REVIEW AND RECOMMENDATIONS ON ISO 26262
Road vehicles – Functional safety

A position paper of the Automotive Parts Remanufacturers Association Europe.

The purpose of this paper is to:

1 Introduce the ISO 26262 standard.

2 Analyse the ISO 26262 from the remanufacturing perspective.

3 Give recommendations in regard of the ISO standard to remanufacturers.

Introduction

The ISO 26262 covers functional safety for electric and/or electronic (E/E) systems that are installed in series production road vehicles, excluding mopeds. Functional safety is a general approach to make car electronics safe and to provide guidelines to protect users from injuries caused by faults in electronics and electric systems. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes. The standard therefore addresses the complete system and its safety architecture, e.g. the redundancy of sensor signals.

Functional safety of automotive systems including E/E is and will be a very relevant topic for the years to come. Indeed, current automotive trends such as emission reduction, powertrain electrification, connected vehicles and Advanced Driver Assistance Systems (ADAS) increase the number and the complexity of E/E systems found in passenger cars. Also, software is now commonly used in safety-critical components of automobiles; such software needs to be safe, secured and reliable.

The starting point of the standard is the Hazard Analysis and Risk Assessment (HARA), which is carried for the subject of the development. From this analysis, the Safety goals are determined, and an Automotive Safety Integrity Level (ASIL) is associated. The standard defines the activities and requirements – ASIL dependent – that should be followed in the hardware and software development, production, operation, service and decommissioning.

The ISO 26262 divides the safety integrity levels from ASIL A to D, ASIL D being the highest requirement level. QM (quality measure) requirements that are not relevant for safety are not discussed in ISO 26262. In this case it is part of a process of quality maintenance, where ISO 9001 or ISO/TS 16949 can be used. For high ASIL levels, faults must be safely controlled by mechanical design, fault detection and be able to put the system into a safe mode so that the drive is not – or it is slightly – affected.

In order to identify the potential risks and requirements, the ISO 26262 also provide examples of methodology which can be applied, like the FMEA and PFMEA. They are well known approaches that aim at identifying all potential failures in a design, manufacturing or assembly process. Priorities are given according to how serious the failure consequences are, how frequently they occur, and how easily they can be detected. Their goal is to take actions to eliminate or reduce failures, starting with the highest-priority ones. Another tool is the Fault Tree Analysis (FTA), an analytical technique which is used to evaluate the probability of failure or reliability of complex systems. ISO 26262 also recommends the use of the Institute of Printed Circuit (IPC) standards, used worldwide in the electronics industry by OEMs, EMS and PCB manufacturers.

While compliance with ISO standards is usually voluntary, it can facilitate international business, be contractually required by customers or be considered as state of the art by a judge in case of an event. As other standards, it also creates a common language which can make communication between stakeholders more efficient as well as to facilitate contractual agreements.

Analysis

Looking at the ISO 26262 from a remanufacturing point of view, three main considerations stand out:

1 This standard is mainly addressed to car makers and components suppliers; it does not concern remanufacturers that maintain the exact same specifications as the original part. For them, it is anyway relevant to understand the methodology described to identify the safety critical aspect of a component and put measures into place to avoid any interference with functional safety mechanisms imbedded in the part during its design phase. It becomes relevant in case the remanufacturer is altering the design and architecture of the product.

2 Being the whole product lifecycle within the scope of the ISO 26262 – with a specific reference to service, maintenance and repair – components suppliers, which outsource remanufacturing activities and aim to be compliant to the standard, can require to the remanufacturer to follow their guidance to secure the mitigation of risk.

3 It is visible, once again, that standards, norms, policies etc. are often not adapted to the remanufacturing business, leaving unsolved challenges which could impact negatively the development of a futureproof circular economy within the European automotive industry. An example is the challenge faced by independent remanufacturers on the lack of access to part design change history, revisions information and safety related software updates. Without it, not up to date or obsolete parts could be mounted on vehicles and, in some specific cases, pose a safety concern. Even with proper information on revisions but no access to software fixes, the regeneration or salvage rate would not be acceptable as only the latest version of the part could be remanufactured. While some EU commission regulation including No 461/2010 and 330/2010 grant access to independent service providers, like independent repair garages, to OEM software required to update vehicles and components by paying « reasonable and proportionate fees » in a way that « is not discouraging access », remanufacturers seem to stand in a grey zone.

Recommendations

As a remanufacturer you are only undermining the safety architecture of a product if you alter it. Therefore, if you want to avoid compliance requirements, you should ensure and document that whatever reconditioning processes you are executing, this is not altering anything to the product architecture, design and specification. For example, if an SMD part is exchanged, the replacement needs to have the exactly same specification and assembly process as the original part. The Delta methodology, hence the benchmark between the OE new unit and the remanufactured one, should enable remanufacturers to verify that their processes do not alter the original safety architecture, design and specification of the part.

Differently, if the Delta methodology shows a discrepancy between the OE new unit and the remanufactured one, meaning that you have altered or modified the design and the product architecture during the reman process, then you are potentially impacting the complete system safety architecture and therefore it is recommended to comply to the ISO 26262, in order to avoid problems related to product liability.

Overall, no matter whether you alter the design or not, the ISO 26262 is a good refence to understand how to improve the remanufacturing process by following industry best practices like PFMEA, FMEA, IPC standard.

Finally, if you have a customer – like a Tier1 supplier – which comply with ISO 26262, he could ask for his own products to perform your process following specific procedures in order for him to be compliant; for this there isn't a fix set of requirements, it is rather recommended to ask what exactly has to be done, as it will depend on the product and its ASIL.

Contact

APRA Europe AISBL
Silversquare Central
coworking community
Kantersteen 47
1000 Brussels
BELGIUM

info@apraeurope.org