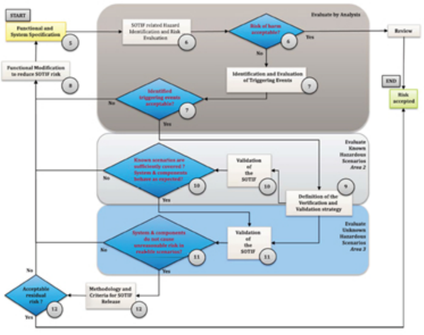
SOTIF (Safety Of The Intended Functionality)

SOTIF 소개 및 주요 내용

SOTIF (Safety Of The Intended Functionality)는 자율주행 차량의 의도한 기능(Intended functionality)의 불충분(Insufficiencies) 또는 사람의 Misuse로 인해 발생된 Hazard를 최소화 하기 위해 제정된 안전 규격으로 2019년 1월에 "ISO/PAS 21448:2019 Road vehicles- Safety of the intended functionality" 이름으로 공식 릴리즈가 되었습니다.

SOTIF 주요 활동

5. Functional and system specification
6. Identification and Evaluation of hazards caused by the intended functionality
7. Identification and Evaluation of triggering events
8. Functional modifications to reduce SOTIF related risks
9. Definition of the verification and validation strategy
10. Verification of the SOTIF (Area 2)
11. Validation of the SOTIF (Area 3)
12. Methodology and criteria for SOTIF release

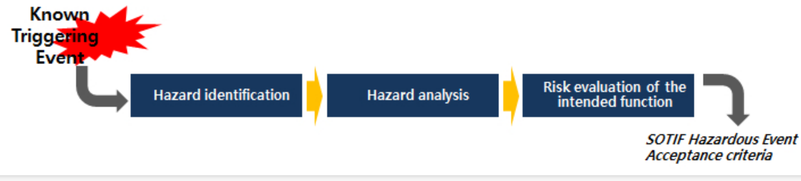


SOTIF 주용 활동에 대해 요약하여 설명하면 다음과 같습니다.

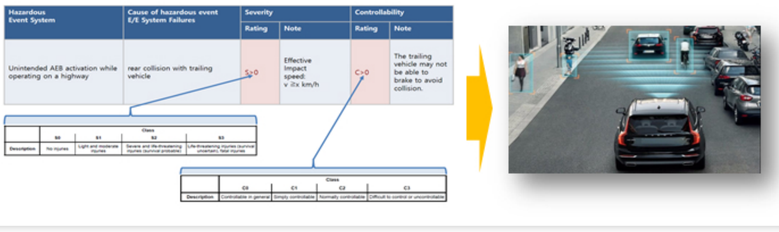
5. Functional and System Specification
   - SOTIF 활동을 위한 스펙의 명세 (e.g. 기능, 환경&타 시스템과 상호작용, 유스케이스, 시스템 적용 컨셉&기술)
6. Identification and Evaluation of hazards caused by the intended functionality
   - 시스템의 의도하지 않은 행위(Unintended Behavior)를 유발하는 기능에 대한 SOTIF 리스크의 식별 및 평가
7. Identification and Evaluation of triggering events
   - 시스템의 의도하지 않은 행위(Unintended Behavior)를 트리거링 하는 특정 운행 시나리오 (driving scenario)
8. Functional modifications to reduce SOTIF related risks
   - SOTIF Risk를 회피, 감소, 완화를 위해 시스템 스펙을 개선 (improvement) 하는 활동
9. Definition of the verification and validation strategy
   - SOTIF 활동을 효과적으로 Verification 및 Validation을 위해 전략을 수립하고 테스트 스펙을 명세하는 활동
10. Verification of the SOTIF (Area 2)
    - 시스템과 컴포넌트의 안전하지 않은 시나리오 (unsafe scenarios)에 대해 Verification 하는 활동
11. Validation of the SOTIF (Area 3)
    - 시스템과 컴포넌트가 실제 환경에서 허용 불가능한 수준의 리스크를 발생시키는 원인이 아님을 Validation 하는 활동
12. Methodology and criteria for SOTIF release
    - SOTIF 릴리즈를 위한 방법 및 기준에 대한 활동

SOTIF Hazard Identification and Evaluation

SOTIF HARA (Hazard Identification and Evaluation)는 성능 한계 또는 운전자 misuse와 같이 의도한 기능 제약으로 인해 발생하는 Hazard를 식별하고 평가하는 안전분석 방법으로 SOTIF 적용을 위한 첫 단계입니다.
SOTIF HARA는 아래와 같이 Hazard를 유발하는 Triggering Event에 대한 Hazard 식별 및 분석 후 이것에 대한 리스크 평가를 통해 SOTIF Hazardous Event와 Acceptance criteria를 도출하는 일련의 절차를 가집니다.



AEB (Autonomous Emergency Braking) 시스템의 경우 고속 도로 주행 중 주행 환경의 잘못된 인식으로 인해 의도하지 않은 AEB 기능이 작동하여 후방 차량과 충돌하는 경우 Severity 및 Controllability가 각각 S>0, C>0 이므로 현재의 AEB는 여전히 SOTIF Risk가 존재합니다. 따라서, 해당 SOTIF 리스크를 허용 가능한 수준(S=0, C=0)까지 낮추기 위해 SOTIF Measure를 체계적으로 적용함으로써 현 기능에 대한 개선(Improvement) 활동을 계속 수행해야 해야 합니다.



SOTIF Improvement Measures

SOTIF Risk를 회피(avoid), 감소(reduce), 완화(mitigate) 하기 위해 SOTIF Measure를 식별하고 이를 시스템 스펙에 명세화 하여 제품에 적용해야 합니다. SOTIF measure는 아래와 같이 구분 될 수 있습니다.

- *System improvement for Sensor*
- *System improvement for Actuator*
- *System improvement for Algorithms*
- *Functional restriction of intended function*
- *Handing over the authority from a system to the driver*
- *Reduction or mitigation of reasonably foreseeable misuse effects*

예를 들어 자율주행 차량에 장착된 센서가 기술적인 한계를 향상 시키기 위해 다음과 같은 Sensor 관점의 SOTIF measure가 고려될 수 있습니다.

- 센서 common cause failure 감소를 위해 Diverse technology 를 가진 센서 사용
- 개별 센서가 가지는 센싱 능력의 한계를 극복하기 위해 Camera, Radar, Lidar와 같은 독립된 센서 사용
- 2oo3 fail operational concept 과 같은 자유주행이 고려된 안전 아키텍처의 적용

또한, 다양한 주변 환경을 프로세싱 하는 최적화된 알고리즘 적용, Warning / Degradation 전략과 같은 Algorithm 관점의 SOTIF measure가 고려될 수 있습니다.

- AI 기반 Dynamic object movement, behavior prediction 등이 가능한 알고리즘 적용
- 다양한 주변 운행 환경을 빠르게 프로세싱 할 수 있는 High-performance decision 소프트웨어 적용
- 자율주행 레벨을 고려하여 지원하지 않는 SOTIF Use Case 발생 시 다양한 시스템의 상태가 고려된 알고리즘 개발 (e.g.
- Disabled Torque assist, Mechanical backup, Partial Torque assist, Full Torque assist)

마지막으로, 현재 가지고 있는 시스템의 의도한 기능에 대한 제약 (restriction) 을 통해 SOTIF 리스크를 최소화 하는 방법도 있습니다.

- 특정 SOTIF Use Case에 대한 관련 기능의 제약
  (e.g. lane detection 을 명확하게 하지 못하는 경우 steering intervention 최소화)
- 특정 SOTIF Use Case 발생 시 운전자의 차량 제어 권한을 시스템에 이관 (또는 운전자에게 이관)

이와 같이 자율 주행 차량의 궁극적인 안전을 보장하기 위한 수단으로 구체적인 SOTIF Measure의 식별 및 체계적인 적용이 필요합니다.