

Handling Freedom from Interference in Mixed Criticality Systems

Presenter: Abhay Khonje¹, Navelkar Varad Krishna²

¹ Robert Bosch Engineering & Business Solutions PVT LTD, Email ID: abhayanna.khonje@in.bosch.com

² Robert Bosch Engineering & Business Solutions PVT LTD, Email ID: navelkar.varadkrishna@bosch.com

Current trends in automotive such as connectivity, autonomous, electrification and shared mobility are triggering an exponential growth in complexities of associated system. This increasing complexities is resulting in a demand for systems capable of managing wide range of critical functionalities and adherence to safety related issues. The quest to explore and define solutions for addressing this growing demand of functionality and safety has resulted in exploring different option. **System on Chip (SoCs)** is one such complex solution which is currently being widely adapted to provide a combination of safety and better driving experience.

A SoC, consists of combinations of microprocessors, microcontrollers, GPUs, FPGA etc. that can support simultaneous processing of applications such as connectivity, large data transfers, image recognition, sensor fusion and lane planning.

SoC is one of the preferred resolutions to address growing demands in terms of requirements and associated system complexities. Addressing future demands in autonomous driving and implementation of feature rich safety-critical system not only is very crucial, but also poses significant challenges from verification point of view. Particularly, in a mixed-criticality system consisting of implementations with different ASIL's, wherein applications with low criticality must be prevented from interfering with high criticality applications.

Ensuring a Freedom from Interference in SoC based mixed criticality system itself can be highly demanding due to multiple complexity and interactions involved within the SoC and also with other related devices. Hence freedom from interference is an important characteristic that needs to be addressed for mixed criticality system.

In this paper, we introduce concepts/methodologies for SoC based systems that provides strong isolation guarantee to applications involving mixed criticalities. These have been evaluated for critical application using mix of conventional & SoC based processing devices, where there are strong dependencies among processors, controllers, GPU, FPGA and applications hosted on multiple operating systems (E.g. RTOS, QNX/LINUX, AUTOSAR etc.)

Freedom from Interference can be achieved by using different methods such as complete physical isolation, virtual method and by use of partitioned software and hardware based solution.

In this paper we present partitioning based isolation concepts with strong support from MPU and MMU as a solution. Implementation is support by spatial and temporal partitioning for both software and hardware architectures hosted on MCU and MPU and also inter/intra core communication.

Keywords: ISO 26262, System on Chip (SoC), Mixed Criticality, Freedom from Interference, Spatial Isolation, Temporal Isolation