Lightweight Contracts for Safety-Critical Automotive Systems

Bernhard Kaiser[1] Stefan Sonski[2] Suryo Buono[3] Hauke Petersen[4] Justyna Zander[5]

Abstract: Complex automotive systems are composed of subsystems and components in a deep hierarchy, often designed by different development partners or reused from preexisting projects. It is therefore a challenging task to break down requirements into sub-requirements fitting the scope of the subsystems and to simultaneously demonstrate that the integrated system fulfills both functional and safety requirements specified on the top-level. Contract-based development is a popular approach for breaking down requirements onto components by means of assumptions and guarantees. However, most current approaches are based on a formal semantics and therefore limited in their expressive power and their acceptance by practitioners from automotive industries. We propose a semi-formal approach that allows specifying assumptions and guarantees at component interfaces in a language with well-defined syntax, but leaving the verification of fulfillment of the contract by a component to expert decision. However, some of the relevant refinement relations can be formalized and automatically checked. We describe our prototypical Eclipse tool that allows the annotation of components with assumptions and guarantees, and the partial checking of the decomposition. We show the applicability by a case study of an automotive electric drive system.

Keywords: contracts, safety, functional safety, requirements engineering, assumption, guarantee

[1] Berner & Mattner Systemtechnik GmbH, Gutenbergstr. 15, Berlin, bernhard.kaiser@berner-mattner.com
[2] Alpha EOS, Stuttgart, s.sonski@gmail.com
[3] Berner & Mattner Systemtechnik GmbH, Gutenbergstr. 15, Berlin, suryo.buono@berner-mattner.com
[4] Freie Universität Berlin, Computer Science Institute, Takustr. 9, 14195 Berlin, hauke.petersen@fu-berlin.de
[5] Berner & Mattner Systemtechnik GmbH, Gutenbergstr. 15, Berlin, justyna.zander@berner-mattner.com