Autobest – Software Hypervisor for Embedded Systems

André Himmighofen

Software Developement
easycore GmbH
Daimlerstraße 11
91058 Erlangen
andre.himmighofen@easycore.com

Many embedded systems are used to compute safety or security relevant tasks. Focused on the automotive market there are Electronic Control Units (ECUs) which control safety critical devices like the brakes or the airbags and security relevant ECUs which must be hardened against malicious attacks, because they can be increasingly accessed from external systems.

The usual way to ensure a security or safety level is to develop software either in accordance with Common Criteria (CC) for security [CC12] or ISO 26262 Automotive Safety Integrity Level (ASIL) for safety related functionality [ISO11]. It is obvious that these standards multiply the effort during the software development. One solution to reduce the cost is to split functionality in critical and non-critical parts and only certify the critical parts. This approach works well as long as there is a dedicated ECU which only has to control one function (the brakes for example). However, to reduce the energy consumption and cut the costs of the increasing number of ECUs in a modern car the OEMs try to consolidate their onboard networks. As a r esult there are ECUs which have a high number of different functions to control of which only a fraction has a security or safety critical aspect. On such an ECU it would be necessary to ensure that not only the critical parts of the software work correctly, but also the non-critical parts have no influence on the critical parts as well. According to the logic above the whole system has to be developed with the same processes and certified afterwards.

A solution to reduce the cost would be to separate critical and non-critical partitions which are then isolated from each other using a certified hypervisor and hardware support to enforce restrictive policies. The Autobest research project, a cooperation of the easycore GmbH in Erlangen and the Hochschule RheinMain in Wiesbaden, aims to develop such a hypervisor which provides the instruments to guarantee that a safety critical partition is not influenced by potential defective partitions and a security critical partition can be hardened against attacks of a compromised partition. As an additional benefit the Autobest hypervisor will help to consolidate legacy ECUs by allowing to port complete ECU software stacks into a hypervisor partition with minimal efforts.

References

[CC12] Common Criteria: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1.4, September 2012.

[ISO11] ISO: ISO 26262, 2011.