Virtualization in Mixed-Criticality Systems

(Varun Sethi, Freescale Semiconductor & Michael Paulitsch, EADS)

Mixed criticality system, i.e. systems where applications of different security or safety-criticality share the same hardware, are becoming increasingly popular. There is also a growing trend towards adopting multicore technology for such systems. Virtualization aids in the adoption of multicore technology for multi-criticality systems by allowing multiple different systems operate on the same hardware platform. However, this leads to challenges related to security and reliability. Also, system requirements may vary across various different virtualized implementations. "System Responsiveness" is one key requirement that must be met while designing mixed-criticality systems for a multicore – virtualized environment. The systems must be able to respond to a stimulus in time predictable and deterministic manner.

A typical mixed-criticality system can be represented as a combination of an RTOS and a general purpose operating system in a virtualized environment. Each of these OS instances caters to different set of tasks, for example the general purpose OS may cater to human directed tasks whereas the RTOS may cater to machine directed task. Now, it's imperative that each of these operating systems do not interfere with each other's operation, especially the real time activities should go on unhindered and completion in time needs to be guaranteed. This is possible if the virtualization layer can ensure adequate isolation between two or more OS instances. Isolation requirements are extremely critical when it comes to shared resources (like system bus, platform cache, memory, I/O etc) access. The virtualization layer should be able to achieve adequate system isolation, with a minimal performance overhead.

In this session we discuss various requirements for designing a reliable and a secure virtualization solution for mission-critical systems. We also welcome solutions addressing these requirements. We would primarily focus on the following questions but are open for other related discussion points:

1. Isolation requirements for mixed-criticality systems in a virtualized environment? What role can hardware assists play in meeting these requirements?
2. Would proactive system monitoring help in ensuring system security? Can this be done non-intrusively, possibly using some hardware assists?
3. What are the set of "must required" hardware assists for meeting the isolation requirement?
4. What are current solutions to virtualization for mixed criticality? How will future solutions likely look?