# Safety product development

Functional safety features form an integral part of every product development phase, and a new inverter designed for electric sports cars meets the ISO 26262 standard

Hofer Electric Drive Systems (Hofer EDS) has developed an inverter under the constraints of ISO 26262 to enter series production in an electric sports car. This development is a direct result of the cooperation between Semikron Automotive and Hofer EDS. The hardware consists of a proprietary Hofer control board and Semikron's SKAI2 platform, combining sophisticated functional safety with robust and compact inverter technology.

On the basis of this well-prepared hardware platform, and in combination with an established software development process, Hofer will achieve the ISO 26262 requirements for ASIL C.

The safety case for the Hofer inverter was based on a hazard analysis and risk assessment at vehicle level, conducted during the concept phase of the project. The outcome of this assessment indicated one central safety goal at component level (defined with ASIL C): prevention of unwanted actual torque. The main challenge with regard to safety during the development of the inverter was to prevent violation of this safety goal in any driving situation.

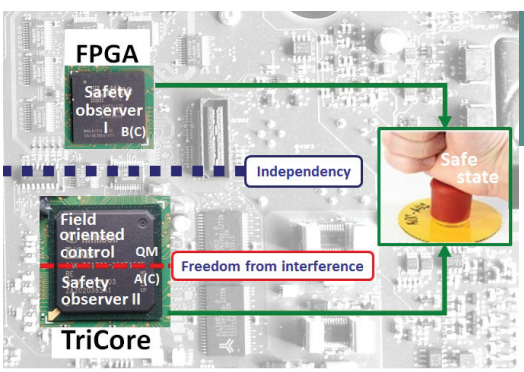
To achieve the target hardware metric values, decomposition was chosen to set up two redundant safety observers (torque and current monitoring) with ASIL A(C) and B(C).

The independency was proven through a detailed dependent failure analysis using fault tree analysis of the hardware and software functionalities. The freedom from interference has to be ensured by dedicated safety measures, such as memory protection, data flow and control flow monitoring within the TriCore processor.

There are five challenges relating to the safety management of the tailored Hofer inverter safety lifecycle. The first focuses on the partitioning and maintenance of proper interfaces within the product development, giving a clear understanding of the responsibilities of the development partners.

The second challenge centers upon the consistent requirements relating to engineering, which includes traceability from the technical safety requirements to the hardware, as well as the software safety requirements and even the corresponding test cases.

The third challenge is goal-oriented safety analysis via a failure modes effects and diagnostic analysis (FMEDA) to prove the effectiveness of the architecture to cope with random hardware failures as well as prevention of safety goal violations due to random hardware failures.




The architecture of the technical safety concept to prevent unwanted actual torque while driving


Hofer EDS's new inverter for electric sports cars combines advanced functional safety with a highly robust and compact exterior design

| | ASIL C | hLE300TF |
|---|---|---|
| Single-point fault metric | ≥ 97 % | 99,1 % |
| Latent-fault metric | ≥ 80 % | 89,4 % |
| Probalistic metric for random hardware failures | < 5 x $10^{-8}$ 1/h | 0,52 x $10^{-8}$ 1/h |

The results for the hardware metrics of Hofer EDS's inverter following FMEDA testing

The fourth challenge relates to the adequate inverter hardware qualification, such as functional testing during typical operation; test of protective functions during emergency conditions; insulation tests; mechanical tests (vibration, shock, drop); resistance to climatic changes; pollution burden; lifetime tests; electromagnetic compatibility.

The final challenge concerns effective testing throughout the various integration levels (hardware, software units, hardware/software integration and system), including fault injection tests to prove the implemented hardware and software safety mechanisms.

During the FMEDA analysis, Hofer's choice of safety mechanisms focused on the trade-off between aspired safety and excessive complexity. In addition to this, assuming an operating time of 187 hours a year, which is typical for electric sports cars, the FMEDA analysis resulted in the metrics for Hofer's inverter.

To evaluate the appropriate suitability of all functional safety activities, a functional safety assessment is performed by TÜV NORD, which included audits and confirmation reviews to verify the effectiveness of the technical safety concept and the implementation of the required processes. As such, Hofer is looking forward to transferring this experience into further safety-related products.

CONTACT

Marco Falco at Hofer
T. +49 931 359 335 400
E. marco.falco@hofer.de
W. www.hofer-em.de

ONLINE READER ENQUIRY NO. 514