Using Rigorous Simulation to Support Hazard Analysis and Risk Assessment (HARA) in the ISO 26262 Functional Safety Standard †

Adam Duracz, Halmstad University
Ferenc A. Bartha, Rice University
Ayman Aljarbouh, Centre de recherche INRIA-IRISA
Jawad Masood, Rice University
Roland Philippson, Halmstad University
Henrik Eriksson, SP Technical Research Institute of Sweden
Jan Duracz, Halmstad University
Fei Xu, Halmstad University
Yingfu Zeng, Rice University
Walid Taha, Halmstad University, Rice University
Christian Grante, Volvo Group Trucks Technology

With the increasing level of automation in road vehicles, the traditional workhorse of safety assessment, namely, physical testing, is no longer adequate as the sole means of ensuring safety. A standard safety assessment benchmark is to evaluate the behavior of a new design in the context of a risk-exposing test scenario and evaluate its behavior. Manual or computerized analysis of the behavior of such systems is challenging because of the presence of non-linear physical dynamics, computational components, and impacts. We study the utility of a new tool technology called rigorous simulation for addressing this problem. Rigorous simulation aims to combine some of the benefits of traditional simulation methods with those of traditional analytical methods such as symbolic algebra. We develop and analyse in detail a case study involving an Intersection Collision Avoidance (ICA) test scenario using the hazard analysis techniques prescribed in the ISO 26262 functional safety standard. We show that it is possible to both formally model and rigorously simulate the test scenario to produce informative results about severity of collisions. The work shows that the technology can handle models of non-trivial complexity and highlights the practical challenges encountered in using it.

CCS Concepts: • Mathematics of computing → Interval arithmetic; Solvers; Nonlinear equations;
• Computing methodologies → Model verification and validation; • Software and its engineering → Domain specific languages;

† This manuscript consolidates and extends several results presented at FISITA 2014 [Masood et al. 2014] and ICESS 2015 [Duracz et al. 2015]. The first version investigated the feasibility of using rigorous simulators in this domain, using a simple one-dimensional model expressed as a single hybrid automaton. The second paper reported on a simulator capable of executing two-dimensional scenarios with collision and sensor models based on rectangular vehicles and a braking controller based on time-to-collision. The present version adds: a significantly improved model including a combination of multiple braking criteria based on recommendations from the automotive industry, a more precise model of the sensor range (trapezoid), and support for simulating scenarios in different terrain. A new section has been added (Section 3), where the braking criteria used in the model are documented. Section 4 has been extended to explain the improved model in detail.

This work was supported by US National Science Foundation award CPS-1136099, the Swedish Knowledge Foundation (KK), The Center for Research on Embedded Systems (CERES), VINNOVA (Dnr. 2011-01819), the Collège Doctoral International de l’Université européenne de Bretagne, and the Conseil Régional de Bretagne.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© YYYY ACM. 1539-9087/ YYYY/01-ARTA $15.00
DOI: http://dx.doi.org/10.1145/0000000.0000000