Jan Peleska – University Bremen, Germany

Hand in Glove: Complete Bounded Model Checking and Testing of Interlocking Systems

Abstract:

In this presentation we focus on automated verification and validation of route-based interlocking systems. It is shown how the safety of interlocking tables and route control algorithms can be verified for given interlocking designs by performing bounded model checking in combination with k-induction. Having a design model at hand that is completely verified with respect to its safety properties, this model can also be used for model-based testing. We show how complete test suites can be applied in practice, if a novel equivalence class testing strategy is applied in combination with a compositional testing strategy. “Complete” testing strategies are capable of detecting any deviation from the reference model, provided that the implementation behaviour is reflected by a member of a given fault domain. We justify why these strategies are preferable over intuitive testing heuristics, because their strength is still superior to that of intuitive random approaches, even when applied against implementations outside the fault domain. The work presented here has been applied to “real-world” interlocking system designs that are part of the new Danish high-speed train network which is currently under construction.