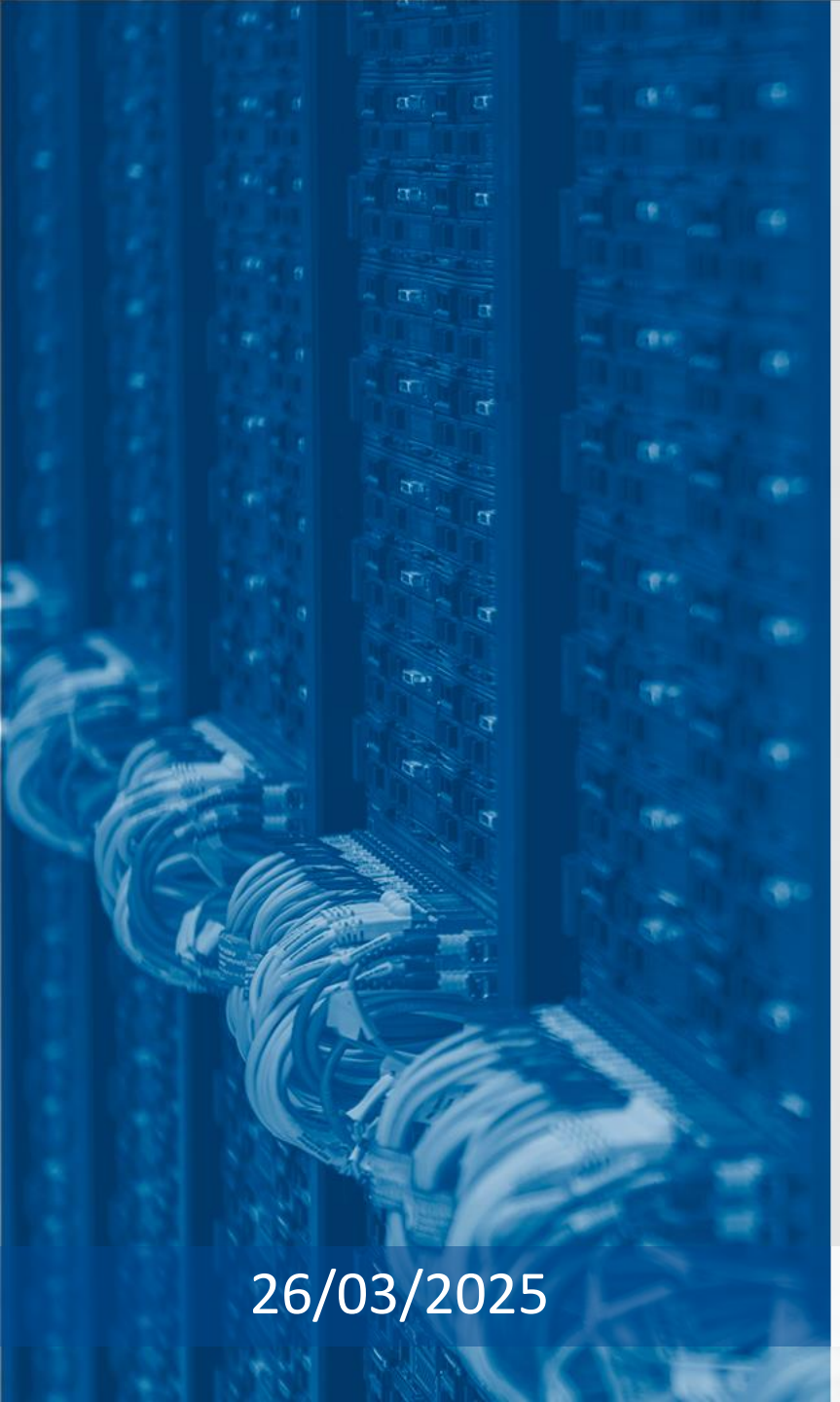


Reusing Automotive Certification and Qualification standards

Leonidas Kosmidis[1,2], Ivan Rodriguez-Ferrandez[1,2] David Steenari[3]

[1]Universitat Politécnica de Catalunya

[2]Barcelona Supercomputing Center

[3]European Space Agency

26/03/2025

ACCEDE 2025

ASIL2ECSS: Project

- ASIL2ECSS: Reusing Automotive Certification and Qualification Standards to Lower the Cost of Space Certification and Qualification for COTS Processors/SoC
- ESA-funded OSIP project in the “New ideas for the use of Commercial Off The Shelf (COTS) components” campaign.
- Planned duration 12 months
- Budget 100K
- November 2021 - December 2023

ASIL2ECSS: Introduction

Why ASIL2ECSS?

- The high cost of space qualification is a significant barrier to innovation.
- Automotive electronics are rigorously tested for safety and reliability under ISO 26262 standards.
- Can we reuse these automotive qualifications to accelerate space certification and reduce costs?
- **Objective:** Create a structured mapping between ECSS (European Cooperation for Space Standardization) and ISO 26262, identifying gaps and additional requirements for space use.

The Need for Cost Reduction in Space Qualification

- **Space industry challenges**:
  - Stringent qualification processes lead to high costs and long timelines.
  - Custom-designed space electronics are expensive and limited in availability.
  - Increasing interest in COTS components for space missions.
- **Automotive industry advantages:**
  - Mass production of high-performance, safety-critical electronic components.
  - Established certification standards such as ISO 26262 and AEC-Q100.
  - Potential cost and efficiency benefits if automotive-certified components can be adapted for space.

Key Standards Involved

- **Space Standards (ECSS):**
  - ECSS-Q-ST-40C: Safety
  - ECSS-Q-ST-60-15C: Radiation hardness assurance for EEE components
  - ECSS-Q-ST-30-02C: Failure modes, effects, and criticality analysis (FMEA/FMECA)
  - ECSS-E-ST-40C: Software engineering
- **Automotive Standards:**
  - ISO 26262: Functional safety of automotive electronic systems.
  - AEC-Q100: Qualification standards for automotive electronic components.
  - JEDEC JESD89B: Soft error testing for semiconductors.

High-Level Differences Between ECSS and ISO 26262

- **ECSS (Space)**
  - Comprehensive system-level assurance (safety, reliability, radiation effects).
  - Focuses on mission success and longevity in extreme conditions.
  - Requires end-to-end qualification and traceability.
- **ISO 26262 (Automotive)**
  - Ensures functional safety for electronic and electrical systems in vehicles.
  - Defines safety integrity levels (ASIL) to classify risks.
  - Emphasizes fault tolerance, fail-safe mechanisms, and high reliability.
- **Key Challenge:** ISO 26262 does not address space-specific environmental factors such as radiation effects.

The V-Model Development Approach

- **V-Model in Space and Automotive**
  - Both sectors use a V-Model for system development, verification, and validation.
  - Requirements are defined and refined at the system level.
  - Components are integrated and tested progressively.
- **ISO 26262 V-Model**
  - Focuses on functional safety lifecycle from concept to decommissioning.
  - Includes ASIL determination, hazard analysis, and validation.
  - Requires reviews between the project phases
  - ISO26262 only defines the V process for safety
- **ECSS V-Model**
  - ECSS defines the V model for the full project, also defining more concrete project phases.
  - ECSS also required reviews between the project phases, but defines the content with more detail than ISO
  - Includes additional steps for mission assurance and space-specific testing.

Hardware Qualification – ISO 26262 vs. ECSS

ISO 26262 Hardware Development Process

- **Hardware Design and Safety Measures**
  - Requires detailed **failure rate analysis** and **diagnostic coverage** evaluation.
  - Uses **quantitative hardware metrics** to assess the probability of violation of safety goals.
  - Safety mechanisms include **fault detection, error correction, and redundancy**.
- **Evaluation of Hardware Elements**
  - Hardware elements are classified based on **failure rates, fault tolerance, and safety mechanisms**.
  - Requires **statistical analysis and reliability assessment** to ensure robustness.
  - Defines **fault injection testing** to verify system response to failures.
- **Environmental Testing in Automotive Standards**
  - ISO 26262 does not cover environmental stress; instead, **AEC-Q100** is used for testing under **temperature, humidity, vibration, and mechanical shock conditions**.
  - Radiation effects are primarily evaluated for **neutron-induced soft errors**, but **space missions require additional radiation hardness assurance**.

Hardware Qualification – ISO 26262 vs. ECSS

ECSS Hardware Requirements

- **Failure Modes, Effects, and Criticality Analysis (FMEA/FMECA)**
  - Ensures **high-reliability hardware operation** in extreme space conditions.
  - Uses **MIL-STD-882** for safety risk assessment.
- **Radiation Hardness Assurance**
  - Automotive standards focus on neutron effects; **ECSS-Q-ST-60-15C** requires testing for:
    - **Total Ionizing Dose (TID)** (long-term radiation exposure).
    - **Single Event Effects (SEE)** (e.g., bit flips, latch-ups).
    - **Displacement Damage (DD)**.
- **Gap Analysis**
  - **Automotive hardware lacks space radiation testing** → Requires additional qualification.
  - **Automotive failure analysis aligns well with space requirements** but needs adaptation.
  - **COTS processors meeting ISO 26262 + AEC-Q100 are viable for ESA Class III missions** but need further assessment for higher classes.

Software Qualification – ISO 26262 vs. ECSS

ISO 26262 Software Safety Requirements

- **Software Development Process**
  - Defines software **architecture, unit design, and implementation**.
  - Enforces **modularity, redundancy, and defensive programming** to enhance reliability.
  - Requires **traceability of safety requirements from design to implementation**.
- **Software Verification and Testing**
  - Verification activities must include **structural coverage analysis** (e.g., branch coverage, statement coverage).
  - Uses **automated testing, simulation, and hardware-in-the-loop (HIL) validation**.
  - Demands **fault injection testing** to assess failure response and system recovery.
- **Software Tool Qualification**
  - Requires **verification of development tools** to ensure they do not introduce systematic errors.
  - Confidence levels are assigned based on tool impact and safety relevance.
- **Gap with ECSS**
  - ISO 26262 allows **flexible verification strategies**; ECSS requires stricter independent assessment.

Software Qualification – ISO 26262 vs. ECSS

ECSS Software Assurance Requirements

- **Software Verification and Validation**
  - ECSS requires **independent verification and validation (IV&V)** for all safety-critical software.
  - Object code coverage is **mandatory** to ensure no unintended behaviours exist.
  - Requires formal reviews at multiple stages, including **Critical Design Review (CDR)** and **Qualification Review (QR)**.
- **Traceability and Documentation**
  - ISO 26262 requires traceability but does not mandate specific formats.
  - ECSS-Q-ST-80 enforces **detailed documentation** for software lifecycle management.
- **Gap Analysis**
  - **Automotive software verification is less strict than ECSS** → Space systems need additional validation steps.
  - **Automotive safety software aligns well with ECSS, but lacks full traceability and independent testing**.
  - **Automotive-certified software can be used in space with additional qualification activities.**

Case Study – NVIDIA Xavier

- **Objective:** Assess whether an ISO 26262-certified automotive SoC (NVIDIA Xavier) can be adapted for space.
- **Key Features of Xavier:**
  - High-performance AI computing with automotive safety certification.
  - ASIL-D functional safety certification.
  - Built-in fault detection and error correction mechanisms.
- **Findings:**
  - Functional safety principles align well with ECSS.
  - **Radiation effects need additional testing.**
  - Software verification processes require extra steps for ECSS compliance.

Key Findings

- **Commonalities between ECSS and ISO 26262**
  - Both use structured safety processes and V-Model development.
  - Automotive hardware has **high reliability and safety** features.
- **Key Differences**
  - Space hardware requires **radiation hardness** and extreme stress testing.
  - Space software must undergo additional **independent verification** and code coverage analysis.
- **Conclusion: Automotive standards can serve as a foundation for space qualification with additional adaptations.**

Benefits of ASIL2ECSS Approach

- **Cost Reduction:** Avoid redundant testing by leveraging existing certifications.
- **Faster Qualification:** Pre-qualified automotive components accelerate space approval.
- **Wider Component Selection:** Access to cutting-edge COTS processors.
- **Increased Reliability:** Automotive safety standards enhance fault tolerance in space applications.

Challenges and Limitations

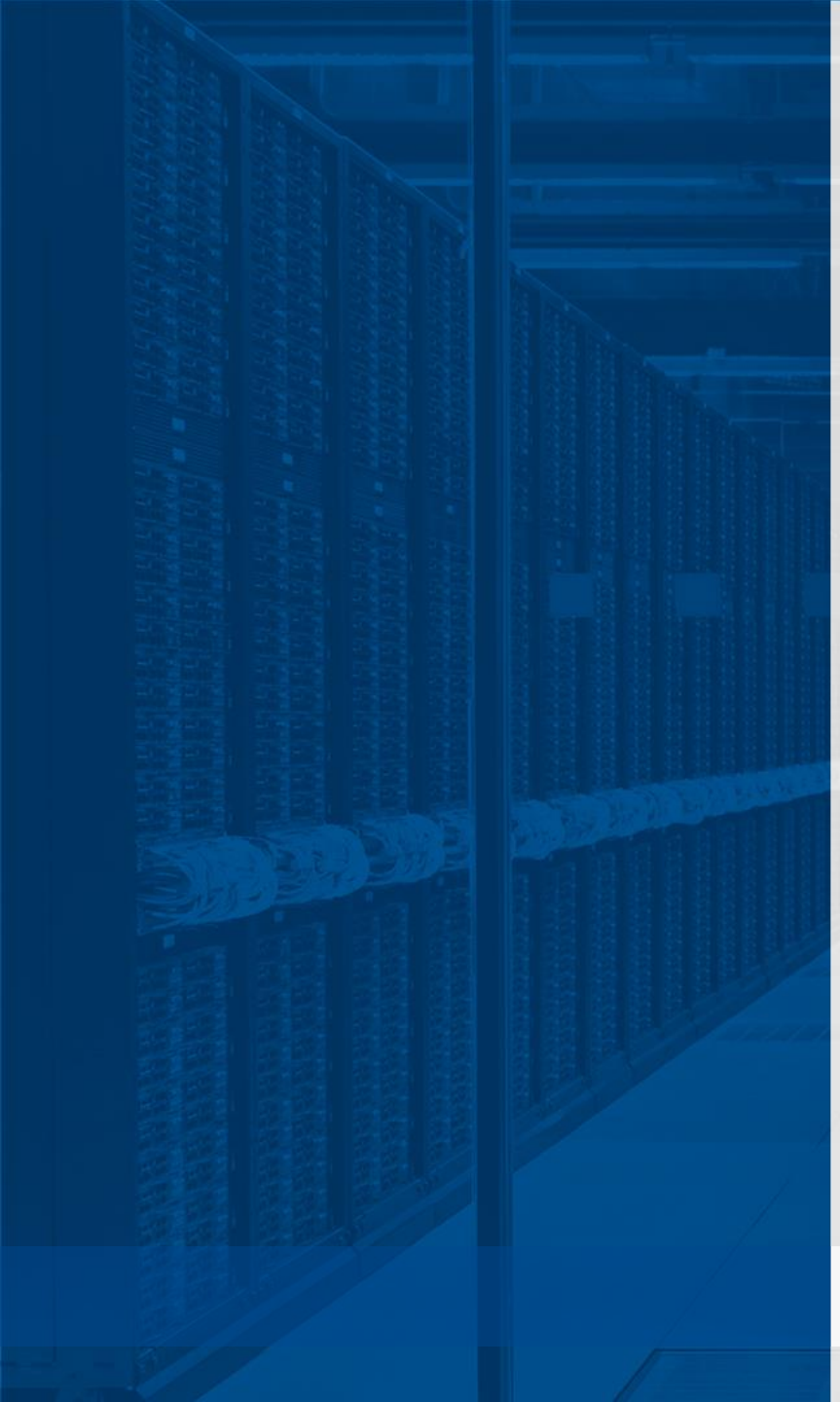
- **Radiation Testing:** Automotive components are not designed for space radiation exposure.
- **Certification Complexity:** ISO 26262 allows flexibility, while ECSS enforces rigid qualification standards.
- **Industry Acceptance:** Space agencies and stakeholders must validate the ASIL2ECSS methodology.

Future Work & Recommendations

- **Further case studies:** Test more automotive hardware and software platforms.
- **Refine codification process:** Improve methodologies for aligning ISO 26262 with ECSS.
- **Develop joint standards:** Foster collaboration between the space and automotive industries.
- **Automate certification mapping:** Use AI to streamline standard cross-referencing and gap analysis.

Conclusions

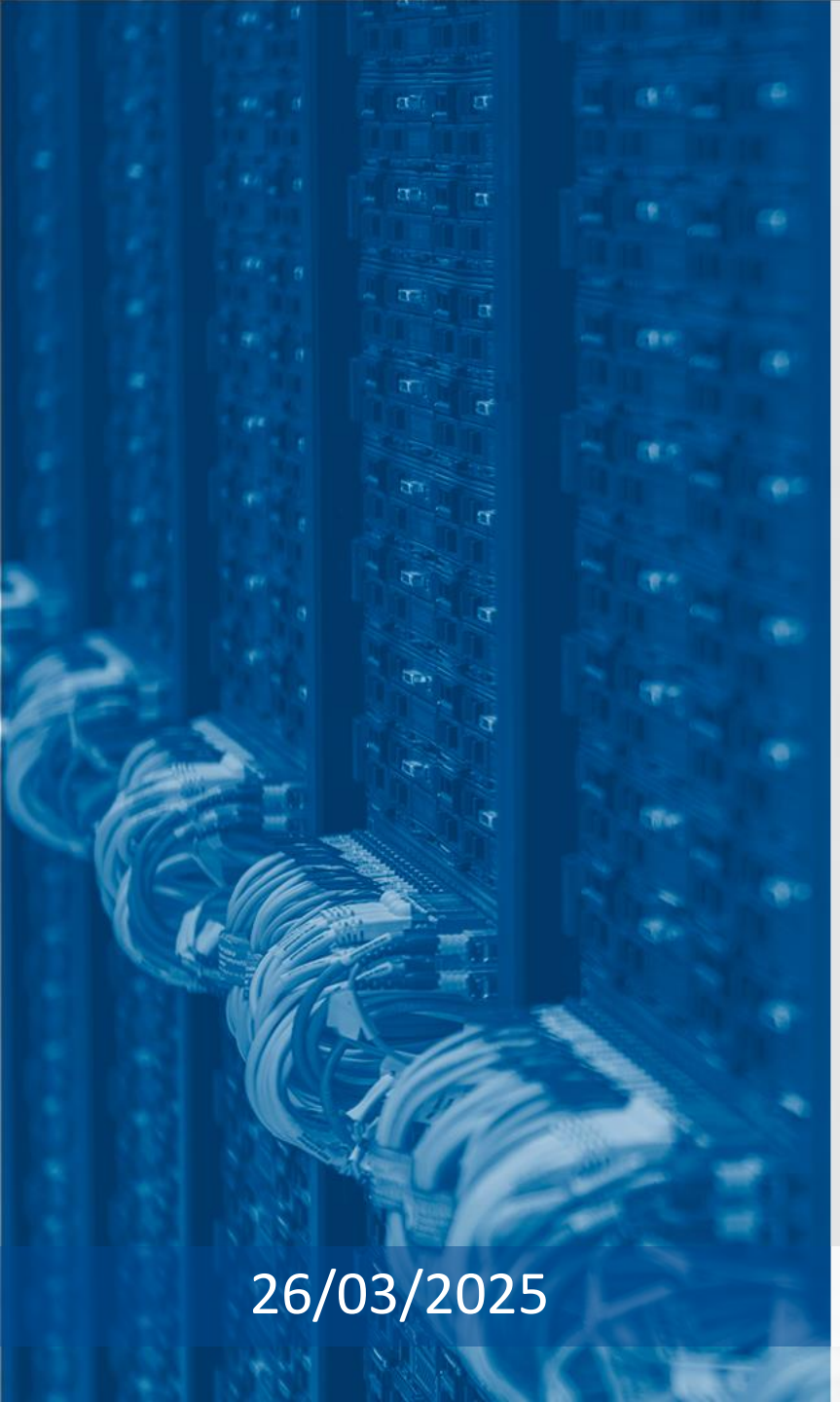
- **Key Takeaways:**
  - Automotive safety standards provide a strong **baseline** for space qualification.
  - Additional **radiation and verification steps** are necessary for ECSS compliance.
  - **ASIL2ECSS can significantly reduce space certification costs** if properly implemented.
- **Next Steps:** Engage with space and automotive stakeholders to implement recommendations.



Barcelona Supercomputing Center
Centro Nacional de Supercomputación

Thank You

Ivan.rodriguez@bsc.es



Reusing Automotive Certification and Qualification standards

Leonidas Kosmidis[1,2], Ivan Rodriguez-Ferrandez[1,2] David Steenari[3]

[1]Universitat Politécnica de Catalunya

[2]Barcelona Supercomputing Center

[3]European Space Agency

26/03/2025

ACCEDE 2025