SW SAFETY ANALYSIS - APPROACH BY ANALYSIS OF SAFETY REQUIREMENTS IN COMPLIANCE TO ISO26262 (2nd EDITION)

Presenter Name: Shashank Muktheser
Company Name: Robert Bosch Engineering and Business solution.
Email: Shashank.Muktheser@in.bosch.com

Ability of SW to be explicitly programmed for user specific task has always motivated engineers to apply them in wide range of sectors ranging from IT, medical sciences to automotive sector. Usage of SW in Automotive finds its applications in safety and non-safety critical systems. Development of SW in safety critical systems needs to undergo stringent V-Cycle from requirements elicitation, design, implementation, testing and validation. Despite such a stringent process, there exists no proper method which will help to perform an analysis at SW architectural level or SW safety requirements level that could bring value additions to safety concept.

Performing SW safety analysis (SSA) as per ISO26262 (2nd edition), helps to identify safety critical failures, possible design weakness, conditions that could potentially affect SW safety requirements. Analyzing such safety critical failures help understand and mitigate undesirable impact and insufficiency in safety concept on SW, system and at vehicle level. This SW safety analysis and approach is additional safety analysis technique to System FMEA where failures of SW is identified and measures are defined to mitigate SW failures. Having such qualitative analysis approach could be first step to defining quantified SW Safety analysis at SW architectural level.

This paper elaborates an approach of performing SW safety analysis. Proposed approach is defined in compliance to ISO26262 (2nd edition) to cover few key points like how to define SW failure modes, identify safety critical failures for given SW safety requirements, analyze negative effect of failure modes on SW, system and vehicle, identify possibilities to mitigate such failures, check the effectiveness of SW safety requirements and mechanisms, value addition to safety concept.

Further few examples of SW safety requirements are taken to elaborate how defined approach can be used practically used to analyze and identify failure modes, identify critical failures, its negative impact on SW, system and vehicle level, and mitigate such failure with safety and test measures.

Keywords: Software safety analysis, ISO26262, Failure modes, identified safety critical failures, Safety mechanisms, safety test measures, critical failures, software component, safety concept.