Standardization and Certification Considerations for Autonomous Train Control

Jan Peleska
Department of Mathematics and Computer Science
University of Bremen
Joint work with Kerstin Eder (University of Bristol), Anne. E. Haxthausen (Denmark Technical University), Wen-ling Huang (University of Bremen), and Thierry Lecomte (CLEARSY, France)

Abstract. We review software-based technologies already known to be or expected to become essential for autonomous train control systems with grade of automation GoA 4 (unattended train operation) in existing open railway environments. It is discussed which types of technology can be developed and certified already today based on existing railway standards. Other essential technologies, however, require modifications or extensions of existing standards, in order to provide a certification basis for introducing these technologies into non-experimental "real-world" rail operation. Regarding these, we check the novel pre-standard ANSI/UL 4600 with respect to suitability as a certification basis for safety-critical autonomous train control functions based on methods from artificial intelligence. As a thought experiment, we propose a novel autonomous train controller design and perform an evaluation according to ANSI/UL 4600. This results in the insight that autonomous freight trains and metro trains using this design could be evaluated and certified based on ANSI/UL 4600.

Just as in the field of autonomous road vehicles, the complete set of verification and validation (V&V) tasks to be performed in order to demonstrate functional system safety and operational safety is so large that V&V needs to be at least partially virtualized. In this context, we discuss the following questions and suggest (at least partial) solutions: (a) How can results about functional correctness on module level help to determine whether sufficient test coverage has been achieved on system level? (b) Which conditions should be fulfilled to obtain certification credit for virtualized (e.g., cloud-based) module and system tests? (c) How can we determine that the percentage of system-level tests with the real target system is sufficiently high? (d) What are the main challenges to be overcome to obtain trustworthy virtualized tests for operational safety?

The results presented in this talk have been elaborated in the context of BMWi (Federal Ministry of Economics and Technology) project *HiDyVe – Highly Dynamic Virtual and Hybrid Validation and Verification.* In the context of HiDyVe, new V&V approaches for highly complex, potentially autonomous cyber physical systems in the transportation domain are investigated.