자율주행 시스템에 대한 안전 표준

이 진 우[1)]

충북대학교 산업인공지능학과[1)]

ISO/PAS 21448 SOTIF(Safety Of The Intended Functionality)

Jinwoo Lee[1)]

Chungbuk University[1)]

Key words : ISO/PAS 21448, SOTIF(Safety Of The Intended Functionality), ISO 26262, Autonomous Vehicle,(자율주행차량), Test Scenario

1. 서론

오늘날 자율주행 시스템에 대한 연구가 활발히 진행되고 있고, 그의 따른 결과물로 다양한 센서를 활용한 자율주행 기능을 갖춘 차량의 보급이 확산되고 있다. 레벨 1~2 에 해당되는 첨단 운전자 지원시스템(Advanced Driver Assistance System, ADAS)의 경우 차량에 설치 된 다양한 센서의 정보로 주변 정보를 파악, 운전자의 판단을 도와주고 제한적이지만 차량의 제어를 수행하고 있다.

자동차 시스템 기술의 변화로 차량의 전자제어 시스템의 종류 및 복잡도가 증가하였다. 또한, 센서, 제어기 엑추에이터, 전자기기 등이 기하급수적으로 증가하였고, 복잡한 알고리즘에 대한 처리가 증가하였다.

자율주행 자동차는 인지, 판단, 행동 등 3 가지의 오류로 인해 사고가 발생할 수 있으며, 2016 년 테슬라의 자율주행 자동차의 사망사고가 발생한 이후, 자율주행 자동차의 안전사고 및 인명사고가 끊임 없이 발생 하고 있다. 자동차에 탑재 되는 E/E(Electrical/Electronic) 시스템의 오류로 인한 사고를 대비하고, 예방하고자 SW 및 HW 의 설계 사양 정의, 시스템 통합 및 검증 등을 다루는 자동차 기능 안전 국제 규격인 ISO 26262 가 발표되었다.

그러나 최근 자율주행 시스템 내. SW 나 HW 의 고장이 아닌 자율주행 기능이 갑작스러운 주변 환경의 변화에 대응하지 못해 인지 센서가 장애물을 인식하지 못하거나 오인식하는 SW 알고리즘의 비중이 늘면서 SW 의 문제로 발생하는 인명 사고가 늘고 있다.

이러한 안전상의 문제들은 기존의 ISO 26262 의 기능안전에서 다루는 범위를 벗어나는 문제이다. 기존의 ISO 26262 는 자동차 설계 단계에서의 문제점을 파악하고 예방할 수 있었으나, 위와 같은 상황은 대비 하지 못하였다. 이를 극복하기 위하여 ISO/PAS 21448 SOTIF 표준이 발표되었다.

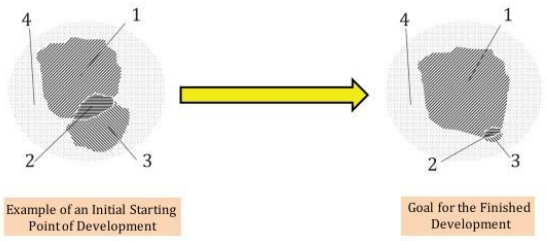
2. ISO/PAS 21448 (SOTIF)의 활동

2.1 SOTIF 의 개념과 목적

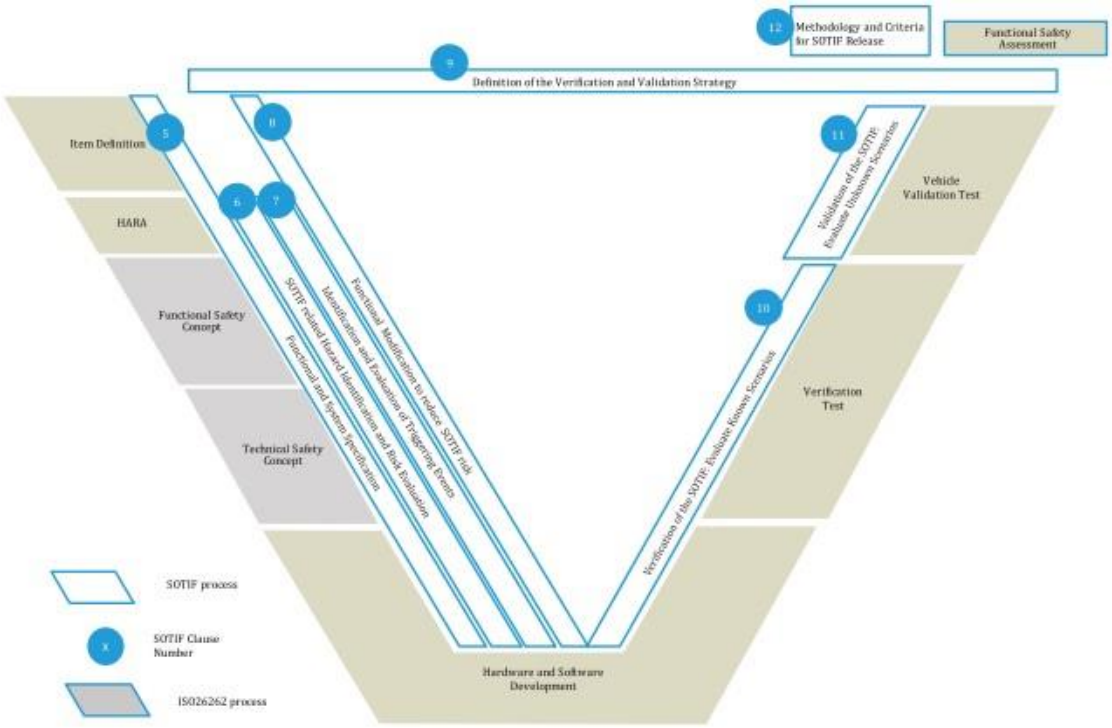
ISO/PAS 21448 (SOTIF)는 시스템 내 SW 나 HW 의 결함이나 고장이 없는 상황에서도 갑작스러운 주변 환경 변화로 인하여 인지 센서의 미인식 또는 오익식이 발생하는 등의 신뢰성 저하 문제를 다루는 기능안전 표준이다.

SOTIF 는 크게 4 영역으로 구분된다. 시나리오를 알고 있으며, 안전한 상황 (area 1), 시나리오는 알고 있지만, 위험한 상황 (area2), 시나리오는 모르지만, 안전한 상황 (area4), 시나리오도 모르고, 안전하지도 않은 상황 (area3)과 같이 4 영역으로 구분된다. SOTIF 를 통해 area 3 에서 시나리오를 식별하여 area 2 로 변환하고, 다시 area 2 를 area 1 의 영역으로 변환한다. 결론적으로 area 2 와 area 3 을 최소화하는 동시에 area 1 의 영역을 최대화 하는 것이 목적이다.

그림 1 은 위에 설명한 SOTIF 의 개념과 목적을 보여주고 있다.



[Figure 1] Purpose of ISO/PAS 21448 Activities



[Figure 2] Relationship between ISO 26262 and SOTIF in the V model

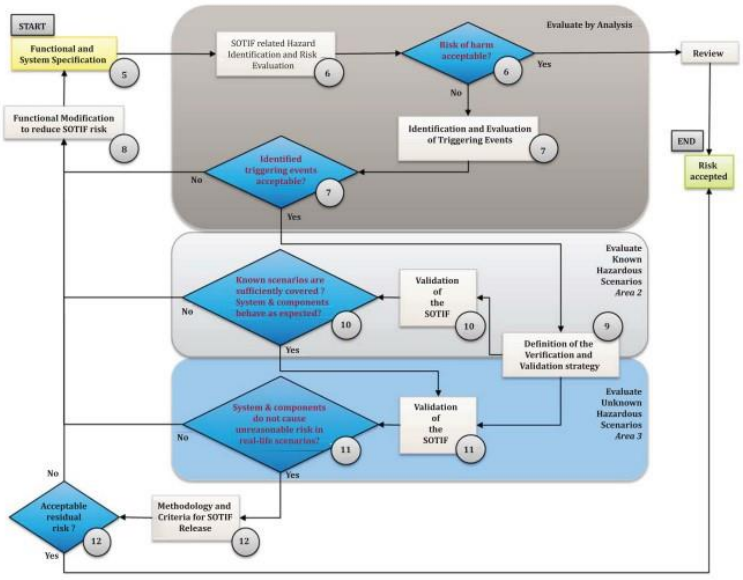
그림 2 는 V 모델에서 ISO 26262 와 SOTIF 프로세스와의 관계를 보여준다. 그림에서 보는 바와 같이 SOTIF 는 시스템 성능에 대한 요구사항부터 시작하여, V 모델 전반에 걸쳐 수행이 이루어진다.

의도된 기능의 가능한 위험 행동은 잠재적 위험 사건을 식별하는 위험 식별 및 위험 평가의 대상이 된다. 잠재적으로 위험한 사건이 원인제공을 초래하지 않는 것으로 판명된 경우, 개선이 필요하지 않으며 의도된 기능은 불합리한 위험이 없는 것으로 간주할 수 있다.

위험 요소 가능성이 있는 것으로 판명된 경우, 발생 가능한 위험 유발 사건(예: 특정 환경 조건에서 특정 물체의 오인식 또는 운전자 오남용)에 대한 분석을 수행한다.

이러한 과정을 통해 제품 개발 단계에서는 일반적으로 최종 기능 및 시스템 사양을 작성하기 위해 여러 번 반복해야 한다.

2.2 SOTIF 의 활동 방법



[Figure 3] SOTIF Process

그림 3에서 보여주는 것처럼 SOTIF 프로세스는 크게 3단계로 구분된다. 먼저 첫 번째 단계는 그림 3의 진한 회색 박스로 나타낸 evaluate by analysis에서는 기능과 시스템 사양, use case, scene, 시나리오 등을 정의하는 단계에 위험원을 식별하고 검증한다.

두 번째 단계는 그림 3의 가운데 부분으로 식별된 area 2의 시나리오를 기반으로 test case를 도출하며, 도출된 test case를 바탕으로 평가를 한 후 안전 목표에 달성하였는지를 확인하는 단계이다. 마지막으로 세 번째 단계는 완성된 시스템의 테스트 등을 기반으로 알지 못하는 시나리오에 대한 평가 및 안전성을 검증한다.

- 의도한 기능과 관련된 SOTIF 관련 위험 요소를 식별하고 평가함.
- 위험 발생 이벤트의 식별 및 평가.
- 기능 수정 또는 use case 제한을 통해 필요에 따라 시스템 설계를 개선하여 SOTIF 위험을 감소시킴.
- SOTIF 에 관한 설계의 적합성을 검증하고 확인함.

2.2.1 설계 단계

위험을 관리하기 위한 요구사항을 정의하는 단계이다. SOTIF 에서 제안 하는 다양한 기능 개선 방안들을 적용하여 평가 된 위험 항목의 회피, 감소, 완화를 목적으로 기능(요구사항) 개선을 수행한다.

SOTIF 관련 위험 회피, 감소, 완화
시스템 개선 방안
센서 성능, 정확도 향상
인식, 의사결정 알고리즘 성능 향상
검증 가능성 향상
기능 제한 방안
특정 사용 사례에 대한 기능/권한 제한
시스템에서 운전자로의 권한 인계
인간 – 기계 인터페이스(HMI) 개선
합리적으로 예측 가능한 오용 효과 감소 및 완화
모니터링 및 경고 시스템 구현

[Table 1] Requirements

표 1과 같이 요구 사항을 통해 센서의 성능을 개선할 수 있으며, 시스템을 정상적으로 구현 할 수 있도록 도와주는 단계이다.

아래 표 2와 같이 요구 사항을 적용하여, 기능 개선을 통해 외부 환경 요인으로 발생 될 수 있는 사고를 줄일 수 있다.

구분	발생 원인	SOTIF 조치 예시
시스템적 요인	시스템의 성능 제한 초과	1. 시스템의 성능을 감소시키며, 해당 상황을 운전자에게 인지시키고, 제어 권한을 인계함 2. 인계 후 해당 기능은 종료
운전자 요인	합리적으로 예측 가능한 오용	1. 운전자에게 올바른 동작에 대해 알림 2. 잘못된 동작이 감지될 경우 경고 전달

[Table 2] Examples of functional improvement

2.2.2 검사 단계

요구사항 자체가 실제 위험에 대해 적절히 대응하는지를 확인하는 단계를 검사 단계라고 한다.

아래 표 3에 명시된 다양한 방법론들을 적용하여 요구사항 및 설계 단계에서 정의 된 기능별 요구 사항들이 잠재적인 위험에 대처하기 위해 적절히 설계 되었는지 확인한다.

요구사항 분석
외부 및 내부 인터페이스 분석 (a)
동일 등급에 대한 생성 및 분석
경계 값 분석
지식 및 경험에 기초한 추측 오류
기능 의존성 분석
공통 한계 조건, 시퀀스 및 종속 고장 발생원 분석
환경조건 및 운영 사용 사례 분석 (b)
현장 경험 분석 (c)
시스템 아키텍처 분석 (중복 설계 포함)
센서 설계 및 알려진 잠재 한계 분석
알고리즘 및 알고리즘의 decision path 분석
시스템 노화 분석
트리거 조건 분석
성능 목표 분석
고장 분석에서 측정 가능한 파라미터의 분석
경계 값에서 코너 케이스와 엣지 케이스 분석 (d)
기존 시스템의 SOTIF 관련 업데이트 분석
수집된 테스트 케이스와 시나리오를 통한 데이터베이스 사용 (e)
a: Car2X, 지도 포함 (사용 가능한 경우) b: 요소 또는 시스템의 잠재 위험 행동에 대해 이미 알려져 있는 발생원 포함 c: 다양한 주행 조건, 주행 스타일, 주행 환경 및 운전자 클레임 고려 d: 엔지니어링에서 코너 케이스는 정상 작동 파라미터 외부에서 발생하는 여러 문제 또는 상황을 포함 엣지 케이스는 극단적인(최대 또는 최소) 동작 파라미터(알고리즘 처리 값이 알고리즘의 특성에 따른 일정한 범위를 넘을 경우 실제 수행이 기대 값 범위를 벗어나는 경우) 발생하는 문제 또는 상황 e: 다른 표준활동의 결과 사용

[Table 3] Inspection and Verification Steps

기술 검토, 선택된 SOTIF의 루프 시험(SIL / HIL / MIL)에서 관련 시나리오의 적용 범위가 높은 테스트 케이스, 잠재적 발생 이벤트(triggering event)의 주입하여 확인한다.

2.2.3 검증 단계

검증 된 요구사항이 그 외의 돌발 상황에서 심각한 위험을 발생하는지 지속적으로 확인하는 타당성 단계를 검증 단계라고 한다.

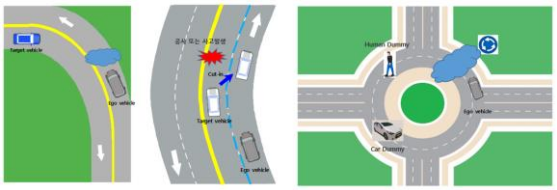
1, 2 단계를 거친 각 요구 사항들이 고려 된 위험 항목 외에 추가적인 위험 동작에서도 정상적으로 대응 가능한지, 시뮬레이션 시험 주행 등을 반복하며 기능에 대한 동작을 확인한다.

SOTIF와 관련 된 실차 테스트는 성능에 영향을 미칠 수 있는 외부요인을 파악하여 테스트 하는 것이 중요하다. 외부 환경적인 요소로는 역광, 저조도, 갑작스러운 조도의 변화, 비, 눈, 안개, 오염, 황사 등이 존재한다. 표 4는 조건별 끼치는 영향에 대해 나타내고 있다.

분류	원인	영향
광원	역광	• 이미지 센서의 광포화로 인한 장애물을 오인식 또는 미인식
	낮은 조도	• 장애물 감지 불가로 인한 미인식
날씨	비	• 빗방울에 의한 왜곡으로 인한 미인식 또는 오인식 • 차선의 미인식 또는 오인식
	눈	• 시야 차단으로 인한 장애물 및 차선을 오인식 또는 미인식
	안개	• 짧은 가시거리로 인한 장애물 및 차선을 오인식 또는 미인식
도로 상태	곡선로	• 전방의 차량을 옆 차선의 차량으로 오인식
	경사로	• 광고판에 있는 사람 그림을 보행자로 오인식
	결빙	• 보이지 않는 도로의 결빙으로 인한 통제 불가 가능성
	노면 반사	• 왜곡된 이미지로 인한 장애물 오인식
외부 환경	진흙	• 시야 차단으로 인한 장애물 및 차선의 오인식 또는 미인식

[Table 4] Effect of each condition

표 4에서 보여주는 바와 같이 다양한 원인으로 인해 장애물을 미인식하거나 오인식하는 문제가 발생할 수 있으며, 이러한 문제는 SW나 HW의 고장과는 관계없이 의도치 않은 위험을 유발한다.



[Figure 4] SOTIF Test Scenario

그림 4와 같이 예기치 못한 사고 또는 공사 상황 발생시 Cut-in, 비, 눈, 안개 상황에서의 사람 및 차량 감지, 회피 등 다양한 시나리오 구현을 통해 SOTIF의 준하는 성능 평가가 가능하다.

안전상의 이유로 검증 단계에 실제 트랙에서 테스트하기 어려운 시나리오를 성능 시험장 (Proving Ground, PG)을 통해 실차와 시뮬레이션 혼합 테스트를 진행 할 수 있다.

3. 결론

오늘날 자율주행 기능을 갖춘 차량의 보급이 증가함에 따라 이와 관련된 안전에 대한 관심도 높아졌으며, SW 나 HW 의 결함으로 인한 고장으로 발생하는 안전사고 및 인명사고를 예방하고자 SW 및 HW 의 설계 사양 정의, 시스템 통합 및 검증 등을 다루는 ISO 26262 가 제정되었다. 하지만 최근 SW나 HW의 결함이 없음에도 갑작스러운 외부 환경 변화로 인한 사고에 대한 이슈가 대두 되었으며, 이는 ISO 26262 에서 다루는 범위를 벗어난 문제이다.

따라서 시스템의 고장 외적인 원인으로 발생하는 위험에 대응하고자 ISO/PAS 21448 SOTIF 가 발표되었다.

어떤 시뮬레이션을 진행하느냐는 자율주행 개발 및 검증의 복잡하고 다양한 요구사항과 단계에 따라 달라질 수 있는 것이고, 이러한 시뮬레이션을 실제와 유사하게 모사할 수 있는지 여부에 따라 시뮬레이션의 성능, 결과에 대한 신뢰도가 높아질 수 있다.

센서 모델의 물리적 특성을 정확하게 표현할 수 있는지, 차량의 거동을 모사하는 차량 동역학 특성 및 타이어와 노면과의 관계를 반영할 수 있는지, 주행 환경을 구성하는 데 필요한 여러 도로 인프라, 건물, 보행자, 대상 차량이 아닌 상대 차량의 주행 또한 물리적으로 재현할 수 있는지에 따라 정확도 높은 케이스를 만들 수 있을 것 같다.

References

1. ISO26262: Road Vehicles – Functional Safety, International Organization for Standardization, 2018

2. ISO/DIS 21448: Road Vehicles – Safety of the intended functionality, International Organization for Standardization, 2021
3. ISO/PAS 21448: Road Vehicles – Safety of the intended functionality, International Organization for Standardization, 2019
4. Moon, B. J. Trend of Functional Safety & SOTIF Regulation for Connected & Automated Vehicle, Auto Journal 12. 2020
5. WP29-GRVA-02-09