Abstract:

Tools for creating safety cases currently on the market target safety experts, whose main concern is the management of safety cases. However, for safety assurance, safety experts should collaborate with technical experts, who have better understanding of technical and operational hazards.Thus, there should be a closer collaboration between the management of safety cases and technical expertise. Technical expertise may be retrieved, among others, from model-based system artifacts and processes. In order to close the gap between safety and technical expertise, we present ExplicitCase, an open-source tool for semi-automatic modeling, maintenance, and verification of safety cases integrated with system models. The advantage of this tool is two-fold. First, it enables its users to capture safety relevant information from model-based artifacts into safety cases. Second, it makes the safety cases rationale available to engineers in order to help them reason about design choices, while minding safety concerns. We evaluate the approach and the implemented tool based on the experiences obtained in a project use case.