# Product Assurance and Safety Approach to New Space in ESA Projects

Lorenzo Marchetti (PA&S Engineer, Product Assurance & Management Section TEC-QQM)

ESA-TECQQM-HO-2024-001195 is. 1

Workshop “L’impegno italiano nel settore dei CubeSat: tecnologie e missioni future” – 2° edizione
July 2024

# Outline

- ECSS vs. Mission Complexity and Risk
- Product Assurance & Safety – Key Requirements
- New Space
- How to use the ECSS in the frame of New Space?
- Product Assurance & Safety Approach with ESA Mission Classification Scheme
- Integration of CubeSat Guidelines into ESA Mission Classification Scheme
- Support Tool: ESA TRL Calculator
- Conclusions & Take-Aways
- Q&A
- Bibliography and Backup slides

# ECSS vs. Complexity and Risk

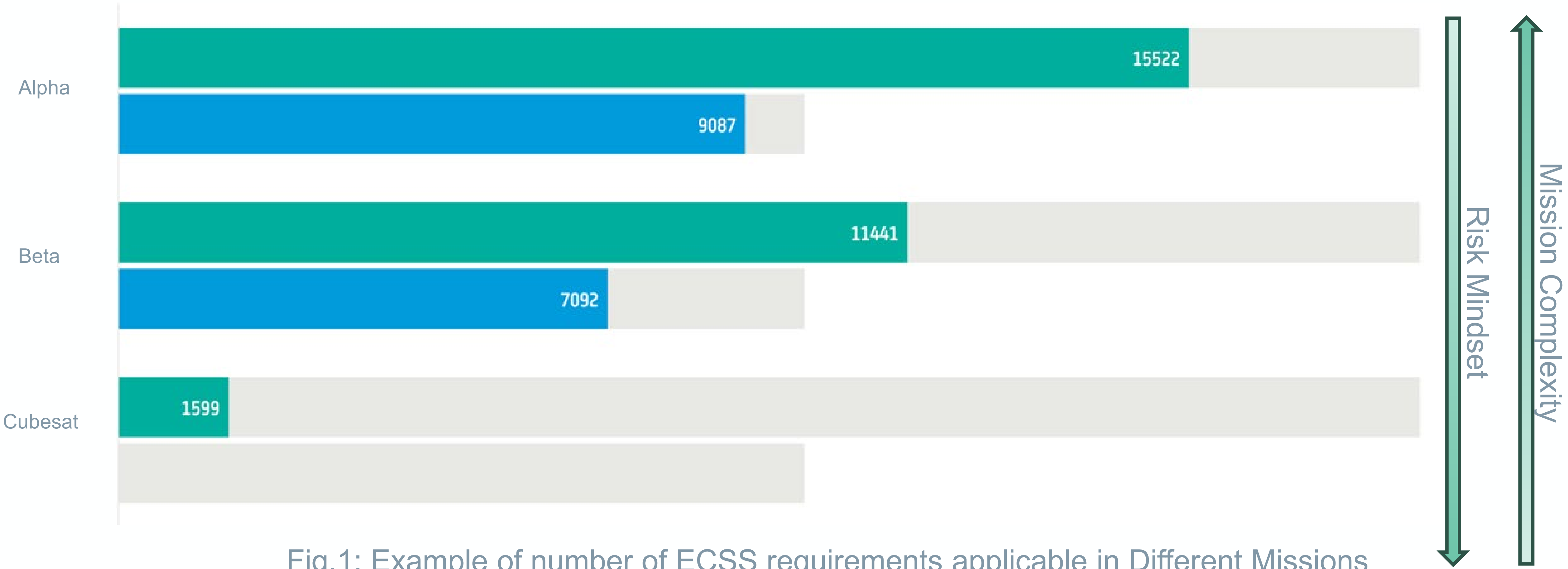



Fig.1: Example of number of ECSS requirements applicable in Different Missions

Adapted from TEC-QES (ESA Requirements and Standards Section) exhibit

# Product Assurance & Safety – Key Requirements

- In ESA, the PA engineer work is based on the management and coordination of experts and execution of processes which are thoroughly normed inside the ECSS (*European Cooperation for Space Standardization*), in particular in the ECSS Quality standards (Q-branch of the ECSS)
- As of now, the complete Q-branch contains **~12600 requirements** [incl. DRD's]

- As a comparison, let's consider a CubeSat: the main normative references applicable to CubeSats, according to ISO, are
  - ISO17770 Space systems — Cube satellites (CubeSats – **15** QA/PA req's))
  - ISO14620-1 Space systems — Safety requirements — Part 1: System safety
  - ISO24113 Space systems — Space debris mitigation requirements

- The ECSS applicable as-is looks **conservative** given the mission profiles, and more in general, for what is now referred to as New Space Projects

**PA/QA**
ECSS-Q-ST-10 and 20

**Dependability**
ECSS-Q-ST-30

**Safety**
ECSS-Q-ST-40

**EEE components**
ECSS-Q-ST-60

**Materials, mech. parts, processes**
ECSS-Q-ST-70

**Software PA**
ECSS-Q-ST-80

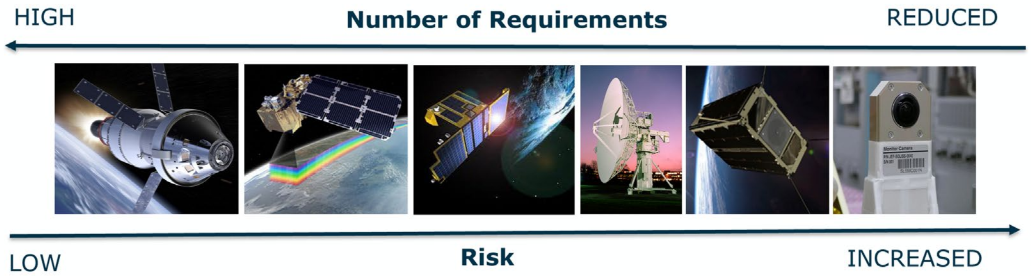
# New Space

**New Space**, in large part, is a concept based on a different **PROCUREMENT** approach w.r.t to the past. It goes in the direction of widening the **ACCESS** to Space to private companies or academia which might not have a long history of space programs.

With respect to a mission there are a few key differences:

1. **Accessibility** to smaller investors, lower mission cost, faster turnover is a MUST
2. **Reliability** (traditionally a major cost driver) must be balanced against cost and schedule constraints
3. The mission is generally of **short duration**, so reliability goal is easier to achieve
4. It normally relies on large usage of **COTS** [Commercial off-the-shelf]
5. The optimal design is traded-off with **modularity** and interchangeability of parts
6. ECSS is often used as a **reference only** in Contracts

# How to use the ECSS in the frame of New Space?




How ***deep*** do we need to go in order to **gain confidence** that our Processes, Materials, EEE, etc are **reliable** enough to be used in our New Space missions, without using the **complete ECSS**?

**The answer is given by the ESA Mission Classification (EMC) Scheme (ECSS Pre-Tailored** requirements for ESA missions)

- The EMC encompasses one-off missions, recurring operational spacecrafts, IOD/IOV and CubeSats
- Satellite mega-constellations and launchers are **not addressed**
- **More flexibility** is given to Industry as a function of class of the mission (highest flexibility and associated risk for class Delta), but also more reliance of ESA on contractor's internal processes, more simplification of the documentation and required reporting, at the cost of the less visibility given to ESA and more delegation of responsibility and of risk is given to industry
- The EMC is supported, when needed, by the **ESA TRL Calculator** (10) to properly assess the maturity of the technology when under development up to qualification, isolating gaps in design and test/validation by means of checklists.

# PA Approach – ESA Mission Classification [2/2]

In the updated ESA Mission Classification Scheme 4 different mission classes have been identified

WORK UNDER PROGRESS

| Mission Characteristics Criteria & Related Weighting Factors | | Class Level: Alpha | Beta | Gamma | Delta | Input Score (1/2/3/4) | Weighted Score |
|---|---|---|---|---|---|---|---|
| **Acceptable Risk**<br>Risk of mission failure which is agreed acceptable to management | | LOW | → | → | HIGH | | |
| **Criticality to Agency Strategy**<br>Flagship mission, international co-operation, impact of strategic ESA goals and image. | | Extremely Critical | Highly Critical | Medium Criticality | Low Criticality | | |
| WF (10/20/30 %): | 20 | | x | | | 2 | 0.40 |
| **Mission Objectives**<br>Directorate priority and purpose e.g. In orbit demonstration, educational. | | Top Priority | High Priority | Medium Priority | Low Priority | | |
| WF (10/20/30 %): | 20 | | x | | | 2 | 0.40 |
| **Cost**<br>Cost at completion inc. Phase E1 | | > 400 M€ | 200 - 400 M€ | 25 – 200 M€ | < 25 M€ | | |
| WF (10/20/30 %): | 20 | | | | x | 4 | 0.80 |
| **Mission Lifetime**<br>Nominal mission life duration | | > 7 years | 5 -7 years | 2-5 years | < 2 years | | |
| WF (10/20/30 %): | 20 | | x | | | 2 | 0.40 |
| **Mission complexity**<br>Design interfaces, unique payloads, new technology development. | | Extremely Complex | Highly Complex | Medium Complexity | Low Complexity | | |
| WF (10/20/30 %): | 20 | | | | x | 4 | 0.80 |
| **Total % (must be 100):** | **100** | | | | | **Total (*):** | **2.80** |
| | | | | | | **CLASS:** | **Gamma** |

<<< Resulting Mission Class

WF: Weighting Factor (10, 20, 30)

>>> Use pull-down menu to select value

| Class | Mass [Kg] |
|---|---|
| Pico | < 1 |
| Nano | 1 – 10 |
| Micro | 10 – 100 |
| Mini | 100 – 500 |

# Integration of Cubesats Requirements in the ESA MC

**There is an-going work to integrate the Cubesat Guidelines developed in ESA into the ESA Mission Classification.**

**The ESA Cubesat Guidelines define the following best-practices:**

**Activity Record and Management**

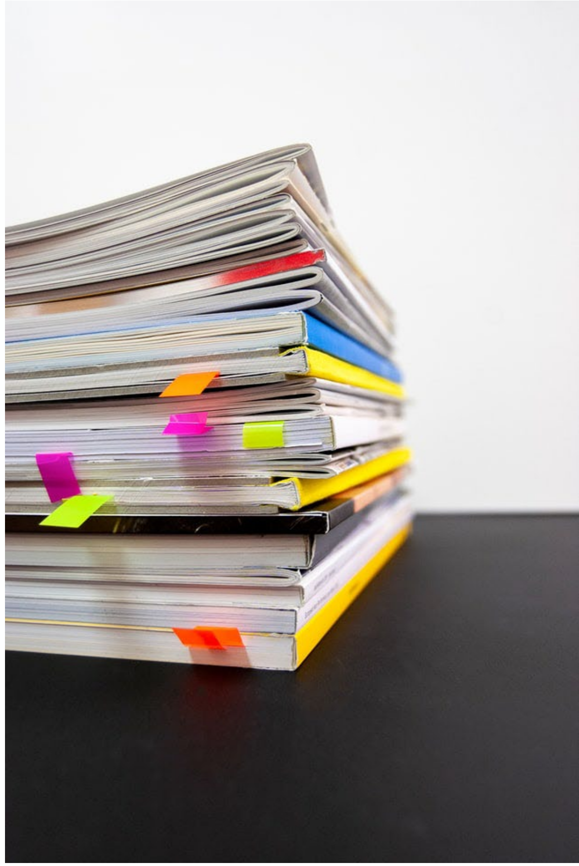
- The Verification Control Matrix vs. Engineering Specs is a key deliverable
- Tracking of Anomalies/Non Conformances (NCR) is mandatory

**System Reliability and Availability**

- **Derating** for Electrical, Electronic and Electro-mechanical (EEE) components selection is required
- Application of **stress margins** for mechanical parts is recommended
- Functions are classified in accordance with criticality, as per ECSS
- Failure Mode Effect Analysis (FMEA) should be performed. Single-Point Failures (SPFs) may be accepted.
- The FMEA is an input to the Failure, Detection, Isolation and Recovery (FDIR), and SAVOIR architecture can be used as a reference for the FDIR implementation
- Radiation wise, Single Event Effect (SEE) risk analysis is recommended. Total Ionising Dose (TID) is generally of low concern

**Model Philosophy**

- PFM is the norm – EM Avionics Test Bench is used to test SW before in-orbit SW update



# Integration of ESA IOD Cubesats Requirements in the ESA MC

**EEE components and Radiation Harness Assurance (RHA)**

- Baseline is EEE COTS. ESA COTS guidelines (8) may be used as a reference
- In case data is not available, Rad Test should be performed, generally at board/module level
- Reduced Declared Component List (DCL) is **mandatory** to keep track of components being used
- Perform burn-in testing @ board level for a duration of 168 hrs at max. acceptable equipm. temperature

**Materials & Processes**

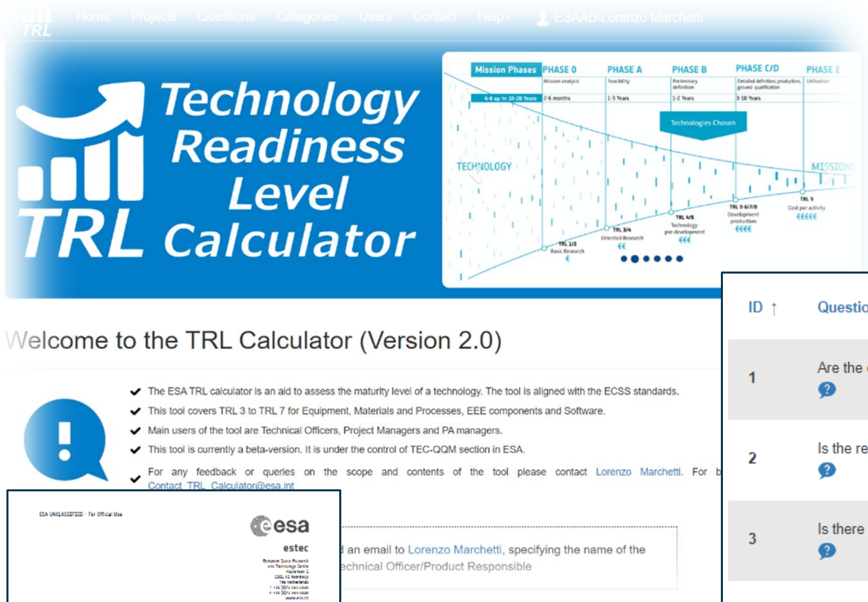
- Reduced Material, Process and Mechanical Part Lists are **mandatory** including basic information like outgassing data, quantity of material, evidence of previous space usage
- Pure tin removal might be worse than living with it, given the short mission duration
- Assembly: Class 3 IPC certificate for soldering is required
- Cleanliness: Visibly clean is generally acceptable

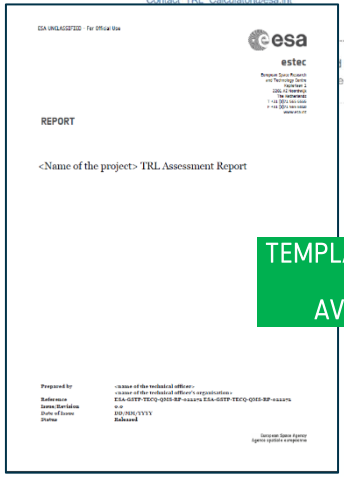
**Software**

- The approach is to abide by recognised coding standards, to perform unit testing, measure code coverage
- Minimum amount of SW documentation that needs to be provided to properly design, verify and validate SW

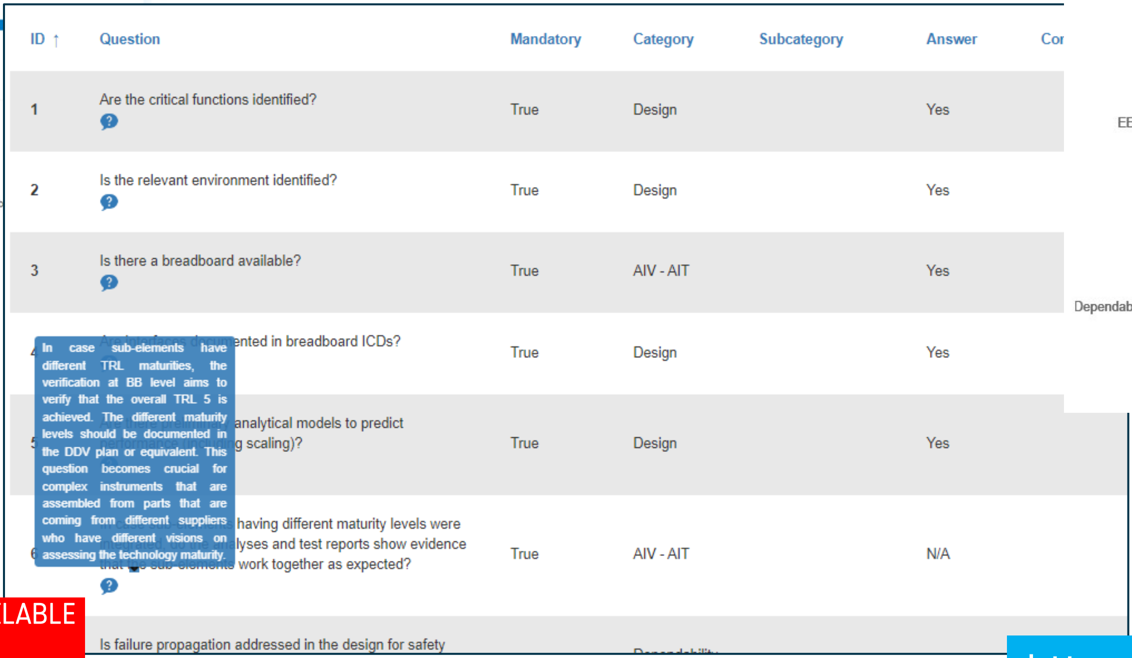
# Support tool: ESA TRL Calculator [1/2]

ESA TRL Calculator is available to Industry (https://trlcalculator.esa.int). It embeds path-to-flight approach for Design, AIV/AIT, PA, M&P, EEE, SW, RAMS, Management



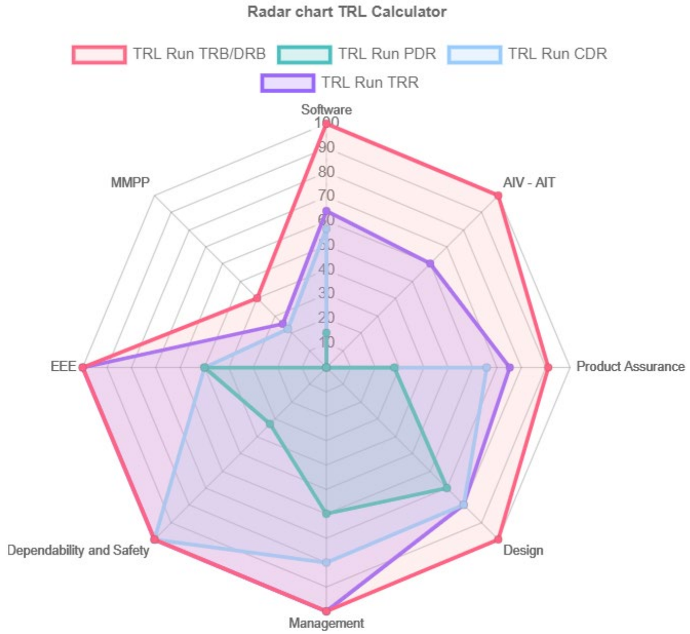

TEMPLATES EASILY AVAILABLE



| ID ↑ | Question | Mandatory | Category | Subcategory | Answer | Cor |
|---|---|---|---|---|---|---|
| 1 | Are the critical functions identified? | True | Design | | Yes | |
| 2 | Is the relevant environment identified? | True | Design | | Yes | |
| 3 | Is there a breadboard available? | True | AIV - AIT | | Yes | |
| 4 | …ented in breadboard ICDs? | True | Design | | Yes | |
| 5 | …analytical models to predict …g scaling)? | True | Design | | Yes | |
| 6 | …having different maturity levels were …lyses and test reports show evidence that …sub-elements work together as expected? | True | AIV - AIT | | N/A | |
| | Is failure propagation addressed in the design for safety | | Dependability… | | | |



CHECKLIST AVAILABLE FOR EACH TRL



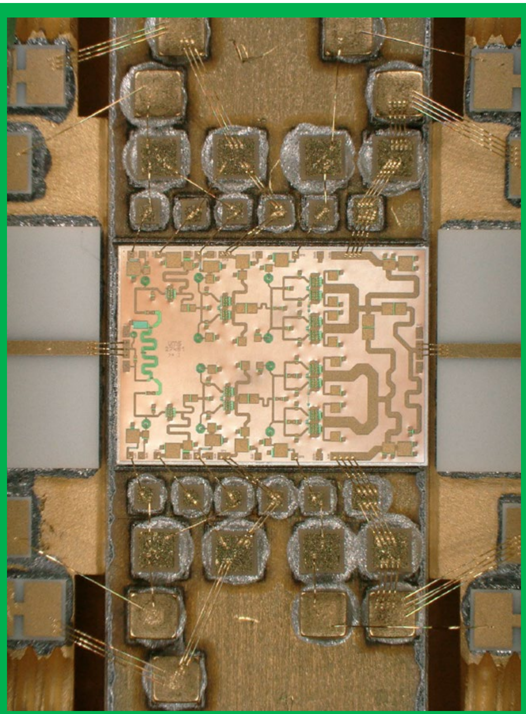

SPIDER CHART FOR EACH AREA AND FOR DIFFERENT MILESTONES

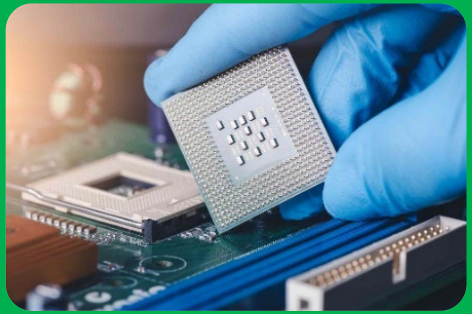
https://trlcalculator.esa.int

# Support tool: ESA TRL Calculator [2/2]

- The use of the ESA TRL calculator defines **what is needed** to achieve a specific level of technology maturity, since the early inception of a contract until the delivery
- The tool helps the Project Team to monitor the progress of the activity in all engineering and **PA/QA areas**, across the complete development and qualification lifecycle
- The tool comes with a **set of templates**, ready for use

- The tool supports industry, especially newcomers to space business, SMEs, Academia and Research Institutes on the information to be provided for achieving a target TRL
- It matches the **New Space** needs as it focuses on the **DOCUMENTED INFORMATION** to be provided, not strictly on a standard, whilst keeping the **ECSS "attitude"** on what is needed to gain confidence that a "quality product" is delivered
- It is a valuable tool to "**educate**" space newcomers on how a space business activity should be carried out with the support of the Agency
- ESA runs **two Training Sessions** per year on TRL for Industry under the ESA Learning Hub





# Conclusions and Take-Aways [on-going work]

- Product Assurance aims at assuring that a space product conforms to the requirements
- This is done by controlling processes, materials, EEE, SW, etc at multiple stages in a project life-cycle
- The PA tasks are normed in the ECSS
- The complete ECSS is generally too heavy for New Space projects → A pre-tailored or technology-oriented approach can be followed
- **Reliability vs. "Budget&Schedule"** constraints is of major concern for PA in New Space Projects
- The proposed approach relies on the use of :
- ESA Mission Classification ***Gamma Class*** with:

  ESA Cubesat Guidelines to be integrated into MC Class Gamma and Delta

  and supported by ESA TRL Calculator, for new tech development [10]
- Status:
  - The ESA Mission Classification [14] is close to full release (expected CMIN 25)
  - The ESA Cubesat Guidelines [9] integration into MC is to be completed by Summer 2024
  - The ESA TRL Calculator [10] is now released in version 1.1

# Bibliography


[1] ECSS-Q-ST-60C Rev. 3 — Electrical, electronic and electromechanical (EEE) components

[2] ECSS-Q-ST-60-13C Rev 1 — Commercial electrical, electronic and electromechanical (EEE) components

[3] ECSS-Q-ST-60-15C — Radiation Hardness Assurance for EEE components

[4] ECSS-Q-ST-30-11C Rev. 2 — Derating for EEE components

[5] ISO17770 Space systems — Cube satellites (CubeSats)

[6] ECSS-E-ST-10-04C Rev. 1 — Space Environment

[7] IAA: 978-2-917761-59-5 — Definition and Requirements of Small Satellites Seeking Low-Cost and Fast-Delivery

[8] ESA-TEC-TN-021473 — ESA COTS guidelines

[9] ESA-TECSPC-MAN-2023-002445 — Engineering ESA CubeSats Guidelines

[10] ESA TRL Calculator — https://trlcalculator.esa.int/

[11] ECSS-Q-ST-30C Rev. 1 — Dependability

[12] SAVOIR-HB-003 is 2 — Savoir FDIR Handbook

[13] ESA-TECSPC-RS-024342 — PA Requirements for In-Orbit Demonstration CubeSat Projects

[14] ESA-TECQQM-WP-016256 — White Paper: ESA Mission Classification

[15] ESA-TECQQM-RS-2023-001942 — Generic Template for PARD Mission Class IV

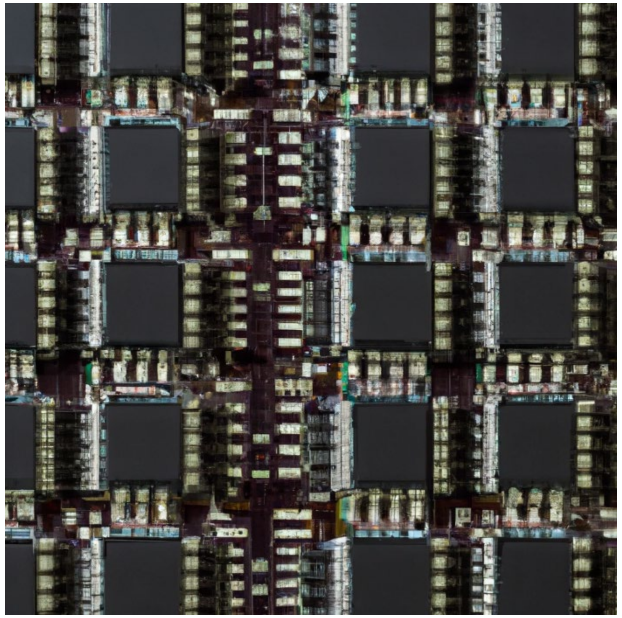
[16] Cost Impacts of Upgrading Electronic Parts for Use in NASA Space Flight Systems (Plante, Sampson)

# Backup Slides

FOCUS on PA for Gamma Missions

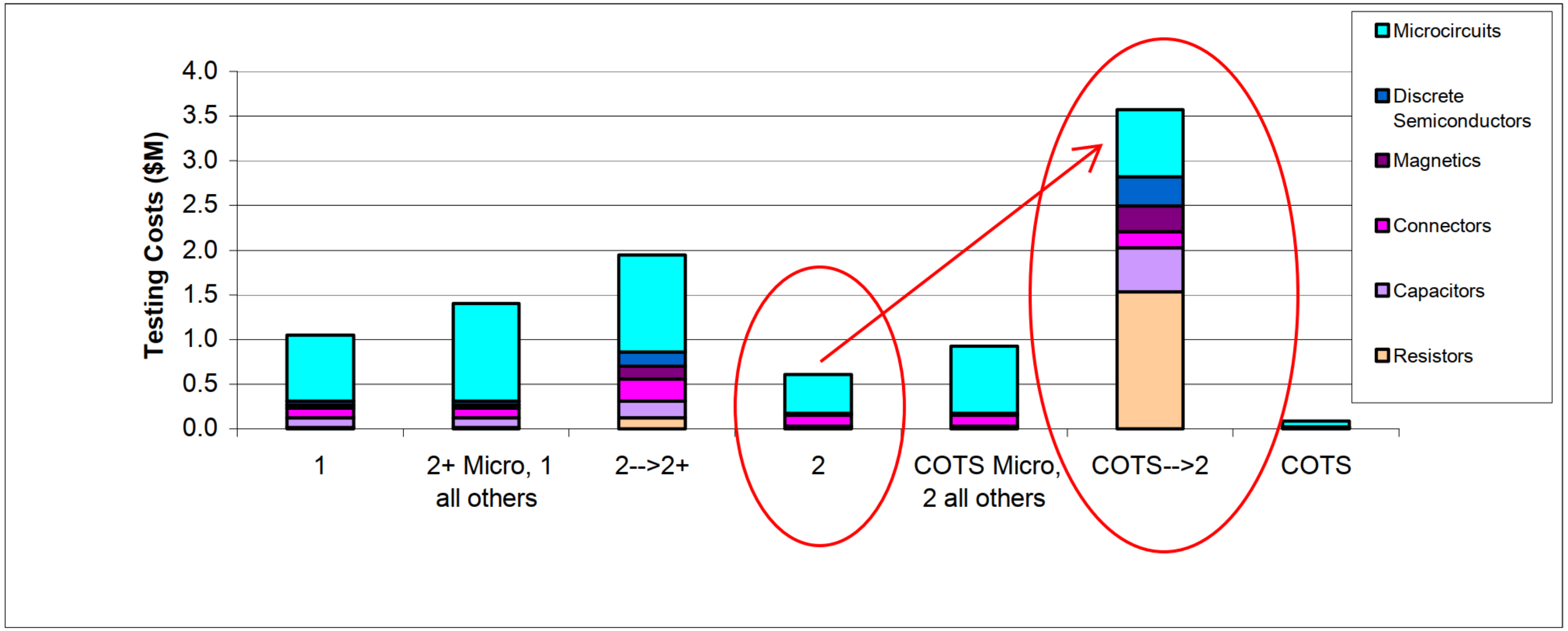
# EEE, COTS, RHA and RAM

# [Introduction]



# Some numbers for non-RHA testing

Figure 4. Cost of Parts with Upgrading Testing Costs Added to the Procurement Costs




Source: Cost Impacts of Upgrading Electronic Parts for Use in NASA Space Flight Systems (NASA)

***Take-away: upgraded parts are always more expensive than level-ready parts***

# A dive into EEE components for Gamma missions

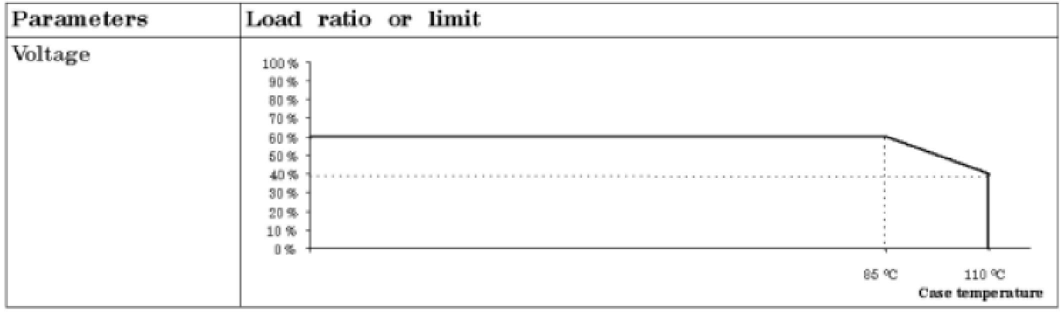
| Procurement and Approval | Remarks |
|---|---|
| Quality Baseline is ECSS (ST-Q-60) Class 3 type of EEE Components, with further relaxations.<br>These requirements are to be applied to equipment deemed as ***critical*** for the success of the mission | ***Class 3 EEE Components*** has the lowest procurement cost, lowest assurance and highest risk among the three classes. Note: The ECSS has its own classification which is different from the MIL-STD. |
| • The supplier is NOT responsible for manufacturer surveillance<br>• Screening is NOT applied to **ALL** components<br>• **Screening** is NOT performed by a certified entity (ex: ESCC)<br>• In case of screening, less stringent requirements apply. For example, on oscillators, chip inductors, wires<br>• **Lot Acceptance Testing** is NOT required for Class 3. It is only required for COTS<br>• **Pre-cap** and **Buy-off** inspections are NOT required<br>• A Program Status of Compliance [**SoC**] to the Q60 is NOT required<br>• A Parts Control Board [**PCB**] is NOT required<br>• A Declared Part List **[DCL]** is STILL required<br>• Control over non-hermetically sealed materials of components is mandatory<br>• Use of **pure tin** inside or outside the part is to be declared in the PAD ← it is up to the project, in any case, to define the specific policy, based on risk assessment | ***Space qualified*** means that the component belongs to a Qualified Parts List [QPL] or a Qualified Manufacturers List [QML] that are recognised by a third-party organization (e.g. ESCC, MIL, NASA, JAXA)<br>______________<br>***Pure Tin*** refers to a content of tin (Sn) inside the alloy of the component higher than 97% of the mass. For soldering applications, in general it is 93% minimum. Please always check against the standards!<br>______________<br>A ***PAD*** is a control document that identifies the component and provides info about its acceptability vs. procurement specs, Lot Acceptance Test [LAT], Radiation Verification Tests [RVT], etc.<br>______________ |

# A dive into EEE COTS components for Gamma missions

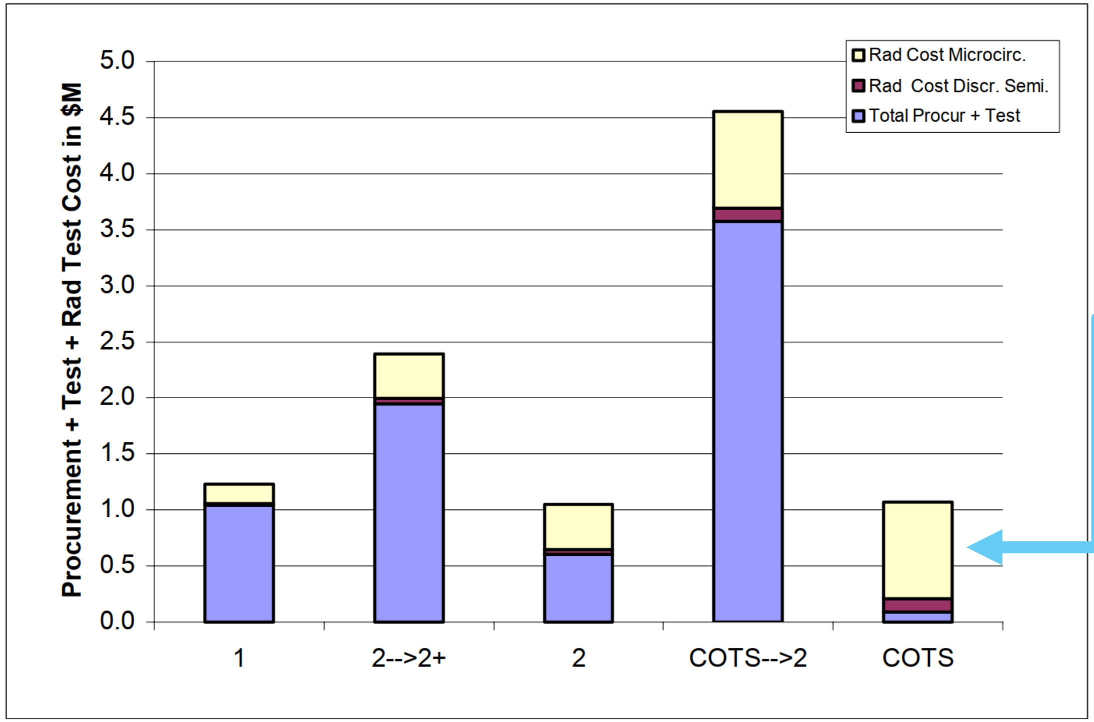
| Procurement and Approval | Remarks |
| --- | --- |
| The ECSS COTS standard aims to **raise the assurance** for COTS components to the same level of one of the previous three space grade Classes.<br>Consequently, for Class IV mission, **COTS Class 3** requirements apply. | ***COTS EEE:*** commercial electronic component, procured from the market, readily available and not manufactured, inspected or tested in accordance with military or space standards. |
| A key piece of information for COTS is the **trace code**, to guarantee lot homogeneity among procured COTS.<br>The assessment of commercial components is done through JD, and evaluation plan is to be approved by the Customer.<br>*Strong relaxation*: for COTS, there is **no minimum content** to be included in the Justification Document, but Customer's approval is needed. In addition, JDs for multiple components can be combined. | ***Trace Code*:** identifier used by a manufacturer to label and trace a quantity of components with **AT LEAST** a common assembly history.<br>________________<br>A ***Justification Document*** for an OTS is akin to what a Part Approval Document is for a Space grade component. |
| Destructive Physical Analysis can be waived for AECQ-100 and AECQ-200 components, in general | |

# A dive into Derating for Gamma missions

| Policy for derating | Remarks |
|---|---|
| The **baseline** policy for derating EEE and COTS components is to be in accordance with the ECSS → **no exceptions** | ***Derating***: to design a **product** to limit the **component** stresses below their ratings, to increase product's reliability<br>***Rating***: max parameter value specified and guaranteed by the manufacturer, not to be exceeded during operations [e.g. current, voltage, power, temperature] |
| The rules of ECSS derating apply to steady state, surge and transient conditions | ***Surge***: strong rush or sweep<br>***Transient:*** brief change in the state of a system |
| Part Stress Analysis [**PSA**] is mandatory | The PSA could be a heavy document, and the contractor needs to be aware |
| In case of components sensitive to **radiation**, then ECSS RHA requirements apply | Limits on current and voltages to get a proper Radiation Design Margin [RDM] imposed by RHA might be more severe than ordinary deratings. |



# Some numbers for RHA testing




Cost for Rad testing increases the cost of COTS by 1100%

Total cost of ownership including Radiation Testing (Source: [16])

# A dive into RHA for Gamma missions

| Radiation Verification Testing [RVT] | Remarks |
| --- | --- |
| A Radiation Hardness Assurance [**RHA**] Program is mandatory for radiation sensitive components | ***RHA*** is a systematic process of ensuring that EEE components can operate reliably in the presence of ionising and non-ionising radiation |
| The RHA Program is project specific, and orbit related<br>RHA can be split into TID RHA, TNID RHA, SEE RHA.<br>For LEO missions, RDM > 1 in general and to be submitted to Customer for approval, if not otherwise defined. | ***TIDL*** Calculated Total Ionising dose Level received by the part at the end of the mission. ***Rad-hard components*** are generically the ones that can withstand high TIDL.<br>__________________<br>***RDM,*** is radiation design margin; conceptually, it is analogue to ***derating,*** i.e. it introduces a design safety margin vs. the max dose that a component can absorb before it exceeds its functional requirements. |
| In case of lack of data for Class 3 EEE components, the approval and execution of the **RVT** is subject to Customer's approval. | ***RVT*** is Radiation Verification Testing |
| When components or units come with no info on RHA:<br>• If TIDL less than 5 krad, no test is needed<br>• If TIDL higher than 5 krad, RVT can be carried out at board level<br>• In case of potential sensitivity to SEE, proton testing is needed | Proton testing can be performed at board/module level. |

It might be difficult to get evidence that the tested board includes components having the same ***lot homogeneity*** as the flight ones → if no RHA data is available, the same flight **procurement lot** can be tested on ground (best effort strategy).

# A dive into RAM for Gamma missions

| Dependability | Remarks |
|---|---|
| A **Dependability Assurance Plan** is not needed, but the dependability critical items criteria are to be defined in any case | The critical items are recorded in the CIL (Critical Item List) – the content of the CIL is defined by the Project. |
| **Failure tolerance** is not mandatory: relevant requirements can be tailored by the Project | For a Cubesat, single-point failure (SPF) is in general accepted |
| **Severity categories** (Catastrophic/Critical/Major/Minor) are the standard ones<br><br>The Classification of **critical functions** (I, II, III and IV) is the standard one | |
| Reliability heavily relies on heritage and proven design rules | |
| The SW criticality follows the usual rules for SW (typically Cat B, C and D) | |
| FMEA & HSIA [reduced]<br>WCA [reduced]<br>FDIR analysis mandatory | FMEA: Failure Modes and Effects Analysis<br>HSIA: Hardware and Software Interaction Analysis<br>WCA: Worst-Case Analysis<br>FDIR: Failure Detection, Isolation and Recovery |
| FTA not mandatory<br>Zonal Analysis not mandatory | FTA: Fault Tree Analysis |

Reliability figures/analyses @Payload level are generally not REQUIRED; @Platform Level, they might be required to support **Space Debris Mitigation** requirements (SDM)