic behavior; have only one processing core; and may not even use an OS. Mitigation techniques still applicable can be parity, EDAC and CRC for on-chip busses and memories, and a simple form of instruction check-pointing (repeated execution and checking of instructions).

- Microcontrollers tend to have extensive set of peripherals, which also need consideration and error mitigation. E.g. EDAC and parity in serial interfaces.

- Microcontrollers are commonly mixed-signal components, so their analog blocks also need special considerations in terms of SEE: PLL, PWM, ADC/DAC, etc.

- COTS microcontrollers can be susceptible to SEL, so an external latch-up protection mechanism is required.

A2.4.2.7 SEE Mitigation Techniques for SoC FPGAs

In recent years there has been an emergence of highly integrated reprogrammable FPGAs featuring one or more microprocessor cores, and also even DSP cores, on-chip. These components, named SoC FPGAs., enable an even wider range of applications than simple FPGAs, due to their higher levels of integration and advanced features. Examples of COTS SoC FPGAs are:

- Xilinx Zynq APSoC, featuring single or dual-core ARM Cortex-A9 processors,
- Intel Agilex and Stratix 10 SoC FPGAs, featuring quad-core ARM Cortex-A53 processors,
- Intel Arria 10, Arria V and Cyclone V SoC FPGAs, featuring dual-core ARM Cortex-A9 processors,
- Microsemi SmartFusion2 and PolarFire SoC, featuring ARM Cortex-M3 and RISC-V cores, respectively.

To mitigate against radiation induced SEE in an SoC FPGA, a combination of mitigation techniques will need to be considered for the FPGA fabric elements (combinational and sequential elements, IP blocks, I/O blocks), the on-chip memories and the embedded processors, and DSP cores if applicable. All the techniques described in the previous sections, related to SEE mitigations for FPGAs, memories and microprocessors, are applicable in this case. The selection of the mitigation techniques to be utilized will depend on the mission profile, the radiation tolerance and performance requirements, the criticality of the design, and the available margins in terms of area and timing, since most of the aforementioned SEE mitigation techniques will incur penalties in either timing performance or in overall area utilization.

The programmable logic (FPGA fabric) in the Programmable SoC can either be configured simultaneously with the boot of the embedded processor, or it can be configured under the supervision of the embedded processor after boot. Both the boot and bitfile images can be stored in an external NVM (Non Volatile Memory), in which case the selection of a radiation tolerant NVM can provide the added benefit of robustness against SEUs for the storage of the configuration and boot files

https://www.intel.com/content/www/us/en/products/programmable/soc.html

https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html

https://www.microsemi.com/product-directory/soc-fpgas/1692-smartfusion2

https://www.microsemi.com/product-directory/soc-fpgas/5498-polarfire-soc-fpga

A2.4.2.8 Bandgap references

- Consider that, due to SET, negative transients can appear in band gap reference voltage with duration dependent on decoupling capacitor (from 1us to some tens of us typical, but it might last longer)
- It is convenient to use RC filtering after bandgap references to filter out such transients
- Critical effects from SET are likely occurring with Hi-energy protons and not only with heavy ions.

A2.4.2.9 Operational amplifiers and comparators

- For comparators, rail to rail transients may appear as result of SEE (both positive and negative), with duration depending on comparator technology but usually limited to few us.
- For comparator applications needing fast response, make use of TMR logic (if signals needs to be controlled in both high to low and low to high direction) or double redundancy logic (if signals needs to be controlled either in high to low or in low to high direction).
  For TMR, see Figure 5 at p.68
- For slow comparator applications, use RC filtering
- For operational amplifiers, count that SEE might cause positive or negative transients at the output of different amplitude and with duration of some hundreds of nanoseconds (fast devices) to some tens of microseconds (slower devices)
- For operational amplifiers inserted in control loops, pay attention that the SET effect is normally far longer than the one observed in the stand alone configuration, and dependent on the control loop bandwidth
- For operational amplifiers needing fast response, make use of TMR logic (if signals needs to be controlled in both high to low and low to high direction) or double redundancy logic (if signals needs to be controlled either in high to low or in low to high direction)
- For operational amplifiers applications, use RC filtering if possible. Note that some operational amplifiers have given rather long transients lasting (up to millisecond being not common, but not rare either). Rail-to-rail output swing is not an overly conservative assumption for the SEE amplitude.

A2.4.2.10 Microwave integrated circuits

- SEGR and SEB might be an issue for RF large signal or RF power MMIC

A2.4.2.11 CMOS

- N/A

A2.4.2.12 CCD, APS

- Typically very sensitive and requires latch-up protection.
- Effects:
  - Image quality degradation by energy deposited by heavy ion or proton in pixels
    - For longer integration time (astronomy applications) the work around is to have continuous sampling without resetting again (up the ramp sampling). An algorithm can detect spikes per pixel and correct digitally (on-board).

- SEFI if ion impacts the register and causes it to flip.
- Row counter – shift register – if bit is flipped then you read out the wrong row.
  - Check image and compare against what you expect to see (if rows and columns are where you expect them). Plausibility.
- There must be current detection, the ability to switch off immediately and power cycle provisions to protect against SEL.
- Configuration and control logic registers in rad-hard APS designs are normally protected against SEE by triplication and voting (TMR). Some devices also incorporate triplicated and phase-shifted clocks and resets for these registers. Data registers are not usually triplicated, due to the large area overheads required. [17]
- In general all SEEs are applicable as per other electronics and mitigation should be considered in the design.

A2.4.2.13 Opto devices

- For optocouplers latch-up would only be a concern for types that contain ICs or MOSFETs. SETs may need to be addressed by analysis.

A2.4.2.14 MOSFET (Si NMOS and PMOS)

- Drain to source voltage derating

A2.4.2.15 HEMT (p-GaN and MISHEMT)

- Drain to source voltage derating, and possibly additional measures will be defined in the future.

A2.4.2.16 Microwave transistors

- Drain to source voltage derating, and possibly additional measures will be defined in the future.

A2.4.2.17 FET (N and P channel)

- Drain to source voltage derating

A2.4.2.18 Other components

- For other integrated components not appearing in the list (for example DAC, ADC, linear regulators, etc) consider the radiation sensitivity of their constituent parts.
- SEL in advanced ADC circuitry may easily be triggered with protons > 100 MeV energy
- PWM control IC circuits, as an example UC1823/25, UCC1806 and UC1846/56, have very sensitive internal latching protections that may temporarily or permanently switch-off the supplied equipment. Usually the likelihood for activation is quite low with GCR calculations, but within a High-energy proton environment (Van Allen belts), the probability or spurious protection activation will be much more severe.
- For MMIC, SEGR and SEB might be an issue

ANNEX 3, CONSERVATIVE TID AND TNID RADIATION ENVIRONMENT MODELLING FOR Q1 AND Q2 CRITICALITY CATEGORIES

a. The radiation environment should be defined according to the mission specifications using models and rules defined in ECSS-E-ST-10-04C [S29].

b. The radiation levels within the spacecraft should be determined at component level according to methods described in ECSS-E-ST-10-12C [S28] [32] with the following additional recommendations c,d, and e.

c. 1D Mission Dose Depth Curve (DDC) look up for minimum shielding level should be the preferred method (as it requires the least amount of modelling work and provides additional margin, making it the most conservative method).
   - The solid sphere total mission dose depth curve should be used.
   - In this definition 'total mission' is the duration over which the component is expected to function within specification.

     NOTE
     The minimum shielding thickness in any given direction is checked.
     For example, if the module box provides 3mm of Aluminium at its thinnest, with a 1mm Aluminium spacecraft panel in the least shielded direction from the spacecraft, look up the dose at 4mm of Aluminium from the total mission DDC and check it is < 5krad(Si).
     If it is <5krad(Si) then no radiation modelling (e.g. in FASTRAD or similar tools) is required.

d. Where 3D sector shielding analysis approach is necessary (for where the 1D approach does not yield doses < 5krad(Si)):
   - The number of sectors used should be at least 2000 to ensure full coverage.
   - A margin of 2 shall be applied to the calculated TIDL. For example for Q2 level, the calculated TIDL at should be < 2.5krad(Si), i.e with a margin of 2 applied to the 5krad(Si) limit for untested COTS components. This margin is specifically for the variability of COTS components.

e. SLANT method should be used in all cases in combination with the solid sphere DDC.

ANNEX 4, DETAILS ON Q2 AND Q1 RADIATION TESTS

A4.1 Personnel safety

a. Experimenters should be supported by the irradiation facility team for radiation safety during the entire experiment, preparation and after experiment.

b. The exposed components and boards and all equipment in the irradiation room should be retrieved only after radiation safety checks have been made by facility personnel.

> NOTE
> High energy protons activate the exposed parts, the time before safe use after experiment can reach several months. Very high energy ions can also induce activation, the time before safe use after experiment can reach several weeks.

A4.2 Documentation

a. For each irradiation test to be performed, 2 sets of documents should be provided:

   1. A Test Plan (prior to irradiation testing) defining the detailed requirements of the irradiation testing to be performed.
   2. A Test Report giving the actual test conditions and test results.

b. As a minimum the Test Report should include the following:

   1. Part traceability information
      - Full part type number
      - Serial number
      - Date code
      - Wafer lot number
      - Package type and marking
      - Die picture
      - Part technology/process
      - Wafer number (if known)
      - Die fab facility (if known)

   2. Irradiation conditions
      - Test date
      - Irradiation facility and radiation source type
      - Irradiation test sequence with detail of irradiation and annealing steps
      - Dose rate(s) or Flux
      - Accuracy of the dose or fluence levels

   3. Bias or operation conditions during irradiation with identification of samples per condition

   4. Pre and Post-irradiation electrical measurements conditions and acceptable limits for the considered design (even if the original manufacturer specifications are exceeded)

   5. Electrical measurements during irradiation

   6. Test results (tabulated and figures) for each electrical parameter measured, showing the measurement results after each irradiation and annealing step of all irradiated EEE components and the control part

c. Any anomalies that occurred during the test should be reported and fully described.

A4.3 TID and TNID test

A4.3.1 TID and TNID test conditions

a. The test devices or test boards should be irradiated in accordance with the Test Plan.

b. All electrical parameters to be tested and biasing conditions should be clearly described.

c. As a minimum, the Test Plan should contain all information according to the Test Plan Notes provided in the ESCC Forms section of https://escies.org

d. For board level the Test Plan Notes mentioned in recommendation A6.3.1c should be modified accordingly.

e. The dose rate should be:

1. For MOS and CMOS devices or boards only containing MOS and CMOS devices, radiation dose rate window 1 as described in section 4.3 of ESCC22900 [S18].
2. For devices or boards containing bipolar transistors (also bipolar based ICs and BiCMOS), radiation dose rate window 2 (low dose rate) as described in section 4.3 of ESCC22900 [S18].
3. As justified by application and/or mission conditions.

f. The foreseen mission TIDL and TNIDL should be exceeded by at least a margin of 50% at component level or of 100% at board/module level, or until board / module out of spec or functional failure, whatever is the minimum

g. The dose steps should be evenly distributed until the maximum mission level, including the 50% (i.e. 1.5) margin.

NOTE
Example: mission TIDL=5 krad, dose steps 1 krad, 2 krad, 3 krad, 4 krad, 5 krad, and 7.5 krad.

A4.3.2 TID and TNID Sample size and serialisation

a. If lot information is available or if sufficient checks have been done to determine the procured lot homogeneity, TID irradiation test should be performed on 5 samples per flight operation condition(s).

NOTE
Consider the especially OFF periods where TID effects might be more severe.

b. If lot information is not available, it is advisable to procure sufficient number of devices to perform irradiation characterisation on 40 devices selected randomly from the procured samples.

NOTE
This to ensure that lot variations are accounted for since for TID performance, in particular bipolar based devices, may exhibit significant lot-to-lot variation.

c. Sample serialization: immediately after selection, each individual sample device should be serialised to facilitate pre- and post-irradiation data identification and comparison.

d. Sample serialization: the system of marking should be such as to ensure that the samples are clearly identified by:
    1. Date-code of the sample.
    2. Their individual serial number.

A4.3.3 Board level testing

a. For procured (not designed) boards, board level testing often represents only a go-no-go test. It is not recommended for Q1 when the homogeneity of the lot cannot be guaranteed for each EEE component.

b. If homogeneity is guaranteed, when selecting the number of boards to be tested, a sufficient number of individual devices should be ensured on one or more boards to satisfy the sample size requirement for individual devices (i.e. minimum 5 samples).

A4.4 SEE test conditions

a. ESCC25100 [S10] should be followed.

b. Visibility. The component/board parameters to be measured should be clearly defined.

c. Visibility. The measured parameters should be carefully chosen to allow analysis of failure modes and of the mitigation techniques.

d. Maximum Coverage. The component/board operating conditions should be clearly defined.

e. Maximum Coverage. It should be recorded if the test is performed in worst-case generic or mission operation conditions covering single or multiple applications/missions.

f. All types of SEE should be recorded with maximum coverage and visibility in operation conditions.

g. Mitigation techniques should be tested.

h. At minimum three board/component samples should be tested.

i. The SEE test verification should be performed with high energy heavy ions at component or board level.

j. For heavy ion tests, the following conditions are recommended:

    1. Heavy ion beam conditions for test characterisation at component level or at board level see a minimum of LET of 38 MeVcm2/mg on the component sensitive volume, fluence minimum 1E7 ions/cm2, following indications of ESCC25100 [S10].

    2. The LET should be calculated at the sensitive volume of the die, taking into account the loss of energy through the layers (also considering BEOL and the passivation layers) and package (when delidding is not possible).

k. If the components on the board cannot be delidded, very high or ultra-high energy accelerator facility should be used.

    NOTE
    If the beam range is sufficient, the board can be tilted to increase the effective LET.

l. Proton test should be performed if heavy ion test shows sensitivity below 15 MeVcm^2/mg.

m. For EEE component level characterisation, minimum three proton energies between 50 MeV up to 200 MeV with fluence minimum 1E11 cm-2 should be applied at each energy, see ESCC25100 [S10], unless a statistically relevant number of events are recorded.

n. If destructive effects (SEB, SEGR, destructive SEL) are observed, the component / board should not be used

ANNEX 5, RECOMMENDATIONS FOR PCBS FOR CATEGORY Q1

The approach for assessment of PCBs used for COTS module of category Q1 is given by the following recommendations.

1. Printed Circuit Boards (PCB) should be procured as per IPC-6012ES, or ECSS-Q-ST-70-60.
   a. Any proposal that this quality class can be further lowered to IPC-6012E class 3 should be submitted for approval by ESA.
2. PCB manufacturers should be listed on the IPC QML or, alternatively, PCB manufacturers may hold a qualification from its customer as per IPC-6012ES, of from ECSS or NADCAP. This should be reviewed by the Satellite or Instrument Prime and their supplier during the equipment selection process (EQSR).
3. The design of the PCB and coupons should be compliant to IPC-2221B.
4. RF PCBs should be as per IPC6018CS.
5. The surface finish should be reflowed SnPb, ENIG or ENEPIG/ENIPIG. Solder mask may be used when this is technically required.
6. Hypercorrosion of ENIG should be evaluated to be in compliance with level 0 or level 1 as per IPC-4552. It is recommended that the PCB customer assesses the compliance of the PCB manufacturer to individual requirements from IPC-4552 for ENIG and IPC-4556 for ENEPIG/ENIPIG and that the compliance is reviewed by the Satellite or Instrument Prime. Note that "ESA-TECMSP-MX-11320 Checklist for ENIG ENEPIG ENIPIG finish" is available on www.escies.org/pcb/ to support such review.

7. The shelf-life of ENIG should be a maximum 6 months, otherwise a re-life test should be performed.
8. Particular care should be paid if state-of-the-art PCB technology is used. Examples are rigid-flex, microvias,back-drilling, metal core, 3-ounce (75 micron) copper foil or thicker, embedded film passives. It is recommended to use an aspect ratio for vias of max 7. In case microvias are used, it is recommended to use an aspect ratio of max 0.7 and not to stack them.
   An assessment of any possible use of state-of-the-art PCB technology and risk mitigations (such as test, inspection) should be submitted to ESA for review and approval.
9. It is recommended NOT to use tented vias (covered with solder mask) or blind vias with depth-controlled drilling (however, depth-controlled back-drilling for RF purpose is acceptable).
   Any use of the non-recommended technology should be described and submitted to ESA for review and approval.
10. It is recommended to use polyimide materials for the PCB. When using epoxy/FR4 laminate materials, they should have high temperature of glass transition (HTg FR4).
11. It is recommended that the PCB customer and the PCB manufacturer hold an MRR for the review of build-up, lay-out, panelisation, coupons, risk factors, compliance to release standard and compliance to capability.
12. All materials (PCB dielectric, solder mask, conformal coating, etc) should meet outgassing requirements.
13. IST coupons should be implemented for rigid-flex and micro-vias, back-drilling and high aspect ratio and should be tested in accordance with section 9.5.5 of ECSS-Q-ST-70-60.
14. All technology covered and not covered by IST should be specified and submitted to ESA for review and approval.
15. The PCB customer should perform incoming inspection of each batch covering the following:
    i. Review of CoC,
    ii. Microscopic inspection on coupons and
    iii. Visual inspection of all PCBs.

16. It is recommended to perform third-party evaluation of microsectioned coupons by an independent, IPC certified test lab.
17. The aspects of the incoming inspection of bare PCBs should be described in the appropriate documentation, including an assignment of the responsible institutes for these tasks, and submitted to ESA for review and approval.
18. High resistance electrical test with 1GOhm threshold is recommended and signature comparison should not be done
19. It is recommended to use 3x thermal shock (solder bath float at 280degC) for evaluation of coupons, instead of 1x.
20. In case microsectioning is already performed for evaluation of the assembly, as described in the table from annex 6, the evaluation of such microsectioning should also cover for an assessment of the quality of the PCB after test.

ANNEX 6, ADDITIONAL RECOMMENDATIONS FOR ASSEMBLY PROCESSES FOR Q1 AND Q0 CATEGORIES

The approach for assembly processes of COTS is provided by the following recommendations:

1. Use of Pb free solder alloys for category Q1 is not recommended. In case Pb free assembly processes are used the verification activities defined in Table 2 might be different. A dedicated Pb free assembly plan should be provided by the supplier.
2. Use of Pb free solder alloys for category Q0 is not allowed.
3. For categories Q1 and Q0 class3: companies which have assembly processes compliant to ECSS standards should apply the ECSS workmanship standards.
4. For categories Q1 and Q0 class3: workmanship standards per J-STD-001G Space addendum should be applied for companies with assembly processes not in compliance with ECSS standards.
5. Assembly on SnPb finished PCB is preferred, assembly on ENIG or ENIPIG/ENEPIG finishes is allowed
6. GEIA-STD-0005-02 should be applied for managing the risk associated with pure Sn finish (for Q1 control level 2B may be applied, for Q0 control level 2C)
7. Verification of the assembly reliability should be demonstrated as follow (tailoring being possible based on criticality of the unit considered):

    a. Review of procedures for compliance to the declared standard (ECSS or J-STD-001+ Space Addendum)
    b. Visit of manufacturing line by customers
    c. Inspection of available HW (recurrent unit already in manufacturing) to identify possible “show stoppers” (lack of de-golding on components, “risky” assembly configuration....)
    d. Review/definition of manufacturing process parameter control (statistical process control)
    e. For procured modules review of the failures and return from the field data.
    f. The assessment of the reliability of the assembly using SnPb solder alloys is based on functional testing at module level following one of the approaches described in Table 2.
    g. Assessment of results of the verification testing
    h. Identification of corrective action/improvement when necessary
    i. Review/Update of the statistical process control strategy
    j. MIP of test vehicles and of Flight Models to be attended.

Verification activities might be invalidated and require repetition in case of changes of design, processes, materials or changes in the components manufacturing/procurement
For modules of category Q0 Class 1 and 2 the requirements of ECSS-Q-ST-70-38C [S11] are applicable.

Table 2 Test conditions for assemblies using SnPb solder alloys

Application	Class	Designed modules	Procured modules (large volume of manufacturing)
One use single batch of procurement	Q2	No reliability testing of assembly	No reliability testing of assembly
	Q1	Annex 6 par. 7a,7b,7c,7d, 7f: vibration, shock, thermal cycling **3x mission time or equivalent to 100 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include repair configuration for selected type of devices. **Assessment by full functional test at RT, hot and cold.** Microsectioning may be applied to assembly sensitive devices or EEE components tested in a statistically non significative amount. Annex 6 par. 7g,7h,7i,7j,	Annex 6 par. 7b,7c,7d,7e 7f: vibration, shock, thermal cycling **3x mission time or equivalent to 100 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include repair configuration for selected type of devices. **Assessment by full functional test at RT, hot and cold.** Microsectioning may be applied to assembly critical devices or EEE components tested in a statistically non significative amount. Annex 6 par. 7g,7h,7i,7j,
	Q0 cl.3	Annex 6 par. 7a,7b,7c,7d, 7f: vibration, shock, thermal cycling **3x mission time or equivalent to 200 thermal cycles** (-55/+100C) whichever is the maximum. **Assessment by full functional test at RT, hot and cold.** Microsectioning to be applied to assembly sensitive devices, EEE components with heat dissipation pads underneath, and EEE components tested in a statistically non significative amount (**<10 for chip devices,**	Annex 6 par. 7a,7b,7c,7d,7e 7f: vibration, shock, thermal cycling **3x mission time or equivalent to 200 thermal cycles** (-55/+100C) whichever is the maximum. **Assessment by full functional test at RT, hot and cold.** Microsectioning to be applied to critical devices and EEE components tested in a statistically non significative amount (**<5 for chip devices <3 for other packages**). For critical devices 1 microsection.

Application	Class	Designed modules	Procured modules (large volume of manufacturing)
		<3 for other packages). For critical devices 2 microsections. pass fail criteria for cracks in solder joints: **75**% of critical area. Annex 6 par. 7g,7h,7i,7j,	pass fail criteria for cracks in solder joints: **75**% of critical area. Annex 6 par. 7g,7h,7i,7j,
Series manufacturing (use in constellation)	Q2	No reliability testing of assembly	No reliability testing of assembly
	Q1	Annex 6 par. 7a,7b,7c,7d, 6f: vibration, shock, thermal cycling **3x mission time or equivalent to 100 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include repair configuration for selected type of devices. **Assessment by full functional test at RT, hot and cold**. Microsectioning to be applied to assembly sensitive devices (2), EEE components with heat dissipation pads underneath, and EEE components tested in a statistically non significative amount **(<10 for chip devices <3 for other packages)**. Pass fail criteria for cracks in solder joints: **85**% of critical area. Annex 6 par. 7g,7h,7i,7j,	Annex 6 par. 7b,7c,7d,7e 7f: vibration, shock, thermal cycling **3x mission time or equivalent to 100 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include repair configuration for selected type of devices. **Assessment by full functional test at RT, hot and cold.** Microsectioning to be applied to assembly sensitive devices (2), EEE components with heat dissipation pads underneath, and EEE components tested in a statistically non significative amount **(<10 for chip devices <3 for other packages)**. Pass fail criteria for cracks in solder joints: **85**% of critical area Annex 6 par. 7g,7h,7i,7j,
	Q0 cl.3	Annex 6 par. 7a,7b,7c,7d,	Annex 6 par. 7a,7b,7c,7d,7e

Application	Class	Designed modules	Procured modules (large volume of manufacturing)
		7f: vibration, shock, thermal cycling **4x mission time or equivalent to 200 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include rework and repair configurations. **Assessment by full functional test at RT, hot and cold.** Microsectioning to be applied to assembly sensitive devices, EEE components with heat dissipation pads underneath, and EEE components tested in a statistically non significative amount (**<15 for chip devices <3 for other packages**). For assembly sensitive devices **3** microsections Pass fail criteria for cracks in solder joints: **75**% of critical area. Annex 6 par. 7g,7h,7i,7j,	7f: vibration, shock, thermal cycling **4x mission time or equivalent to 200 thermal cycles** (-55/+100C) whichever is the maximum. Test vehicle to include rework and repair configurations. **Assessment by full functional test at RT, hot and cold.** Microsectioning to be applied to assembly sensitive devices, EEE components with heat dissipation pads underneath, and EEE components tested in a statistically non significative amount (**<10 for chip devices <3 for other packages**). For assembly sensitive devices 2 microsections. Pass fail criteria for cracks in solder joints: **75**% of critical area. Annex 6 par. 7g,7h,7i,7j,

ANNEX 7, ELECTRICAL SAFETY BARRIER EXAMPLES

A7.1 Power lines

In the following example (Figure 13) unit1 is considered part of the reliable satellite platform of criticality class Q0 and unit1 is thought to be part of the equipment of criticality class Q_2 or Q_1.

The power supply line from unit 1 is configured as a current limited voltage source.
In case of unit 2 overload, the line is opened thanks to the latching current limited provision after a predefined time, so preventing failure propagation.

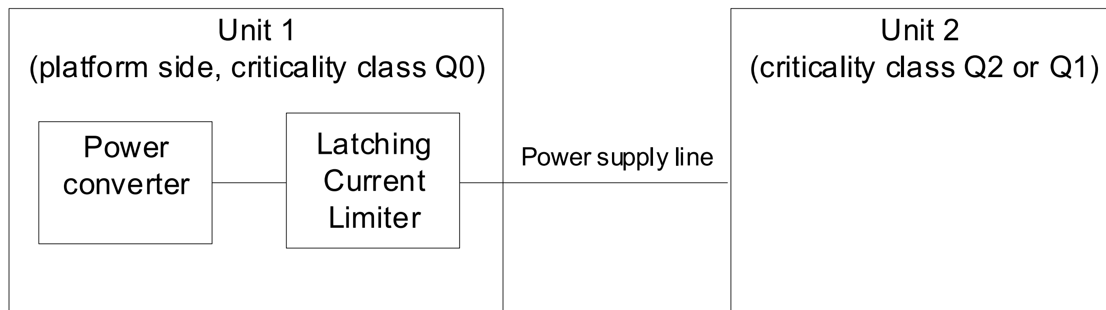


Figure 13, Power line example

A7.2 Signal lines

Two examples are provided, the first (Figure 14) relevant to a slow serial line case, where it is possible to add serial decoupling resistors without affecting the communication, the second (Figure 15) where it is not possible to add serial decoupling resistors because they would affect the communication.
In both examples, unit1 is thought to be part of the equipment of criticality class Q2 or Q1 and unit2 is considered ad part of the reliable satellite platform of criticality class Q0.

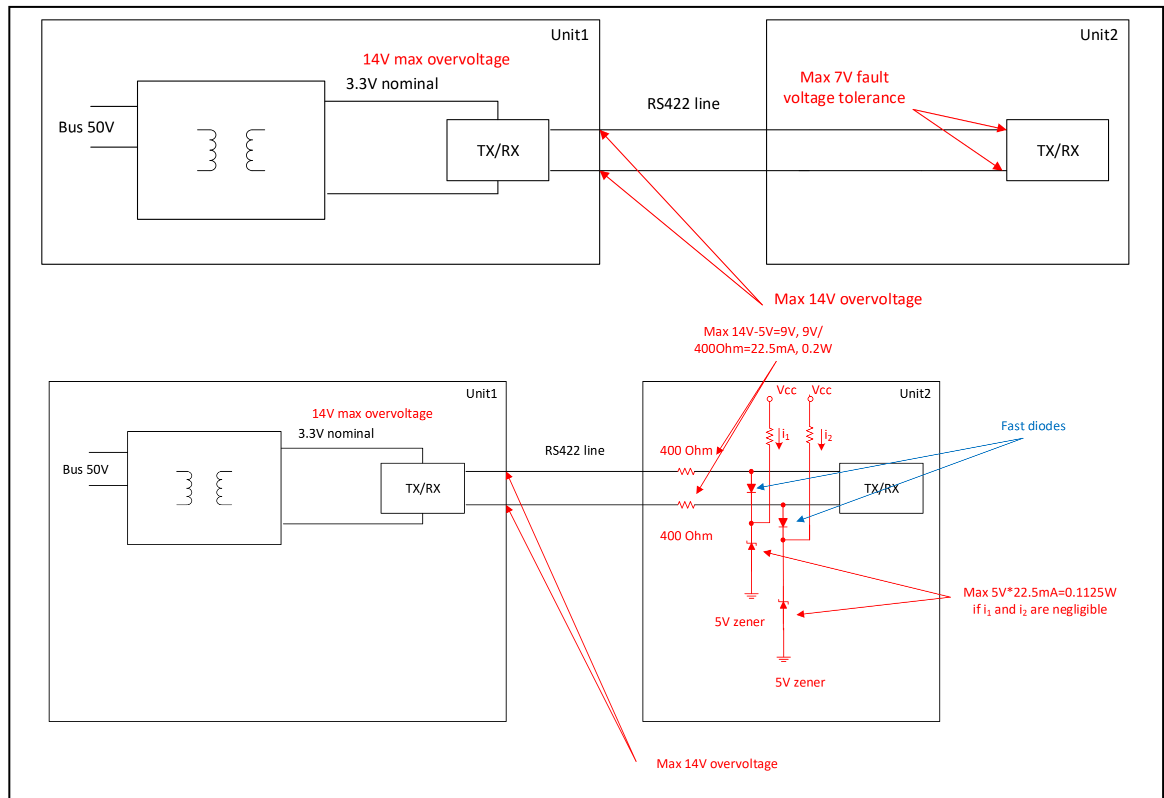


Figure 14, Slow serial line example (it is possible to insert decoupling resistors without affecting the communication)

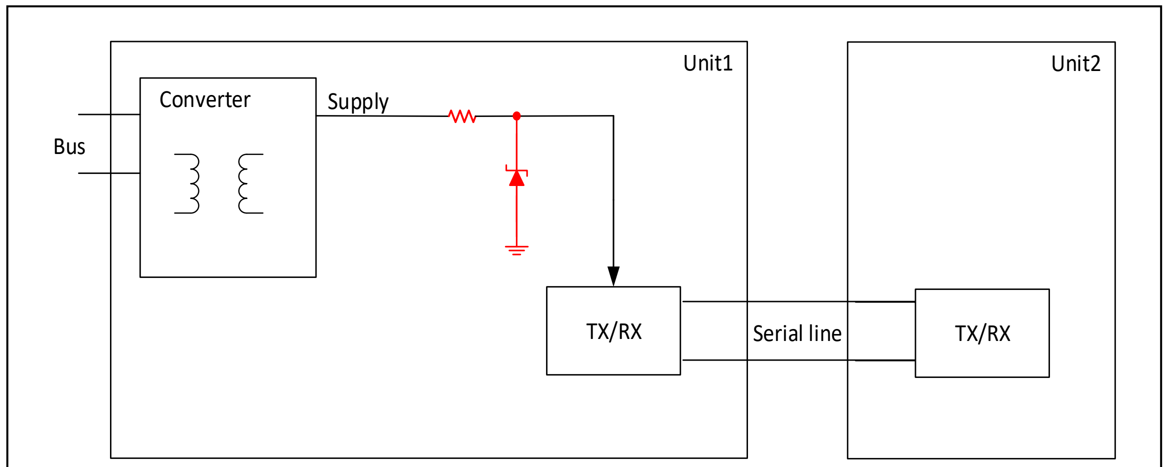


Figure 15, Fast serial line example (it is not possible to insert decoupling resistors without affecting the communication)

In the example of Figure 15 the voltage emission at the unit 1 interface is controlled by the presence of the zener diode, also in case of failures in the converter causing over voltage conditions at its supply output. In this way it is possible to control the overvoltage emission to Unit 2 under the applicable fault tolerance limits.