Software Bugs Seen from an Industrial Perspective or Can Formal Methods Help on Automotive Software Development? (Invited Talk)

Thomas Kropf

Robert Bosch GmbH

Developing software for automotive applications is a challenging task. To stay competitive conflicting goals must be met: complex and innovative algorithms with many versions for different car line variants have to be implemented within the tight resource boundaries of embedded systems; high reliability especially for safety critical applications like airbag or braking applications has to be ensured under immense cost pressure. Despite these demanding constraints in recent years automotive software development has made significant progress in terms of productivity and quality. All this has been achieved without direct usage of formal methods.

However, software is still a good part away from being bug-free. If looking closer it becomes apparent that often unclear specifications or an incomplete understanding of the application domain is the root cause of erroneous software. In such cases any validation approach for a given piece of software would not succeed. Still there are many cases where the software implementation indeed violates a given specification.

Consequently, the second part of the talk gives a set of application areas where current development and validation techniques still lead to unsatisfactory results, i.e., where software bugs are still hard to detect. In these cases, formal methods may help to improve the current situation. Some examples are given where and how those approaches are already used or where an introduction into real-life design flows is imminent. The talk ends with some challenging problems where basic research is still needed.

W. Damm and H. Hermanns (Eds.): CAV 2007, LNCS 4590, p. 3, 2007.