
Abstract:

Safety-critical applications could benefit from the standardization, cost reduction and cross-domain suitability of current heterogeneous computing platforms. These are of particular interest for mixed-criticality product lines (MCPL), as both safety- and non-safety functions can be deployed on a single embedded device, provided that suitable isolation artefacts and development processes are used. Development of MCPLs can be facilitated by providing a reference architecture, model-based design and analysis tools and modular safety cases (MSC) to support the safety claims. In this paper, we present our method to ease the certification of MCPL based on MSC. Our approach consists of a semi-automated composition of layered argument fragments to trace the argumentation from the safety-requirements to the supporting evidences. The core is a database of arguments, described using the Goal Structuring Notation language (GSN) which is hosted in a database management system. This enables the concurrent development of the arguments and the compilation of evidences, as well as the automated composition of safety-cases for each product variant by a design optimization algorithm. We exemplify our approach with an industrial-grade case study, consisting of a safety wind turbine controller that is designed and deployed for an heterogeneous platform that undergoes an IEC 61508 safety certification.