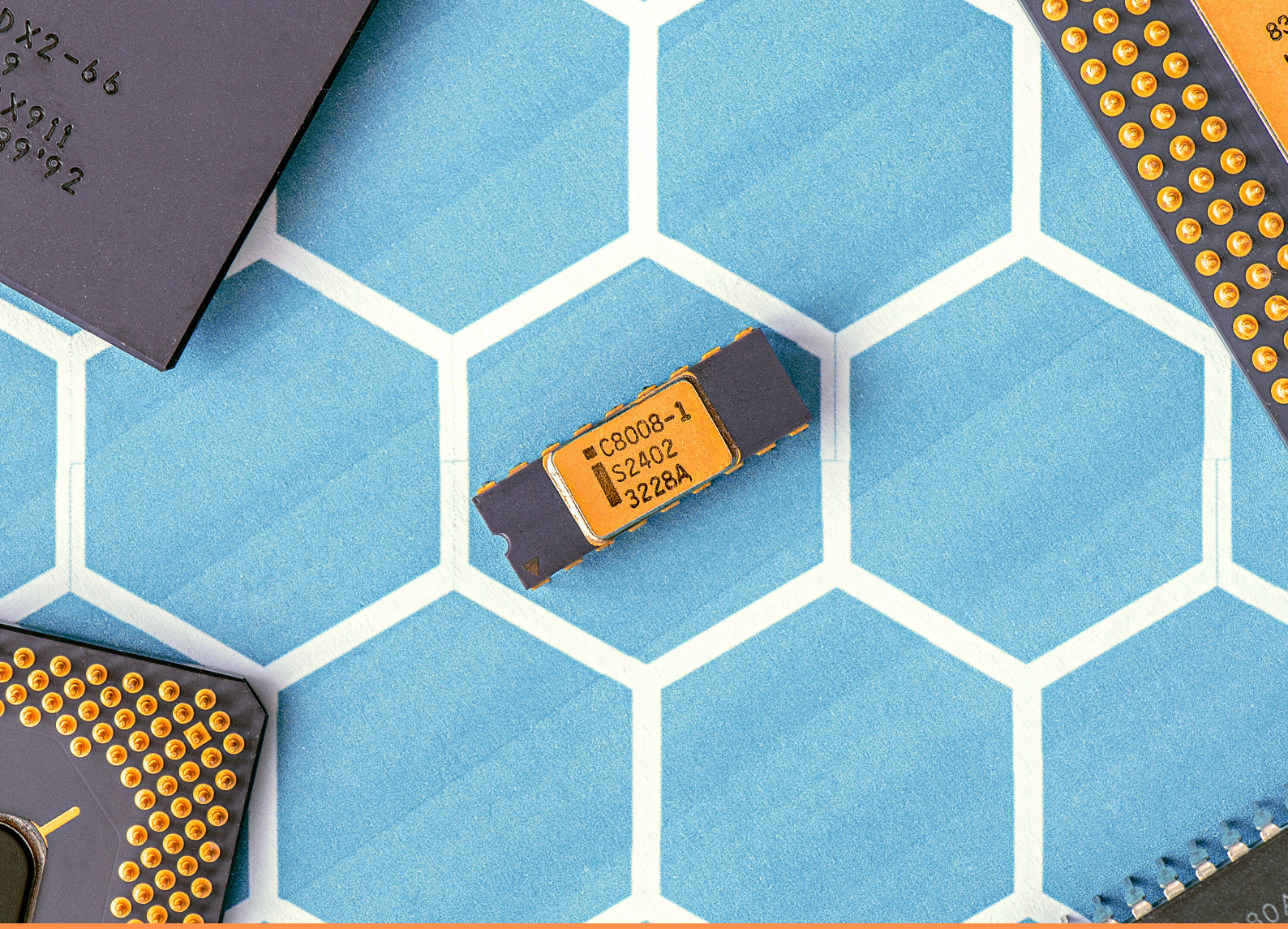


# ISO 26262 FOR SEMICONDUCTORS:

## *SYSTEM LEVEL RADIATION TESTING FOR SAFETY CRITICAL PLATFORMS*

Interview with:

**Jyotika Athavale**

*Intel Corporation, USA*

# Jyotika Athavale

Principal Engineer Senior Functional Safety and RAS Architect.
Intel Corporation, USA

*In the lead-up to IQPC's ISO 26262 for Semiconductors USA Conference 2020, Jyotika Athavale explains System Level Radiation Testing. As she explains, System Radiation Testing helps to accurately model transient reliability for safety critical platforms compared to the traditional methodology of bottom-up individual component characterization. It also saves cost and certification time.*

**Please give us an overview of what System Level Radiation Testing for Safety Critical Platforms is.**

Radiation can degrade and/or destroy information and devices. The malfunction of safety critical platforms can lead to catastrophic injury or death as well as expensive damages.  Hence, ensuring safe operation of these systems is an important concern. With growing complexity and processing power, ensuring safe and accurate operation of these systems can become more challenging. In the case of radiation induced soft errors,  particle radiation can be the cause of transient faults.

Such soft errors have the potential of resulting in system errors, malfunction and failure thereby introducing unacceptable safety risks or causing expensive damage. In order to mitigate risk, the focus is on reducing these errors and improved data integrity.

System radiation testing helps to accurately model transient reliability for safety critical platforms compared to the traditional methodology of bottom-up individual component characterization.

**For the automotive/semiconductor industry, what are the specific advantages of system level radiation testing?**

System-level radiation testing guidance for space, avionics and automotive applications is an important area of focus with increasing performance demands driving larger quantities of commercial off the shelf (COTS) technologies into equipment..

The goal is to accurately model or validate soft error performance and drive recommendations for mitigation in addition to validating existing mitigations, while focusing on key SEE mechanisms including SEU, MBU, SEL, SEFI, SET, SEB and SEGR.

This is needed to meet the stringent system safety requirements (FuSa metrics per target ASIL / SIL / DAL) per the functional safety standards. System-level testing can help save cost and certification time and also enables the evaluation of complex functions that would not be available at the component level.

## How can the impact of cyber-attacks be mitigated in safety critical platforms, specifically those in the car?

With systems now increasingly complex, interconnected, and software-driven, security concerns are continuing to grow. Datalink and networking capabilities are bringing additional data to safety critical platforms, and this can cause serious security issues to occur. To address cybersecurity, isolation must hinder the ability of one partition to infer information about the other. MCPs are highly-complex SOCs (System On Chip) that provide many resources, including processing cores, memory devices, interconnects, and others.

Users can tailor the resources to the requirements of their equipment by selecting specific aspects, such as which cores are activated, their execution frequencies, whether shared memory are used and how they are allocated, etc.

However if these configuration settings of the MCP, are inadvertently altered during operation, they could cause the MCP to no longer comply with their requirements. Systems must enforce critical functional separation / robust partitioning so that the behavior of functions or applications within a partition cannot undesirably affect the behavior of functions or applications in another partition. Intel provides updates to its software and firmware as needed to address vulnerabilities.

In addition, Intel hardware and system support software provides technologies for security as well as protection and separation mechanisms.

## How can companies implement functional safety in cost-efficient manner?

Scalable architectures and customers' demands for high-compute and high-safety automotive solutions are challenging requirements to be fulfilled altogether. ISO 26262 ASIL decomposition is an advanced technique that can be leveraged to solve the problem in a cost effective way. ASIL decomposition is a method of ASIL tailoring during the concept and development phases.

During the safety requirements allocation process, benefit can be obtained from architectural decisions including the existence of sufficiently independent architectural elements. This offers the opportunity to implement safety requirements redundantly by these independent architectural elements, to assign a potentially lower ASIL to (some of) these decomposed safety requirements.

ASIL decomposition is an ASIL tailoring measure that can be applied to the functional, technical, hardware or software safety requirements of the item or element. Although a single or dual FuSa certified HW running certified SW on a certified OS (MCU era) is preferred, this approach is too expensive for new complex systems.

A FuSa approach enabling high performance multicore QM COTS running open source SW, non deterministic algorithms is a more desirable option. This architecture allows to significantly reduce the safety requirements on the complex part while keeping higher safety claims on the monitor.

*Interview conducted by Cristian Bustos*
*Cristian.Bustos@iqpc.de*

## Also, David Ward, Senior Technical Manager, Functional Safety of HORIBA MIRA will present at IQPC's ISO 26262 for Semiconductors Conference USA, among other topics:

### OVERVIEW OF DRAFT STANDARD ISO/SAE DIS 21434 – ROAD VEHICLES – CYBERSECURITY ENGINEERING

- Why do we need a standard for vehicle cybersecurity?
- The wider political and regulatory landscape
- Towards dynamic risk management in cybersecurity
- Processes for analysis, assessment and management of cybersecurity risk
- Processes and activities relative to cybersecurity engineering during concept phase
- Risks and opportunities in its adoption
- Balancing automotive and IoT approaches
- Identifying and resolving conflicts between safety and security goals

Guidance of

# ISO 26262

## TO SEMICONDUCTORS

*15 - 18 June 2020 | Detroit, MI*

*"I am excited to have all the experts on semiconductor FuSa joining this conference with me as it will be a unique opportunity to spread out knowledge and having exclusive insights on that very hot and important topic. Starting from the work done in ISO/PAS 19451-1, the 2nd edition of ISO 26262 is adding an important focus to semiconductors with a dedicated part (ISO 26262-11) on 'Guideline on application of ISO 26262 to semiconductors."*

*Riccardo Mariani, VP Industry Safety, NVIDIA*

**DOWNLOAD AGENDA**