강연 3 10:20 ~ 10:40

● 발표 주제

현대자동차 SOTIF 대응 체계 및 개발 방향

HMC's Body of SOTIF Implementation & Development Strategy

정지열
Gi Yeol Jeong

현대자동차
제어프로세스개발팀/책임연구원
2567726@hyundai.com

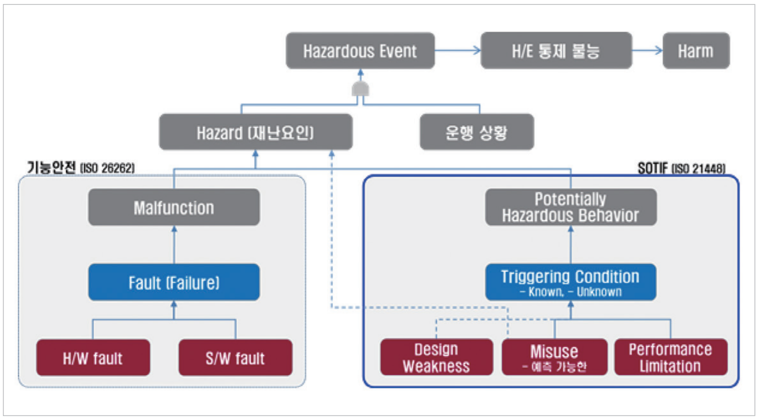
Professional Career

- 현) 제어프로세스 개발
- 新전기구동시스템 개발 (E-4WD, 인휠)
- 자율주행차량 개발
- 샤시통합제어시스템 개발 (VSM)
- 샤시제어시스템 개발 (ESC外)
- 샤시설계 (제동)

● 발표초록

• 개요 : 자율주행 기능의 안전을 중심으로 SOTIF 국제 표준이 갖는 의미와 현황을 설명하고, 현대자동차의 대응 체계 및 개발 방향을 공유

• 키워드 : Triggering Condition, Performance Limitation, System weakness, Misuse, Unknown Hazardous, HAZOP, STPA, Design Improvement, Verification & Validation

기능안전은 전기/전자 장비의 하드웨어 및 소프트웨어의 결함(fault)으로 유발되는 재난요인(hazard)을 방지하기 위한 것으로 완전 무결(integrity)하더라도 본질적인 제어시스템이 의도하고 있는 기능 또는 성능의 부족(shortcoming) 등으로 인해 동일한 재난요인이 발생할 수도 있다. 이러한 문제들을 방지하고자 제안되는 개발 방안을 SOTIF (Safety Of The Intended Functionality)라고 칭한다. 국제표준기구 ISO에서도 SOTIF 관련 국제표준(ISO IS 21448)을 개발 중에 있으며 이는 전기/전자 시스템에 의도된 기능들이 안전하게 작동할 수 있도록 개발 프로세스 및 방법론을 정의하고 있다.

본 발표는 SOTIF 국제표준 개발절차 상에서 완성차 업체가 필수로 수행해야 하는 SOTIF 안전 컨셉 개발 활동과 관련하여 효과적인 안전 요구사양 개발 방법론에 대한 내용과 현황을 설명하고자 한다. 더 나아가 현대자동차가 추구하는 개발 방향 및 연구 사례 등을 소개하여 2022년 3월 발효 예정인 본 표준의 안정적인 개발 문화 정착에 기여할 수 있도록 관련 분야 개발 참여자에 가이드 하고자 한다.