

Certification of Embedded Software – Impact of ISO DIS 26262 in the Automotive Domain

Bernhard Schätz

fortiss gGmbH
Guerickestr. 25, 80805 München, Germany
schaetz@fortiss.org

Abstract. The publication of the ISO 26262 (“Road vehicles – Functional safety”) as Draft International Standard (DIS) and its expected release as international standard in 2011 has a substantial impact on the development of automotive software. By defining the current state of technique for the development of safe automotive software, the lack of or inadequate use of these techniques has severe legal consequences.

Like its ancestor, IEC 61508, as a process standard the ISO DIS 26262 defines artifacts and activities of the development process; consequently, Part 6 of the ISO standard (“Product development: Software Level”) defines the artifacts and activities for requirements specification, architectural design, unit implementation and testing, as well as system integration and verification. Depending on the hazard analysis and risk assessment, and on the resulting Automotive Safety Integrity Level (ASIL) of the function under development, the standard, e.g., prescribes the use of (semi)formal methods for the verification of requirements, (semi-)formal notations for software design, the use of control and data flow analysis techniques, static and semantic code analysis, the use of test case generation, or in-the-loop verification mechanisms. Furthermore, the standard specifically acknowledges the application of model-based development in automotive software engineering.

Currently, several of these rather advanced techniques are only required for higher safety integrity levels. Consequently, even though embedded software has become the leading innovation factor in automotive applications, many highly safety-critical automotive functionalities are only reluctantly implemented with software-based solutions. Here, by advancing the applicability and scalability of these advanced technologies and providing support in form of qualified tool chains, a substantial change in the development of automotive software can be achieved, allowing not only to virtualize and thus substitute physical solutions of automotive functions (e.g., X-by-wire solutions), but also to implement a new range of functionalities (e.g., autonomic driving).