Functional Safety Methodologies: Using Model Coverage Analysis as a tool for requirement optimization in a model based software development environment of an automotive E/E subsystem

Abdullah Khan, Maruti Suzuki India Limited, Abdullah.Khan@maruti.co.in

Abstract

Automotive systems have always been safety-critical but due to increasing complexity in electronics involved, Safety is now fundamental requirement in the automotive systems. In order to address these requirements, ISO26262 was introduced in 2007. It is derived from the original standard IEC-61508 and made exclusively for automotive applications.

In order to make system safer, ISO26262 focuses on many verification and validation methodologies. Model/Code coverage is one important criterion through which completeness of test cases is judged. If required, then more test cases are adapted to test the parts that are not covered. ISO26262 also highly recommends good coverage especially for high risk applications.

In this presentation, Model coverage is used as a mathematical tool to analyze the control requirement and find out the redundancies and undesired conditions further simplifying the system under development. This simplification will not only lead to better coverage but also provide less complex model and software, free from any type of dead logic, decreasing the risk factor and hence achieving the goal of better functional safety.

Key Words: Functional Safety, ISO26262-6, Unit testing, Model/Code Coverage, Requirement engineering