

ASIL2ECSS Reusing Automotive Certification and Qualification Standards to Lower the Cost of Space Certification and Qualification for COTS Processors/SoC

ESA Contract No. 4000136128/21/NL/GLC/ov

Mapping of Automotive and Space Standards

Executive Summary Report

Document Information

Author	Leonidas Kosmidis (BSC)
Project Contributors	Matina Maria Trompouki (BSC), Sergi Alcaide (BSC), Iván Rodríguez (BSC), Alvaro Jover (BSC), Marc Sole (BSC), Jannis Wolf (BSC)
Distribution list:	David Steenari (ESA)
Classification:	Public
Release Date:	22/12/2023
Keywords	

The ASIL2ECSS ESA-funded activity aims to reduce the space qualification cost by reusing hardware and software developed for the automotive domain, which complies with the ISO 26262 functional safety standard. In order to do so, ASIL2ECSS created a mapping between the various ECSS standards and ISO 26262 and related automotive standards in a structured way.

First the basic concepts between the two standards were covered, specifically their overview, the development process, the criticality and availability. In addition, the hardware and software standards of the two domains were studied and a codification that allows automotive items to be qualified for use in space, by identifying the additional activities that need to be performed for various class missions of the new ESA mission classification was presented. Finally, the codification was applied to a small case study with the hardware and software stack of an automotive platform, the NVIDIA Xavier.

Our analysis indicated that both the space and automotive sectors have many common aspects, such as the V-development process and similar management for safety. However, we noticed that ISO 26262 is only focused on safety, while ECSS deals with much more aspects of the system. This meant that several additional automotive standards had to be covered.

In general, while ISO 26262 has several similarities with ECSS, it has also significant differences, especially at the hardware level. Primarily, ISO 26262 is concerned with functional safety and not with environmental, stress and radiation effects, which are covered by other standards like AEC-Q100. While some parts of this standard are very close to the ECSS ones (testing based on MIL-STD 882), die inspection, reproducible fabrication and lot tests, some of the testing methodology is more relaxed and focused on different types of radiation sources such as neutrons. Therefore, automotive qualified hardware needs to undergo new radiation tests relevant to space. Overall, a hardware part qualified both for ISO 26262 and AEC-Q100 is a good candidate for use in space up to ESA mission class III.

At the software level the two standards are closer, requiring only the repetition of verification activities with independence, as well as to obtain object code coverage for Category A software. Overall, despite the additional activities required, automotive qualified hardware and software provide a significant quality leap compared to regular COTS.