Deriving Reusable Process-based Arguments from Process Models in the Context of Railway Safety Standards

Barbara Gallina, Mälardalen University, Västerås, Sweden
Luciana Provenzano, Bombardier Transportation, Västerås, Sweden

In the context of safety-critical railway systems engineering, various standards (e.g. EN 5012x) play a crucial role in prescribing process reference models at system (i.e., EN 50126 [1]) as well as at subsystem level (e.g., EN 50128 [2]). These models define sets of partially ordered tasks that have to be executed to develop safety-critical railway systems (e.g. entire vehicle, signaling components, etc). To these partially ordered tasks other core process elements are directly or indirectly associated namely roles, work-products, and guidelines. These core process elements allow process engineers to establish responsibilities by defining roles (who) for producing specified work products (what). Moreover, for the execution of the tasks well-defined principles and techniques are recommended.
Within EN 50129 [3], a safety case is defined as a structured justification document that includes the required evidence i.e., evidence of quality management, evidence of safety management (compliance with EN 50126-RAMS process), and evidence of functional and technical safety. Evidence of quality as well as safety management represents process-related evidence. Thus, the EN 50129-compliant safety case includes a justification concerning process compliance. The provision of such justification is time-consuming and costly.

To reduce time and cost, we apply MDSafeCer, which was explored [4] in the framework of the SafeCer [5] project and which is currently being implemented in WEFACT [6]. MDSafeCer is a model-driven certification method for the (semi) automatic generation of process-related deliverables. In this presentation, we consider a portion of a safety plan, we model it in SPEM2.0 [7], which is an OMG process modeling language, and then we show how (reusable) process-based fragments of a safety case can be derived from the safety plan model. More specifically, we derive process-based fragments in two different formats: in form of GSN-compliant goal structures [8] to explore best practices within the state of the art related to safety case presentation; in form of structured normal prose to address requirements within the state of practice related to safety case presentation.

Finally we provide our lessons learned, concluding remarks and perspectives for future work.

References

1. BS EN 50126-1:1999. Railway applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process, including corrigendum May 2010.
2. BS EN50128. Railway applications: Communications, signalling and processing systems, Software for railway control and protection systems - 2011.
3. BS EN 50129: Railway Applications – Communications, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling, 1999.
4. B. Gallina. A Model-driven Safety Certification Method for Process Compliance. 2nd IEEE International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), joint event of ISSRE, Naples, Italy, November 3-6, 2014.
5. ARTEMIS-JU- 269265 SafeCer - Safety Certification of Software-Intensive Systems with Reusable Components.
6. WEFACT: http://www.ait.ac.at/research-services/research-services-digital-safety-security/verification-and-validation/methods-and-tools/wefact-workflow-engine-for-analysis-certification-and-test/?L=1
7. OMG. Software & systems Process Engineering Meta-model (SPEM), v 2.0. Full Specification formal/08-04-01, Object Management Group, 2008.
8. GSN, “Community Standard Version 1,” 2011.