Achieving ISO 26262 ASIL Metrics Using Modern Static and Dynamic Failure Mode Fault Analysis.

Automotive Functional Safety Analysis under the ISO 26262 standard has evolved over the last few years, as the challenges have become better understood and respective solutions refined. Early approaches to demonstrate that devices meet specific Automotive Safety Integrity Level (ASIL) requirements have given way to more effective techniques and technologies. In this workshop we present new solutions that accelerate and increase the accuracy of this development phase.

To achieve an appropriate ASIL rating, an automotive semiconductor chip has to meet specific requirements prescribed in the standard. The Single Point Fault Metric (SPFM), Latent Point Failure Metric (LPFM) and the Failure in Time (FiT) metric are all critical measures that must be satisfied to a certain proportion. Different failure modes and safety mechanisms, analyzing varied permanent and transient fault types, and overall product requirements and time-to-market all factor into this analysis process.

Identifying the faults in a design that can lead to a failure of a block or system requires a process of injecting faults during simulation and analyzing these injected faults with respect to a failure or detection strobe. Today, a multi-pronged approach involving both static and dynamic analysis is required to achieve the necessary analysis performance and quality, given the size and complexity of modern automotive ASICs.

System Architects and Chip Designers work together to reduce the number faults that can cause failures without safety mechanisms in place, or build in safety mechanisms using a cohesive strategy to detect and mitigate the failure. Single Point Faults (SPFs) represent the set of faults that violate the safety goal and are not handled by appropriate safety mechanisms. Where there are safety mechanisms in place for the majority of faults, it may not be effective for some of them, termed Residual faults. Multi-point faults, where an individual fault does not violate a safety goal but multiple faults occurring together do, also need analysis. These faults are subcategorized detectable, perceivable or latent.

Along with the fault metrics it is very important to examine the Failure in Time (FiT) rate of the whole device. Soft Error analysis is also important to determine the safety of the device in the presence of faults that are transient or momentary in nature.

In this workshop we introduce the various concepts of ISO 26262, commencing with ASIL level determination right through to overall FiT rate calculation. We present a modernized methodology to establish the metrics starting from safety setup definition involving failure and detect strobes, static analysis to quickly understand the single point and residual faults followed by advanced fault analysis to precisely categorize the faults that are residual, detected and safe. We present a Soft Error analysis approach and FiT rate calculation, based on selective flip flop hardening to reduce device power overhead.