

## ● 발표 주제

# 기능안전 지원을 위해 AUTOSAR 플랫폼에서 제공되는 안전메커니즘 소개

Introduction of Safety Mechanism supported by AUTOSAR to satisfy Functional Safety



## 장재호

Jae-Ho Chang

현대오토론

상무/차량융합제어실

JaeHo.Chang@hyundai-autron.com

## Professional Career

Ph.D. : KAIST, 1998

- 2012~(현)     현대오토론, 차량융합제어실
- 2005~2012    현대카네스
- 2004~2005    현대모비스
- 2000~2004    네스테크
- 1998~2000    현대전자, 전장사업본부

## ● 발표초록

In this presentation, safety mechanism supported by AUTOSAR to satisfy functional safety is introduced.

ISO26262 overview, ASIL level, FFI(Freedom From Interference), AUTOSAR are briefly explained.

Also the relationship between ISO26262 and AUTOSAR is roughly explained. ISO26262 is a system-level requirement and AUTOSAR is only a platform which performs a part of whole. AUTOSAR Safety Mechanism for functional safety will follow procedure of SeooC(Safety Element out of Context).

SEooC approach is described in ISO 26262 part 10. AUTOSAR safety mechanisms are designed and released based on SEooC.

AUTOSAR provides at least 4 safety mechanism in order for the system to guarantee FFI and satisfy functional safety.

- 1) Safety OS : Time & Memory protection → Detect Time & Memory Interference
- 2) Safety RTE : Provide safe API between ASW & BSW → Detect Data Exchange Interference
- 3) Safety WDG : SW processing sequence monitoring → Detect Time & Execution Interference
- 4) Safety E2E (CRC) : Detection of data corruption → Detection of Data exchange Interference

It doesn't satisfy ISO26262 even though AUTOSAR platform is applied to the system. In other words, The AUTOSAR alone does not satisfy ISO26262. However, AUTOSAR provides good support for the development of safety-related system