Transactions of KSAE, Vol. 33, No. 1, pp.61-80 (January, 2025)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2025.33.1.61

자율주행 시스템의 SOTIF 확보를 위한 STPA 안전 분석 및 V & V 방법론

한 승 재[1] · 변 진 규[1] · 안 수 민[1] · 유 진 우[*2]

국민대학교 자동차모빌리티대학원[1] · 국민대학교 자동차IT융합학과[2]

Derivation of STPA Safety Analysis and V&V Methodology for Ensuring SOTIF in Autonomous Driving System

Seungjae Han[1] · Jingyu Byeon[1] · Sumin Ahn[1] · Jinwoo Yoo[*2]

[1]*Graduate of Automobile and Mobility, Kookmin University, Seoul 02707, Korea*
[2]*Department of Automobile and IT Convergence, Kookmin University, Seoul 02707, Korea*
(Received 5 September 2024 / Revised 25 September 2024 / Accepted 30 September 2024)

Abstract : In this study, we established the safety requirements and risk mitigation strategies for a longitudinal Smart Cruise Control(SCC) system by using LiDAR sensors, focusing on Safety of The Intended Functionality(SOTIF). We applied the System-Theoretic Process Analysis(STPA) to identify Unsafe Control Actions(UCAs), and developed risk scenarios by analyzing disturbance factors in LiDAR sensors. These scenarios were assessed in a virtual simulation, determining Effective Collision Speed, Time to Collision(TTC), and the Fault Tolerant Time Interval(FTTI). We evaluated the feasibility of driver control transfer within FTTI. If it was deemed infeasible, additional time to handle defects was considered to meet safety requirements. Furthermore, safety mechanisms were designed to ensure timely transitions and effective handling. Simulation results confirmed that these mechanisms met safety requirements and mitigated risks. This study provided a comprehensive guide to the SOTIF process, supporting future autonomous driving research and commercialization by enhancing safety standards.

Key words : Autonomous driving system(자율주행 시스템), STPA(시스템-이론적 프로세스 분석), SOTIF(의도된 기능의 안전성), Hazard analysis & Risk assessment(위험 분석 및 평가), Safety requirement(안전 요구 사항), Safety mechanism(안전 메커니즘), Verification & Validation(검증 및 확인)

Nomenclature

K_p	: proportional gain
K_i	: integral gain
V_{xe}	: the effective collision velocity of vehicle x, km/h
V_x	: the collision initiation velocity of vehicle x, km/h
V_C	: the post collision velocity of both vehicle, km/h
m_x	: the mass of vehicle x, kg
τ	: threshold

Subscripts

L	: loss
VH	: vehicle hazard
SC	: safety constraint
CS	: causal scenario
TC	: triggering condition
TOT	: take over time
TOR	: take over request time
TOP	: take over possibility

*Corresponding author, E-mail: jwyoo@kookmin.ac.kr

1. 서 론

자율 주행 기술의 급속한 발전에 따라 자율 주행 시스템이 점점 더 많은 안전 책임을 지게 되면서 지능형 차량의 안전 문제 해결이 중요한 과제로 대두되고 있다.[1,2] 현재 자율 주행 차량이 직면한 주요 안전 문제는 기능 안전(Functional safety), 정보 보안(Automotive-Software process improvement and capability determination) 그리고 의도된 기능 안전(Safety Of The Intended Functionality, SOTIF)에 주로 집중되어 있다.[3-5] 이 중 SOTIF는 도로 차량의 안전성과 관련된 개념이며, 이 개념은 시스템의 고장이나 오작동이 아닌, 의도된 기능 자체에서 발생할 수 있는 위험을 다룬다.[6] 전통적인 기능 안전 국제 표준인 ISO 26262에서는 시스템 고장과 관련된 위험을 완화하는 데 초점을 맞추고 있지만, SOTIF는 이와 별도로 시스템이 올바르게 작동하더라도 발생할 수 있는 위험, 즉 의도된 기능의 한계나 환경 변화에 대한 대응 부족 등에서 발생할 수 있는 위험을 다루는 개념이다. ISO 21448은 바로 이 SOTIF를 다루고 있으며, 이 표준은 차량의 자율 주행 기능과 관련된 다양한 위험 요소를 최소화하기 위해 고안되었다. 특히 차량 외부나 내부 환경을 인식하여 상황을 파악하는 시스템, 예를 들어 센서를 통해 수집된 데이터를 처리하고 의사 결정을 내리는 시스템에서 발생할 수 있는 위험에 초점을 맞추고 있다. SOTIF의 첫 번째 판은 2019년에 발행되었으며, 2022년에 새롭게 개정되었다.

SOTIF 관점의 문제로 인해 발생한 자율 주행 사고는 많은 안전 사고와 인명 피해를 초래해왔다. 대표적으로 자율주행의 인지 시스템의 기능 불충분 및 성능 한계 상황에서 객체를 미인지/오인지하여 발생한 사고 사례들이 다수 존재한다.

2019년 테슬라 Model 3의 사고에 따르면, 고속도로에서 자율주행을 하던 해당 차량이 고속도로로 진입하기 위해 좌회전하던 세미 트레일러를 미인지하여 충돌 사고가 발생했다. 차량은 충돌 후에도 끝까지 트레일러를 인지하지 못해 결국 트레일러의 밑을 그대로 지나가며 약 480 m를 더 진행해서야 멈췄다.[7]

2018년 우버 시험용 차량의 사고에 따르면, Camera, Radar, LiDAR 등으로 이루어진 자율주행 시스템이 탑재된 차량이 전방의 자전거를 끌고 가던 보행자를 오인지하여 충돌 사고가 발생했다. 인지 시스템이 보행자 인식을 너무 늦게 했기 때문에, 그만큼 늦은 시점에 수행된 제동 제어가 적절히 수행되지 않았다.[7]

이처럼 자율주행 센서의 미인지 혹은 오인지 사례로 인한 불합리한 위험을 줄이고자 하는 SOTIF 연구가 진행되고 있으며, 시스템 수준에서 위험을 해결하지 못하는 경우 운전자에게 적절한 제어권을 전환해야 하는 연구는 필수적이다.

Choi 등[8]은 SOTIF 관련 연구가 대부분 시스템 성능 하락에 따른 위험 시나리오를 도출했지만, 이를 실제 테스트 환경에서 검증하거나 시스템 설계 개선을 위한 구체적인 가이드라인 도출이 부족하다는 점을 지적하면서, Camera 센서를 대상으로 SOTIF 관점의 위험 분석 및 평가 방법론을 제시하였다. 위험을 판단하기 위한 방법으로 시스템의 Time budget을 도입하였으며, 도출한 Time budget 내에 제어권 전환이 이뤄질 수 없는 경우 추가적인 결함 대응 시간을 도출하는 것을 제안하였다.

그러나 안전 요구 사항은 시스템의 수명 주기 동안 지속적으로 업데이트되고 개선되어야 한다. 이를 위해서는 구체적인 안전 메커니즘의 설계가 필수적이며, 이러한 메커니즘을 통해 시스템에서 발생할 수 있는 불합리한 위험을 줄이는 것이 중요하다.

또한 자율주행 Level 3 이상의 경우, LiDAR 센서의 사용이 필수적이지만, 현재까지는 LiDAR 센서의 성능 한계 상황에 대한 SOTIF 연구가 매우 부족한 실정이다.[9]

따라서 기존 연구를 바탕으로, 본 논문은 LiDAR 센서의 성능한계 상황 발생 시 SCC(Smart Cruise Control)시스템의 SOTIF 확보를 위한 가이드라인을 제안한다. STPA (System-Theoretic Process Analysis)를 기반으로 시스템의 위험 발생 요인과 시나리오를 정의하며, 위험 분석 및 평가를 통해 안전 요구 사항을 도출한다. 나아가 불합리한 위험을 방지하기 위한 안전 메커니즘 설계를 통해 안전 요구 사항을 만족하여 시스템의 SOTIF 달성을 목표로 한다.

2장에서는 SOTIF의 정의, 주요 목적, 그리고 프로세스에 대한 개요를 보여준다. 3장에서는 STPA 기반 안전 분석을 진행하여, SOTIF관점의 위험을 평가하고자 하는 위험 발생 원인 시나리오 도출 과정을 보여준다. 4장에서는 위험을 평가 및 검증하기 위한 시뮬레이션 환경 구성을 보여준다. 5장에서는 SOTIF 확보를 위한 안전 요구 사항을 도출하고, 안전 메커니즘 설계와 구현을 보여주며, 6장에서 결론을 맺는다.

2. SOTIF Overview

SOTIF는 의도된 기능의 안전을 의미하며, 의도된 기능 불충분 또는 성능 한계로 인해 발생할 수 있는 불합리한 위험을 방지하기 위해 설계된 개념이다. ISO 26262는 의도된 기능이 안전하다고 가정하고, E/E 시스템의 오작동으로 인한 위험을 다룬다. 그러나 시스템에 오작동이 없더라도 사양 부족이나 성능 한계로 인해 위험이 발생

할 수 있다. 이러한 위험을 방지하기 위해 SOTIF가 제정되었으며, 이는 의도된 기능의 안전성을 보장하기 위한 지침을 제공한다. SOTIF를 확보한다는 것은 차량 수준에서 의도된 기능의 사양 부족이나 E/E 시스템의 성능 부족으로 인한 위험이 없음을 의미한다.

2.1 SOTIF Objectivity

SOTIF의 주요 목적은 사양 부족 및 성능한계로 인한 위험 수준이 낮다는 것을 보장하기 위해 수행되는 활동과 논리를 설명하는 것이다. ISO 21448 표준 문서에 의하면 SOTIF 확보를 위해서 시나리오 기반 방법을 제안한다. Fig. 1을 보면, 시나리오는 4가지 영역으로 나눌 수 있다.

영역 1은 시스템이 의도한 대로 작동하며, 예상된 안전한 결과를 가져오는 시나리오다. 영역 2는 시스템이 의도한 대로 작동하지 않으며, 위험한 결과를 초래하는 시나리오다. 영역 3은 시스템이 예상치 못한 방식으로 작동하지만, 결과적으로 안전한 상태를 유지하는 시나리오다. 영역 4는 시스템이 예상치 못한 방식으로 작동하며, 위험한 결과를 초래하는 시나리오다. SOTIF 활동을 통해서 영역 2와 영역 3의 위험을 줄이고, 영역 1을 지속적으로 확장하여 SOTIF 확보에 대한 신뢰를 높이는 것이 SOTIF 활동의 목적이다.[10]

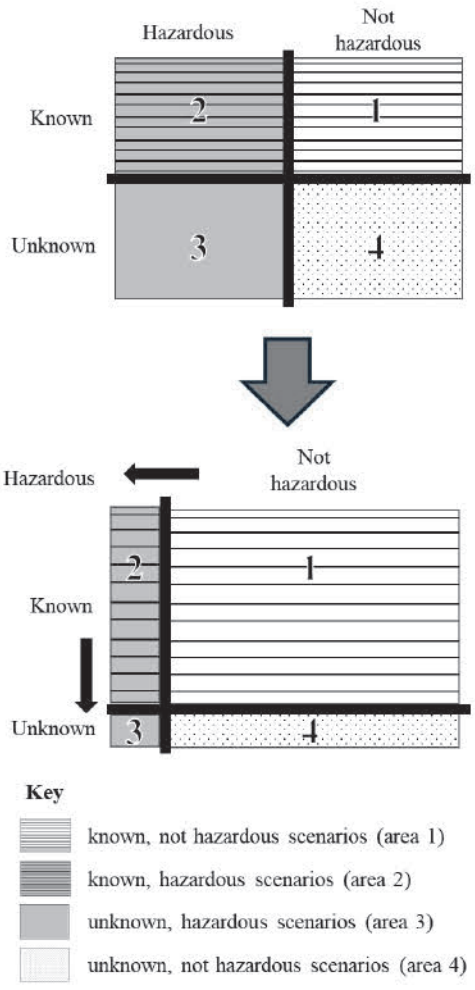


Fig. 1 Visualisation of the four scenario categories

2.2 SOTIF activities

SOTIF 활동에는 크게 두 가지 절차로 나눌 수 있으며, 첫 번째는 "Evaluate by Analysis" 단계이다. 이 단계에서는 기능과 시스템 사양, 사용 사례, 시나리오 등을 정의하는 단계로, FMEA(Failure Modes and Effects Analysis), FTA(Fault Tree Analysis), HAZOP(Hazard and Operability Study)등의 방법론을 활용하여 잠재적인 위험원을 식별하고 이를 체계적으로 검증한다.[11] 두 번째는 "Verification & Validation" 단계이다. 이 단계에서는 첫 번째 단계에서 식별된 위험 시나리오를 기반으로 시스템의 안전성을 평가하고, 이를 통해 시스템이 지켜야 할 안전 요구 사항을 도출한다. 특히 이 과정에서는 SOTIF 확보를 위해 Fig. 1의 영역 2와 3에서 나타난 위험을 최소화했는지를 확인하는 것이 핵심이다. 이를 통해 시스템이 예상치 못한 상황에서도 안전하게 동작할 수 있도록 보장한다. 이후 절차로는, 앞선 두 가지 단계의 상호작용을 통해 자율주행 시스템의 안전성을 확보하는 데 중점을 둔다.[11]

본 논문에서는 ISO 21448에서 제안하는 SOTIF 활동을 바탕으로 새로운 프로세스를 제안한다. STPA를 기반으로 SOTIF에서 요구하는 Triggering Condition 즉 시스템의 의도된 기능이 위험한 상황으로 이어질 수 있는 특정 조건이나 상황을 도출하고 관련된 시나리오를 구성한다. 위험 분석 및 위험 평가를 통해 안전 요구 사항을 도출하며, 이를 만족할 수 있도록 안전 메커니즘을 설계한다. 설계된 안전 메커니즘을 적용하여 위험 시나리오를 재평가하고 평가 결과 위험원이 최소화되었다고 판단된다면, SOTIF 프로세스를 종료한다. 하지만 잔여 위험이 위험 수준 이상으로 존재한다고 평가된다면, 또다시 추가적인 안전 메커니즘을 설계하여 SOTIF 목적을 달성할 때까지 반복한다. 이를 Fig. 2의 블록 선도로 표현하였다.

3. STPA 기반 Triggering Condition 분석

STPA는 시스템의 복잡성과 상호작용을 고려하여 안전성을 분석하는 최신 안전 분석 방법론으로, 전통적인 안전 분석 기법들과 차별화된다. 전통적인 안전 분석 기법들은 주로 물리적 고장(Failure)이나 하드웨어적 결함에 초점을 맞추는 경향이 있다. 이러한 기법들은 고장의

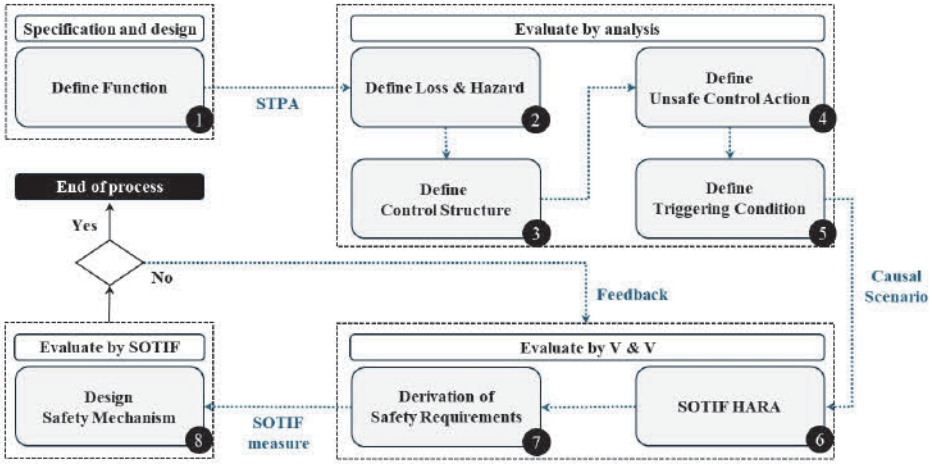


Fig. 2 Block diagram of new ISO 21448 - SOTIF activities

결과를 분석하고, 그에 따른 안전 조치를 설계하는 데 중점을 둔다. 반면, STPA는 물리적 고장을 넘어서 시스템의 제어 구조와 피드백 루프에 대한 심층적인 분석을 통해 잠재적인 위험 요소를 식별하고 이를 사전에 예방하는 데 초점을 맞춘다. 또한 시스템의 복잡한 상호작용 속에서 발생할 수 있는 기능적 실패와 비정상적인 시스템 동작을 다루며, 이러한 분석을 통해 시스템 전반의 안전성을 강화하는데 기여한다. Fig. 3은 STPA의 Flowchart를 보여주며 4단계로 이루어져 있다. 먼저 손실과 위험을 정의하고, 이후 분석하고자 하는 시스템을 제어관점에서 모델링한다. 이때 컴포넌트간 제어 명령을 정의할 수

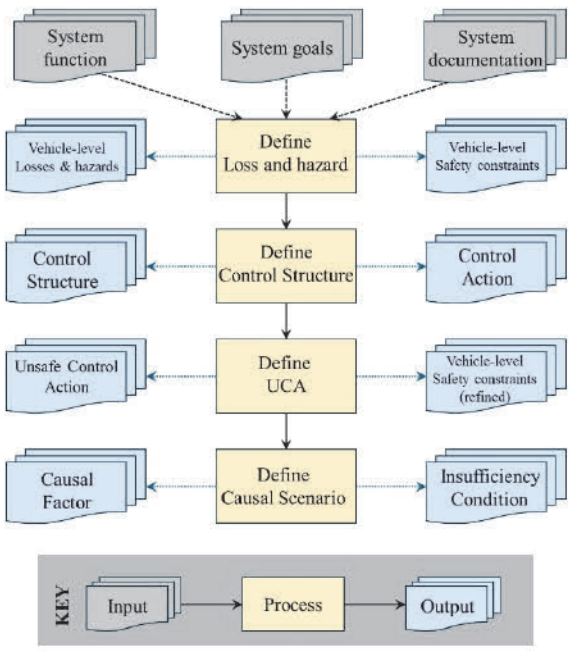


Fig. 3 Flowchart of STPA Process

있으며, 이는 다음 단계인 위험한 제어 명령을 정의하는 데 사용된다. 마지막 단계에서는 위험한 제어 명령을 발생할 수 있는 원인을 식별하여 시나리오를 도출하는 것으로 마무리된다.[12] 이 과정에서 도출된 원인 시나리오는 SOTIF 관점의 위험을 유발시키는 Triggering condition으로 작용할 수 있다.[12]

3.1 Defining the loss and hazard

STPA의 첫 번째 단계에서는 시스템에 대한 이해를 바탕으로 시스템이 초래할 수 있는 다양한 손실 유형을 식별하고, 식별된 손실을 방지하기 위해 차량 수준에서 발생할 수 있는 잠재적인 위험 행동을 체계적으로 분석한다.[13] 본 논문에서는 LiDAR 기반 종방향 SCC 시스템의 충돌 방지에 중점을 두고 있으며, 따라서 피해야 할 손실로는 주변 차량 간 충돌로 인한 차량의 손실 또는 손상(L1)과, 차량의 급격한 거동으로 인해 탑승자에게 발생할 수 있는 잠재적인 부상(L2)이 있다. 이러한 손실은 잘못된 가속 명령으로 인해 안전거리가 확보되지 않는 상황(VH1)과, 잘못된 감속 명령으로 인해 안전거리가 확보되지 않는 상황(VH2)을 주요 위험 요소로 식별하였으며, 이를 Table 1에 정리하였다.

정의된 Hazard를 바탕으로 시스템의 안전성을 확보하기 위한 안전 제약 조건(Safety constraints)을 도출한다. 이러한 제약 조건은 시스템의 모든 제어 동작이 안전하게 수행되도록 보장하기 위해 필요하다. 본 논문에서는 차량 수준에서의 위험 요소와 이에 대응하는 안전 제약 조건을 도출하였으며, 이를 Table 2에 정리하였다. 이러한 안전 제약 조건은 시스템의 안전성을 확보하기 위해 필수적으로 준수해야 하며, 이를 통해 LiDAR 기반 종방향 SCC 시스템의 잠재적 위험을 식별하고 분석할 수 있다.

Table 1 Loss and hazard identification

Loss	Vehicle-level hazards
[L1] Loss or damage to a vehicle due to collisions with surrounding vehicles	[VH1] Failure to maintain a safe distance due to incorrect acceleration command output
[L2] Injury to passengers inside the vehicle due to sudden movements of the vehicle	[VH2] Failure to maintain a safe distance due to incorrect deceleration command output

Table 2 Vehicle-level safety constraints identification

Hazard	Description
[VH1] Failure to maintain a safe distance due to incorrect acceleration command output	[SC1] Incorrect acceleration commands must be prevented to ensure a safe distance from the leading vehicle.
[VH2] Failure to maintain a safe distance due to incorrect deceleration command output	[SC2] Incorrect deceleration commands must be prevented to ensure a safe distance from the leading vehicle.

3.2 Modeling of the control structure

STPA 2단계는 분석 시스템을 Control structure 형태로 모델링하는 단계이다. Control structure는 시스템의 제어 흐름을 파악하고 관련 컴포넌트를 식별하는 제어 아키텍처로, 타겟 시스템과 주변 환경의 상호작용을 모델링하며, 제어 명령과 피드백 루프를 포함한다. 이러한 구조를 통해 시스템의 안전성을 분석하고 잠재적 위험 요소를 식별할 수 있다.

Fig. 4는 LiDAR 기반 SCC 시스템의 Control structure를 나타낸다. 이 시스템에서 전방 차량의 정보는 LiDAR 센서를 통해 수집되며, 상대 거리 정보가 SCC 시스템에 전달된다. SCC 시스템은 자차량의 속도와 안전 거리를 토대로 차량 간 거리를 유지하거나 가/감속 명령을 생성하여 차량에 전달한다. 차량은 이 정보를 바탕으로 Throttle, Brake 신호를 받아 차량을 제어하게 된다. 이러한 Control structure는 시스템의 전반적인 제어 흐름을 이해하고, 이를 통해 Control Actions(CA)를 정의하는 데 활용된다. 본 논문에서는 LiDAR 센서 기반 SCC 시스템에서 객체 인식(Object detection) 그리고 객체 추적(Object tracking)을 CA로 정의하였다.

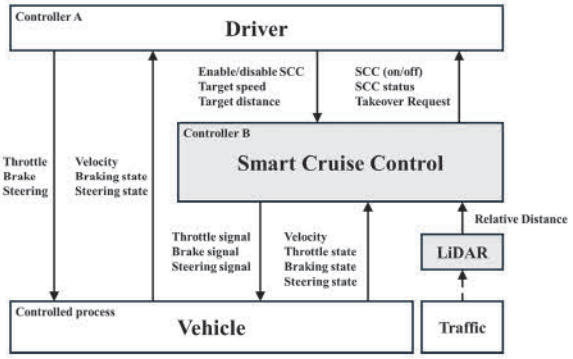


Fig. 4 SCC System Control Structure

3.3 Identification of unsafe control actions

STPA 3단계는 시스템의 제어 명령이 어떤 상황에서 안전하지 않은지 Unsafe Control Action(UCA)를 식별하는 과정이다. UCA는 특정 상황과 최악의 환경에서 시스템을 위험 상태로 몰고 갈 수 있는 제어 명령을 의미한다. UCA를 도출하기 위해 앞서 정의된 CA에 STPA 가이드북에서 제시한 4가지 Guideword를 적용하여, 다음 조건들이 정상적으로 안전한 제어 동작을 어떻게 위험하게 만들 수 있는지를 분석한다.[14] 4가지 STPA guidewords는 다음과 같다.

- Not providing causes hazard
- Providing causes hazard
- Too early, too late, out of order
- Stopped too soon, applied too long

이로부터 도출된 UCA는 Table 3에 정리하였다.

Table 3을 보면, controller인 SCC 시스템의 제어 명령인 Object Detection과 Object Tracking에 대해, 4가지 타입의 STPA guidewords를 조합하여 발생할 수 있는 잠재적인 위험을 분석하였다. 대표적으로 UCA-1은 SCC 시스템의 LiDAR 센서가 Object Detection 정보를 제공하지 않았을 경우를 정의하였으며, 이로 인해 발생할 수 있는 차량 수준의 위험은 자차량의 잘못된 가속 명령 출력으로 인해 안전 거리를 유지 못함[VH1]이다. 같은 방법으로 UCA-8까지 추가적으로 정의하였으며, 이러한 분석을 통해 시스템의 잠재적인 위험을 미리 식별하고 적절한 대책을 마련할 수 있다.

Table 4는 UCA가 발생할 경우, 시스템의 안전 제약 조건을 추가로 정의한 것이다. 해당 단계에서 안전 제약 조건은 UCA 발생을 방지하기 위해 제어 시스템에서 반드시 준수해야 하는 명제 또는 불변성을 정의한 것이다. 이 과정은 UCA 발생 방지가능성을 최소화하는데 필수적이다.

Table 3 Unsafe control actions for the control action of the controller SCC

Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Object Detection	UCA-1 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor does not provide object recognition information. [VH1]	UCA-2 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides incorrect object recognition information. [VH1] [VH2]	UCA-3 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides object recognition information either too late, too early, or in the wrong sequence. [VH1] [VH2]	UCA-4 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor stops providing object recognition information too early or continues providing it for too long. [VH1] [VH2]
Object tracking	UCA-5 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor does not provide relative distance information. [VH1]	UCA-6 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides incorrect relative distance information. [VH1] [VH2]	UCA-7 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides relative distance information either too late, too early, or in the wrong sequence. [VH1] [VH2]	UCA-8 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor stops providing relative distance information too early or continues providing it for too long. [VH1] [VH2]

Table 4 Transformation of UCAs into requirements(safety constraints)

Unsafe control action	Safety constraint
UCA-1 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor does not provide object recognition information. [VH1]	SC-1 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor must provide object recognition information. [UCA-1]
UCA-2 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides incorrect object recognition information. [VH1] [VH2]	SC-2 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor must accurately identify objects. If it fails to do so, control must be transferred to the driver in a timely manner. [UCA-2]
UCA-3 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor provides object recognition information either too late, too early, or in the wrong sequence. [VH1] [VH2]	SC-3 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor must provide object recognition information in a timely manner. [UCA-3]
UCA-4 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor stops providing object recognition information too early or continues providing it for too long. [VH1] [VH2]	SC-4 : When the ego vehicle is using the SCC system to follow the vehicle in front, the LiDAR sensor must provide object recognition information accurately at the required times. [UCA-4]

Table 5 Identification of Triggering Conditions

Causal scenario	UCA	Insufficiency condition	Triggering condition
CS-1	UCA-1	[IC-1] The LiDAR sensor does not provide object recognition information due to a failure in detecting the desired signal.	[TC-1] Sticking objects (water, ice, snow, mud, dust, car wash wax, insects, bird droppings) are adhered to the sensor surface.
			[TC-2] Cracks or distortions on the sensor surface alter the sensor characteristics.
CS-2	UCA-2	[IC-2] The LiDAR sensor provides incorrect object recognition information due to the point cloud data being perceived with an unexpected distribution.	[TC-3] Spatial obstacles (snow, rain, sand, fog, insects, etc.) are present in the same space.
			[TC-4] Interference with the LiDAR signal (direct wavelengths from other vehicles, infrastructure, natural environments) is present in the same space.

3.4 Identification of causal scenarios

STPA에서는 UCA를 유발시키는 원인으로 Causal factor라는 개념이 도입된다. 이는 SOTIF에서 말하는 Triggering condition과 동일한 개념이며, 본 논문에서는 Triggering Condition(TC)으로 통일하도록 한다. 도출된 UCA 중 대표적인 UCA로 UCA-1과 UCA-2를 정의하였으며, 이를 유발시키는 TC를 찾기 위해 기능 불충분(Insufficiency Condition, IC)한 것으로부터 도출해낸다. TC를 도출하기 위해서는 LiDAR센서의 외란 요소를 정의해야 할 필요가 있다. 또한 외란 요소로 인한 LiDAR 센서에 어떤 영향이 있는지 파악하여야 한다. 본 논문에서는 'ISO34502: Road Vehicles-Test scenarios for automated driving systems-Scenario based safety evaluation framework'를 참고하였다. 해당 표준 문서는 시스템의 의도된 기능에 영향을 미치는 Triggering condition 및 관련 위험을 식별하고 시스템이 불합리한 위험으로부터 보호될 수 있는지 여부를 평가하기 위해 엔지니어링 프레임워크 및 시나리오 기반 안전 평가 프로세스에 대해 설명한다.[15] 이를 통해 최종적으로 4가지 TC를 정의하였으며, 해당 TC에 따른 대표 Causal scenario를 도출하였다.

Causal scenario는 시스템이 특정한 위험 상태에 놓이게 하는 상황을 나타낸다. 각 시나리오는 대표 UCA를 기반으로 하며, 관련된 IC와 TC를 식별하여 도출된다. Table 5는 본 논문에서 정의한 대표적인 Causal scenario와 이에 따른 TC의 식별이다.

CS-1의 경우, UCA-1을 유발하는 IC-1는 LiDAR 센서가 원하는 신호를 감지하지 못하는 상황이다. 이는 센서 표면에 물, 얼음, 눈 등의 물질이 붙어 있거나 센서 표면에 균열 또는 왜곡이 발생하여 감지 성능이 저하되는 상황에서 발생할 수 있다.

CS-2의 경우, UCA-2를 유발하는 IC-2는 LiDAR 센서가 포인트 클라우드 데이터를 예상치 못한 분포로 인식하여 잘못된 객체 인식 정보를 제공하는 상황이다. 이는 공간 장애물이나 LiDAR 신호에 간섭이 발생하는 상황에서 나타날 수 있다.

식별된 위험 원인 시나리오를 기반으로 본 논문에서는 STPA 분석을 통해 LiDAR 기반 SCC 시스템의 안전성을 확보하고자 잠재적인 위험을 유발시키는 원인을 도출하였다. 이로 인한 위험을 최소화하기 위한 구체적인 안전 요구 사항을 도출하고, 이를 만족하는 위험 완화 전략을 수립하는 것을 목표로 한다.

4. 시뮬레이션 기반 V&V 환경 구축

본 논문의 목표는 위험원 분석 및 위험 평가를 통해 안전 요구 사항을 도출하고, 이를 충족시키기 위한 위험 완화 전략을 수립하는 것이다. SOTIF 관점에서의 위험 평가를 위해 V&V(Verification and Validation) 환경을 구축하였다. 평가 환경은 MIL(Model-in-the-Loop) 시뮬레이션을 기반으로 하며, 센서 데이터를 통한 인지, 판단, 제어의 순서로 이루어진다. ROS 기반의 검증 환경을 구축하였으며, 차량 시뮬레이션, MATLAB/SIMULINK, 그리고 인지 알고리즘으로 구성된 세 가지 루프 시스템을 구성하였다. 실험 환경에 대한 아키텍처를 Fig. 5에 나타내었다. 앞 절에서 STPA 안전 분석 기법을 통해 SOTIF 관점에서 위험을 유발하는 Triggering condition을 도출하였으며, 이를 바탕으로 위험 시나리오에 등속과 감속 상황의 주행 조건을 적용하여 V&V를 진행하였다. 또한, 외란이 유지되는 시간을 0초부터 3초까지 0.1초 간격으로 나누어 시나리오를 생성하였다. 외란이 주입되는 시점은 트래픽 이벤트가 발생한 순간이며, 등속 주행 시에는 전방 차량의 속도를 정확히 추종하는 순간에 주입하였다. 각 시나리오당 데이터 신뢰성을 확보하기 위해 동일한 조건에서 20회 반복 테스트를 진행하였다. 제어기는

상위 제어기인 Sliding Mode Control(SMC)와 피드백 기반 하위 제어기로 구성되어 있다. LiDAR 센서 인지 시스템은 Point Cloud Library(PCL) 알고리즘을 통해 종방향 전방 차량의 상대 거리를 추종한다.

실험은 다음과 같은 하드웨어 환경에서 진행되었다: CPU: Intel i7 11세대, GPU: NVIDIA GeForce RTX 3090, RAM: 32 GB.

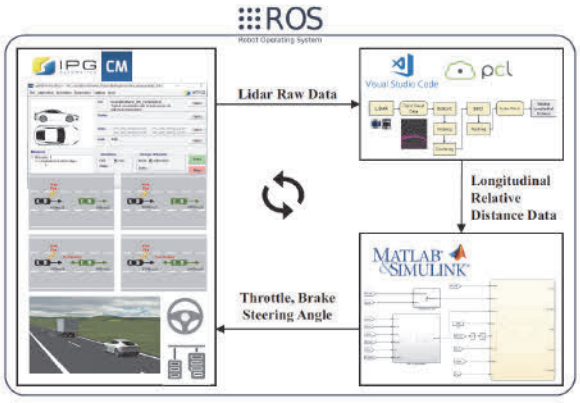


Fig. 5 Simulation Environment Architecture

4.1 SCC Model

LiDAR 기반의 종방향 제어기는 전방 차량 추종 및 목표 속도의 정속 주행, 자동 긴급 제동 기능을 능동적으로 수행하는 SCC 시스템과 같이 설계되어야 한다. SCC 시스템은 목표 가속도를 계산하는 상위 제어기와 계산된 목표 가속도를 추정하기 위해 Throttle과 Brake input을 계산하는 하위 제어기로 구성된다.[16] 상위 제어기는 LiDAR 센서를 통해 측정된 전방 차량과의 상대거리를 이용하여 목표 가속도를 계산한다. CarMaker 차량은 Gas/Brake 페달 입력을 통해 속도를 제어한다. 그렇기에 하위 제어기는 계산된 목표 가속도를 추종하도록 Engine throttle과 Brake pressure 값을 계산하여 차량의 속도를 제어한다. LiDAR 기반의 종방향 제어 알고리즘은 종방향 가속도를 생성하며, 주행 환경에 실시간으로 대응하기 위해서 제어 시스템의 계산 복잡도를 줄이는 것이 중요하다. 본 연구에서는 속도 유지 및 감속 상황만 고려하는 선형 종방향 제어 모델을 적용한다. SCC 제어 알고리즘으로는 Roh가 제안한 SMC 기반 상위 제어기와 PI 제어 기반 하위 제어기를 참고하여 구현하였다.[17] 본 연구의 목적은 SCC 기능의 제어 성능 개발이 아닌, SOTIF 관점에서 위험 상황 발생 이후 SCC 기능을 대체하는 Fail-Safe 전략, 즉 Minimum Risk Maneuver(MRM) 관점의 위험 대응 알고리즘을 개발하고 검증하는 데 있다. 따라서 SCC 로직에 대한 상세한 설명은 생략하도록 한다.

4.1.1 SMC 기반 상위 제어기

인지 센서를 통해 얻은 상대거리 값은 차량의 주행 중 외란이 발생하여 측정 데이터의 신뢰성이 저하되는 문제가 있다. 이를 해결하기 위해, 시스템의 비선형성과 차량 파라미터의 불확실성에도 차량 거동의 안정성을 확보할 수 있도록 강건 제어 기법 중 하나인 SMC 기반 상위 제어기를 SCC 로직에 적용하였다. SMC 제어는 차량 간의 추종 오차를 바탕으로 목표 가속도를 계산한다. 또한, 차량 동역학 모델을 기반으로 공기저항과 구름 저항 등을 고려한 식을 통해 자차의 가속도를 산출하며, 전방 차량과의 상대 거리, 속도, 그리고 Time gap을 고려하여 안전거리를 유지하도록 설계되었다.[17] 본 논문에서 제안하는 SMC 기반 상위 제어기의 출력은 자차의 목표 가속도이며, SCC 기능의 전방 차량을 추종하는 Follow mode (Stop & Go)에서 이를 출력하도록 설계되었다.

4.1.2 PI 기반 하위 제어기

상위 제어기에서 출력된 목표 가속도 값과 자차량의 가속도와의 오차는 PI 제어 기반 하위 제어기에 입력되어 Engine torque 및 Brake pressure값으로 변환되어 CarMaker 차량에 입력된다. PI 제어기는 Fig. 6과 같이 비례제어기와 적분 제어기로 구성된다.

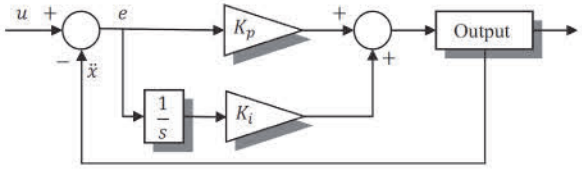


Fig. 6 Block diagram of PI feedback controller

비례제어기는 제어 입력 값과 현재 값의 오차에 비례하여 출력을 만들어 감소시킨다. 이 때 비례제어기만 사용한다면 정상상태 오차를 제거할 수 없다는 한계가 존재하여 정상상태 오차를 제거하기 위하여 적분 제어기를 추가하여 사용하였다. 적분 제어기는 제어기의 입력 값과 현재 값의 차이를 적분한 값을 오차로 설정하고 적분 계수에 비례하는 출력을 만든다. 제어기의 튜닝 파라미터 K_p와 K_i는 경험에 따라 시행착오를 통해 최적화된 값이다.

4.2 LiDAR 인지 알고리즘

본 논문에서는 PCL에서 제공하는 라이브러리를 활용하여 LiDAR 인지 알고리즘을 구축하였다. PCL은 2D/3D 이미지 및 포인트 클라우드 처리를 위한 오픈소스 소프트웨어로, 다양한 컴퓨터 비전 및 로보틱스 분야에서 널

리 사용된다.[18] 본 인지 알고리즘은 CarMaker 시뮬레이션에서 송신된 LiDAR RSI(Raw Signal Interface) 데이터를 바탕으로 전방 차량에 대한 종방향 상대 거리를 도출하기 위해 설계되었다.

Fig. 7은 앞서 설명한 LiDAR 인지 알고리즘 아키텍처이다. 시뮬레이션 환경에서 Traffic A의 정보가 Ego 차량의 좌・우측에 장착된 LiDAR 센서에 전달된다. 각각의 LiDAR 센서에서 측정한 Point Cloude Data(PCD)를 결합하여 PCL 알고리즘에 전달하게 된다. 이때, Ego 차량의 좌・우측에 부착된 LiDAR 센서로부터 측정된 PCD는 각각 (x_L, y_L, z_L)와 (x_R, y_R, z_R)로 표현한다. 두 데이터가 결합된 PCD는 (x_C, y_C, z_C)로 표현한다. 주요 포인트 클라우드 전처리 과정에서는 RANdom SAmple Consensus (RANSAC), Filtering, Clustering 알고리즘을 사용하였으며, 이 과정에서 PCL에서 제공하는 Voxel grid와 Pass through 필터링 기법을 활용하였다.

각 알고리즘과 전처리 과정에 대한 설명은 다음과 같다.

- RANSAC은 데이터셋에서 노이즈를 제거하고 모델을 예측하는 데 사용되는 알고리즘으로, 다양한 분야에서 활용된다. RANSAC은 특정 임계값을 초과하는 데이터를 무시함으로써 노이즈에 매우 강건한 특성을 지닌다. 이를 통해, LiDAR 데이터에서 신뢰할 수 있는 객체 모델을 추출할 수 있다.
- Filtering 단계에서는 Voxel grid 필터링을 사용하여 포인트 클라우드를 Down sampling한다. 이 과정은 데이터의 밀도를 줄여 처리 속도를 향상시키면서도 중요한 지형적 특징을 유지하도록 한다. 추가적으로, Pass through 필터를 사용하여 (x, y, z) 축 범위를 설정함으로써 해당 범위 내의 점들만 남기고 나머지 데이터를 제거한다. 이를 통해, 관심 영역 내의 데이터만을 처리하게 되어 효율성을 높일 수 있다.
- Clustering 과정에서는 유클리드 클러스터 추출 알고리즘을 사용하여 Down sampling된 PCD를 처리한다. 이 알고리즘은 지정된 임계값을 기준으로 인접한 포인트들을 그룹화하여 클러스터를 형성하며, 이러한 클러스터는 개별 객체를 나타내게 된다.

이를 통해 LiDAR 데이터에서 효과적으로 객체를 분리하고, 그 위치를 추정할 수 있다. 이 과정을 거친 후, 객체에 Bounding box가 생성이 되며 중심 좌표를 추출한다. 추출된 중심 좌표는 Euclidean distance 계산을 통해 최종적으로 전방 차량과의 상대 거리를 추출하게 된다.

PCL을 활용한 LiDAR 인지 알고리즘은 전방의 대상 차량의 종방향 상대거리를 추출하는데 특화되어 있어, 그 외의 상황에서는 한계점이 있다. 포인트 클라우드를 활용한 학습 기반 전방 차량 추종 모델을 사용하면 객체 검출 및 추적에 빠르고 효율적인 성능을 가지며, 다양한 시나리오에 대응할 수 있는 범용적인 객체 인식 모델을 구현할 수 있다. 하지만 본 논문의 주요 목표는 모델의 성능과는 별개로 SOTIF 프로세스를 통해 안전 요구 사항을 도출하고 안전 메커니즘 설계를 통한 개선 가이드라인을 제안하는 것이다. 따라서 본 논문에서는 학습 모델을 사용하는 대신 직관적이고 경량화 된 객체 인식 알고리즘을 설계하여 SOTIF 위험 분석 및 검증 환경에 적용하였다.

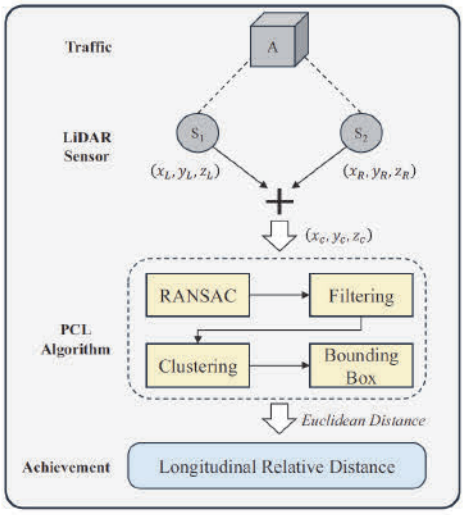


Fig. 7 LiDAR sensor recognition algorithm architecture

4.3 LiDAR 외란 모델

LiDAR 센서를 이용한 자율주행 시스템에서 현실과 유사한 가상환경을 구축하기 위해서는 다양한 외란 요소들을 고려해야 한다. 이러한 외란 요소는 SOTIF 관점에서 위험 시나리오를 평가할 때 중요한 역할을 한다. 외란 모델을 사용함으로써, 시뮬레이션 상에서 발생할 수 있는 다양한 환경적 요인들을 모방하고, 이에 대한 시스템의 반응을 평가할 수 있다. 이는 시스템의 신뢰성을 높이고, 실제 운용 환경에서의 안전성을 확보하는 데 필수적이다.

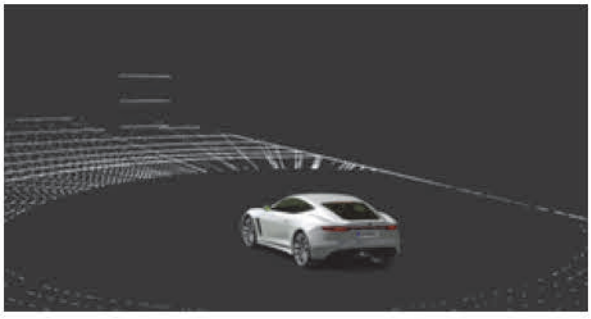
본 논문에서는 LiDAR 센서에 영향을 미치는 주요 외란 조건을 Table 5에서 도출한 4가지 Triggering Conditions으로 정의하였다. 외란 모델은 미인지와 오인지 개념으로 구성되며, 각 외란 조건은 LiDAR 센서를 통해 얻어지는 PCD에 noise를 추가하는 방식으로 실제 외란 현상을 재현하였다.

먼저 TC-1, TC-2에 의해 LiDAR 센서가 미인지 하도록 모방하는 외란 모델을 구현하기 위해 Random dropout 방법을 적용하였다. Random dropout 방법은 PCD 중에서

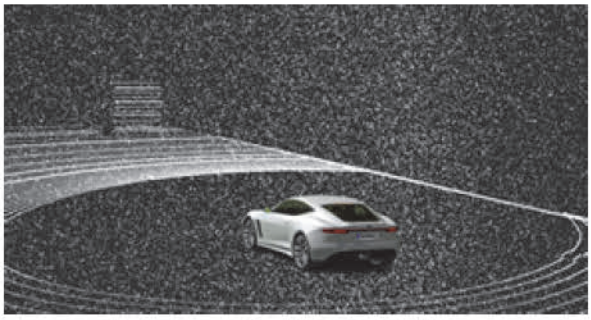
(a) CarMaker image

(b) Point cloud data

Fig. 8 CarMaker LiDAR sensor



(a) Random dropout - False Negative



(b) Gaussian noise - False Positive

Fig. 9 LiDAR sensor disturbance model

임의로 일정 비율의 포인트를 삭제하도록 알고리즘을 구현하였으며, 이는 특정 환경에서의 데이터 손실이나 부분적인 센서 장애를 시뮬레이션 상에서 모방할 수 있게 된다.[19]

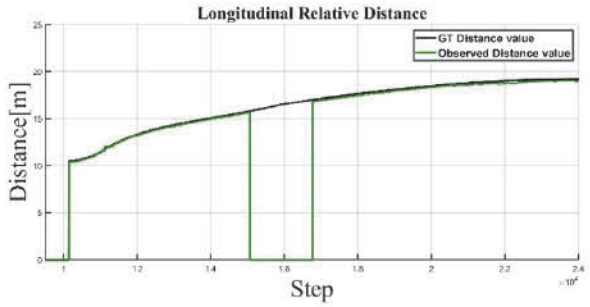
다음으로 TC-3, TC-4에 의해 LiDAR 센서가 오인지 하도록 모방하는 외란 모델을 구현하기 위해 Gaussian noise를 적용하였다. 본 연구에 활용된 Gaussian noise 적용 방법은 PCD가 (x, y, z) 값에 대해 평균이 0이고 표준편차가 특정 값인 Gaussian 분포를 따르는 노이즈를 추가한다. 이 방법은 노이즈가 분포적으로 중립적이며, 이는 센서의 간헐적 False-Positive 현상을 시뮬레이션상에서 모방할 수 있게 된다. 이렇게 PCD에 외란 모델을 적용하여 실제 환경에서 발생할 수 있는 Triggering Condition을 CarMaker 시뮬레이션에서 재현하도록 설계하였다.[19]

Fig. 8(a)는 차량 시뮬레이션인 CarMaker에서 시각화할 수 있는 IPG Movie 기능으로 확인한 주행 상황이다. 주행 상황은 전방 Traffic 차량과 Ego 차량으로 구성되어 있으며, Ego 차량에는 LiDAR 센서가 부착되어 있다. Fig. 8(b)는 Ego 차량의 LiDAR 센서 Point Cloud Data를 Rviz(ROS Visualization Tool)를 통해 시각화한 것이다. Ego 차량을 기준으로 전방 Traffic과 주변 환경을 점들로 표현한 것을 볼 수 있으며, 각 점은 LiDAR 센서가 감지한 물체의 표면을 나타낸다.

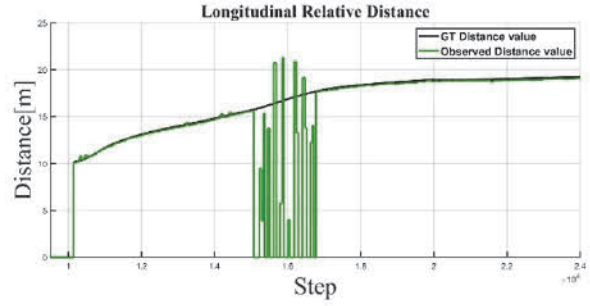
Fig. 9는 앞서 설명한 외란 모델이 적용된 PCD이며, Fig. 9(a)는 Random dropout을 이용한 미인지 현상, Fig. 9(b)는 Gaussian noise를 사용한 오인지 현상을 재현한 Rviz 이미지이다.

외란 모델을 구현할 때, 노이즈의 강도나 빈도와 같은 파라미터 설정은 매우 중요한 요소이다. 이러한 파라미터들은 시스템이 다양한 상황에서 어떻게 반응하는지를 관찰하고, 여러 번의 실험과 시행착오를 통해 최적의 값을 찾아내는 과정에서 결정되었다. 실제 실험을 반복적으로 진행하면서 노이즈 파라미터를 조정한 결과이며, 이는 외란 모델의 신뢰성과 정확성을 높이기 위한 필수적인 단계이다.

Fig. 10은 앞서 설명한 외란 모델을 적용하여 종방향 상대거리 결과값을 측정한 그림이다. 외란 주입 시점과 종료 시점을 동일한 시나리오에 적용하였으며, Fig. 10(a)는 미인지, Fig. 10(b)는 오인지 외란 모델을 적용하여 측정한 종방향 상대거리 값이다. 검정색 그래프는 시뮬레이션에서 차량 간의 거리를 계산한 Ground truth 값이며, 초록색 그래프는 시뮬레이션에서 LiDAR 센서를 통한 측정값이다. Fig. 10(a) 미인지 외란 모델을 적용한 그래프를 보면 외란이 주입된 시점에 전방 차량을 인식하지 못하여 종방향 상대거리 값이 측정되지 않아 0값으로 나



(a) False negative



(b) False positive

Fig. 10 LiDAR sensor disturbance model

타낸 것을 확인할 수 있다. Fig. 10(b) 오인지 외란 모델을 적용한 그래프를 보면 외란이 주입된 시점에 전방 차량을 간헐적으로 측정하지 못하며, 실제 상대거리 값이 아닌, 0값 혹은 다른 값이 측정되는 것을 확인할 수 있다. 그래프의 x축은 시뮬레이션에서 처리되는 스텝 횟수이고 y축은 거리이다.

5. Verification & Validation

본 절에서는 STPA 안전분석기법을 통해 도출한 SOTIF 관점의 위험 시나리오를 구축한 검증 환경에서 위험 평가를 진행한다. 60 km/h와 100 km/h에서 자차량 주행 중 전방 차량 등속/감속 주행 상황에서 SCC 시스템에 성능 한계 상황을 고려하여 시나리오를 구체화하였다. 시나리오는 전방 차량이 60 km/h로 등속 주행 상황(60 km/h Constant Speed Driving, 60CD)과 60 Km/h로 감속 주행 상황(60 km/h Deceleration Driving, 60DD)로 정의하였으며, 속도 조건을 100 Km/h(100CD, 100DD)를 추가하여 총 4가지 Driving condition으로 정의하였다. 앞서 정의한 두 가지 외란이 유지되는 시간을 K_n로 정의하고 n은 0초부터 3초까지 0.1초 간격으로 시나리오를 생성하였다. 각 시나리오 당 데이터 신뢰성 확보를 위해 동일한 조건에서 K_n을 I 번 총 20회 반복 테스트를 진행하였다. 시나리오 생성에 대한 위 내용을 Fig. 11에 아키텍처로 나타내었다.

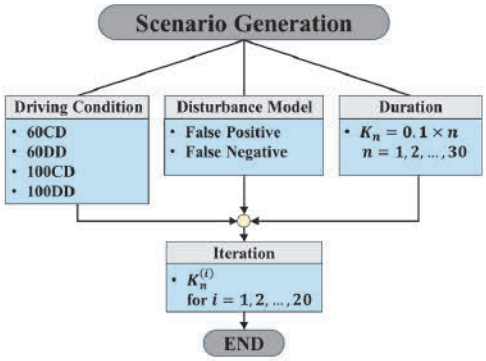


Fig. 11 Scenario generation architecture

외란이 유지되는 시간동안 불합리한 위험을 피하기 위한 안전 요구 사항을 정의하고, 이를 만족하는 안전 메커니즘을 설계하는 것을 목표로 한다. 유효충돌속도와 TTC(Time to Collision)를 기준으로 SOTIF 관점의 위험 분석을 진행한다. 안전 메커니즘이 활성화되지 않을 때, 시스템에서 결함이 발생부터 위험 사건의 가능한 발생까지 최소 시간을 결함 허용 시간 간격(Fault Tolerant Time Interval, FTTI)를 도입하여, 안전 요구 사항을 정의한다. 0초부터 3초까지 외란 지속 시간을 조절하여 시스템 수준에서 위험 시점의 FTTI를 도출한다. 도출된 FTTI 내에 제어권이 전환되어야 한다는 안전 목표를 중점으로 결함 대응 시간을 정의하며, 이를 지키는 안전 메커니즘 설계하는 과정을 보여준다. 이후, 안전 메커니즘이 적용된 자율주행 시스템을 통해 위험이 완화되는 것을 마지막으로 프로세스를 종료한다.

5.1 SOTIF HARA

SOTIF HARA(Hazard Analysis and Risk Assessment)는 차량 시스템의 의도된 기능이 가져올 수 있는 위험을 식별하고 평가하는 과정이다. 이 과정은 ISO 26262-Part.3의 HARA와 밀접하게 연관되어 있으며, 두 절차는 상호보완적으로 작동한다. 기능안전의 HARA는 시스템의 오작동으로 인해 발생하는 위험을 식별하고 평가하는 반면, SOTIF HARA는 시스템이 의도된 대로 작동할 때 발생할 수 있는 잠재적인 위험을 추가적으로 고려한다. 또한 ISO 26262 문서에서는 HARA 프로세스를 통해서 ASIL(Automotive Safety Integrity Level) 등급이 결정되면, 그에 따른 안전 목표가 정의가 된다. 하지만, SOTIF 관점에서는 ASIL 등급을 결정하지 않으며, Severity와 Controllability가 0보다 큰지 여부를 평가한다.[20] 본 논문에서는 Severity와 Controllability를 0으로 만드는 전략을 수립하였으며, 위험 평가를 위해 유효 충돌 속도와 TTC를 검증 지표로 사용하였다.

5.1.1 Severity 도출

SOTIF 관점에서 Severity는 특정 위험이 발생했을 때 운전자나 차량에 미치는 잠재적 결과나 영향을 평가하는 중요한 요소이다. 이 절에서는 SAE J2980 문서를 참고하여 유효 충돌 속도를 사용해 Severity를 산정하는 방법을 설명한다. SAE J2980 문서는 차량 모션 제어 시스템의 우선순위를 설정하고, 차량 수준에서 발생할 수 있는 위험 이벤트를 식별하고 분류하는 지침을 제공한다.[21] 이 문서는 ISO 26262- Part.3의 요구사항에 맞추어 HARA 프로세스를 설계하였으며, ASIL 등급을 도출하기 위해 Severity, Exposure, Controllability(S, E, C) 레벨을 근거로 평가하는 방법을 제시한다.

본 논문에서는 J2980 문서에서 제시하는 방법론 중 하나인 유효 충돌 속도를 활용하여 Severity를 산정한다. 이 방법론을 통해 특정 위험 상황에서 발생할 수 있는 충돌의 강도와 그로 인해 예상되는 잠재적 영향을 정량적으로 평가하는 방법을 제시한다.

5.1.1.1 유효 충돌 속도

유효 충돌 속도는 차량 간의 사고가 발생했을 때 추돌 차량의 속도 변화를 의미한다. 이는 충돌 상황에서 나타나는 상대 속도를 두 차량의 질량에 비례하여 분배한 값으로, 차량의 주행 속도와 질량에 따라 변화한다. 질량이 m_x, 충돌개시속도가 V_x인 차량 X가 질량이 m_y, 충돌개시속도가 V_y인 차량 Y와 충돌할 경우 운동량의 교환이 이루어지고 공통속도 V_C를 목적으로 속도가 변화하는 관계식은 (1)과 같다. 각 차량 X, Y의 유효 충돌 속도는유효 충돌 속도(V_{xe}, V_{ye})를 표현한 관계식은 (2), (3)과 같다.[22]

$$V_c = \frac{m_x V_x + m_y V_y}{m_x + m_y} \tag{1}$$

$$V_{xe} = V_x - V_c = \frac{m_y}{m_x + m_y}\left(V_x - V_y\right) \tag{2}$$

$$V_{ye} = V_c - V_y = \frac{m_x}{m_x + m_y}\left(V_x - V_y\right) \tag{3}$$

여기서, V_{xe}: 차량 X의 유효충돌속도 (km/h)
V_{ye} : 차량 Y의 유효충돌속도 (km/h)
V_x : 차량 X의 충돌개시속도 (km/h)
V_y : 차량 Y의 충돌개시속도 (km/h)
V_C : 충돌 후 양차의 속도 (km/h)
$V_x - V_y$: 차량 X, Y의 상대 속도 (km/h)
m_x : 차량 X의 질량 (kg)
m_y : 차량 Y의 질량 (kg)

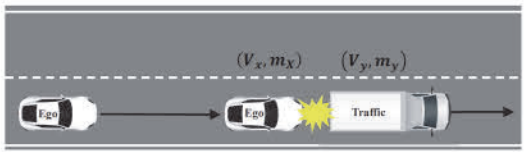


Fig. 12 Severity assessment using effective collision speed

Fig. 12는 유효 충돌 속도를 이해하기 위한 그림이며, 앞서 정리된 수식을 통해 유효 충돌 속도를 정의하여 Severity를 측정할 수 있다. Severity 관점에서 위험 시나리오를 정의하기 위해, 자율 주행 시스템에 충돌 가능성과 충돌 발생 시 상해 위험도가 존재하는지 4가지 Driving condition에 대해 평가를 진행하였다. 실험 결과 현재 Driving condition에 따른 4가지 위험 시나리오를 정의하였으며, 이 시나리오들은 모두 S가 0보다 큰 상황으로 평가되었다. Table 6은 이러한 Severity 관점에서의 위험 시나리오를 Triggering condition과 매칭하여 정리한 것이며, 이렇게 정의된 위험 시나리오는 Controllability 관점에서 추가적인 위험 시나리오를 도출하는 데 사용된다.

Table 6 Risk Assessment Analysis Severity

Causal scenario	Driving condition	Severity
CS-1 [TC-1][TC-2]	60CD	>S0
	60DD	>S0
	100CD	>S0
	100DD	>S0
CS-2 [TC-3][TC-4]	60CD	>S0
	60DD	>S0
	100CD	>S0
	100DD	>S0

5.1.2 Controllability 도출

SOTIF HARA에서의 Controllability는 특정 위험 상황에서 운전자가 차량을 제어할 수 있는 능력을 평가하는 요소이다. 이는 위험 상황 발생 시 운전자가 적절히 대응하여 사고를 방지하거나 그 영향을 최소화할 수 있는지 여부를 판단하는 데 중요하다. 본 절에서는 ISO 26262-Part.1에서 말하는 FTTI와 제어권 전환 시간을 참고하여 Controllability를 산정하는 방법을 설명한다.

5.1.2.1 FTTI 정의

ISO 26262에서 정의된 FTTI 개념은 시스템에서 결함의 발생부터 위험이 발생하기까지의 시간 간격을 의미하며, 시스템의 오동작 행위로 인해 발생할 수 있는 위험원과 관련이 있다. 그러나 본 논문에서는 SOTIF HARA 과정에 FTTI 개념을 확장하여 적용하고자 한다. 시스템의 성능 한계로 인해 발생할 수 있는 위험원에 대해 위험 발생 간격을 도출하기 위해 FTTI를 활용하며, 외란이 지속되는 시간 간격을 통해 TTC가 임계값 이상 측정이 되면 C>0으로 정의한다. Fig. 13은 SOTIF에 적용된 FTTI의 그림이다.

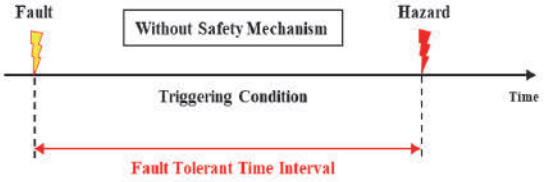
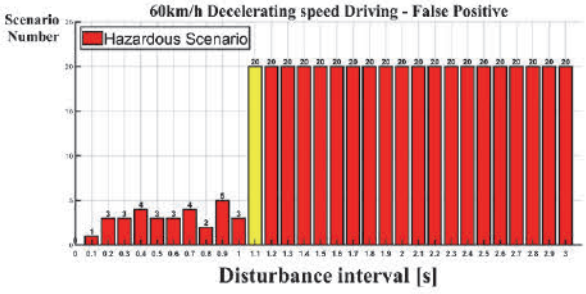
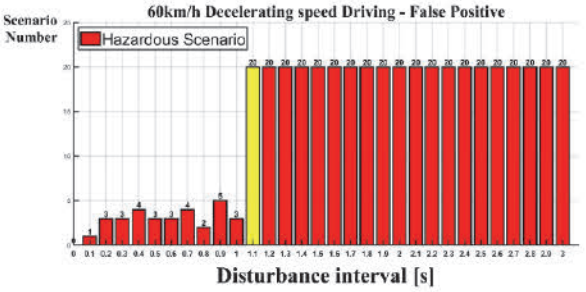


Fig. 13 FTTI as defined in ISO 26262

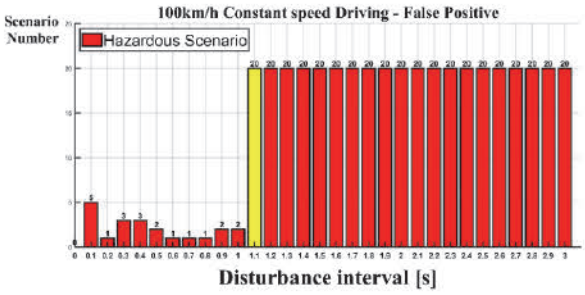
외란 모델이 적용된 Driving condition에 대해 위험 시나리오가 발생하는 최소 성능한계 발생 간격(Disturbance interval)을 FTTI로 도출한다. Fig. 14와 Fig. 15의 그래프의 X축은 외란 주입 시간이며, Y축은 위험 시나리오 개수다. 위험 시나리오가 급증하는 순간을 노란색 막대 그래프로 표현하였으며, 그 순간의 Disturbance interval이 FTTI이다.



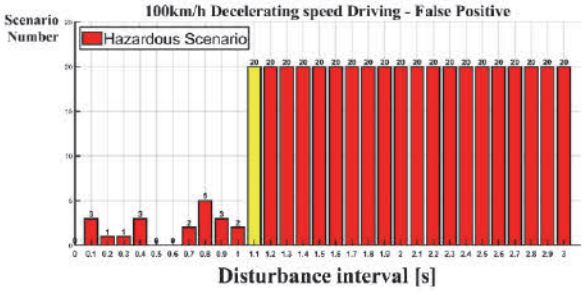
(a)



(b)



(c)

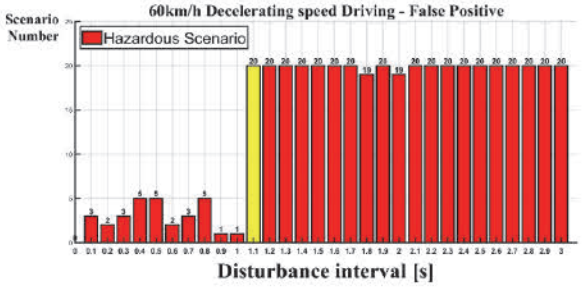


(d)

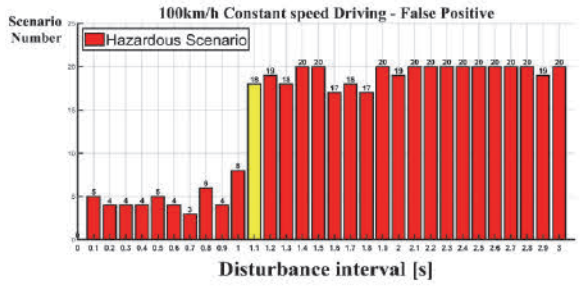
Fig. 14 Results of FTTI by false negative

Fig. 14는 미인지 외란을 주입하였을 때, 시나리오 별 FTTI 도출한 결과이다. 위험 시나리오가 급증한 외란 주입 시간은 노란색 막대가 그래프로 표현된 것으로 4가지 Driving condition의 위험 시나리오 모두 FTTI는 1초로 도출되었다. 같은 방식으로 Fig. 15는 오인지 외란을 주입하였을 때를 나타내며, 이때 FTTI도 1초로 도출되었다.

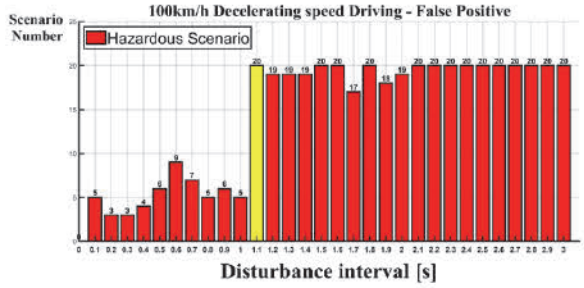
(a)



(b)



(c)



(d)

Fig. 15 Results of FTTI by false positive

따라서 8가지 위험 시나리오의 FTTI는 전부 1초로 산정되었다.

5.1.2.2 제어권 전환 시간 정의

제어권 전환 시간(Take over time)은 자율주행 시스템에서 차량의 제어권이 자동 모드에서 운전자로 전환되는 데 걸리는 시간을 의미한다. 이 시간은 자율주행 시스템의 안전성과 신뢰성을 평가하는 중요한 요소로 작용하며, 특히 Level 3 이상의 자율주행 차량에서 매우 중요하다. 제어권 전환 시간은 시스템의 결함 발생 시점부터 제어권 전환 요청 시간, 그리고 운전자의 인지 및 반응 시간에 따라 결정된다. 따라서, 이 시간을 정의할 때 앞서 도출한 FTTI를 기준으로 고려한다. Fig. 16은 자율주행 모드에서 제어권 전환 과정의 단계를 보여준다. 먼저, 차량은 자율주행 모드로 운행 중일 때, 결함이 발생하면, 시스템이 이를 인지하는 데 일정 시간이 소요된다. 이후

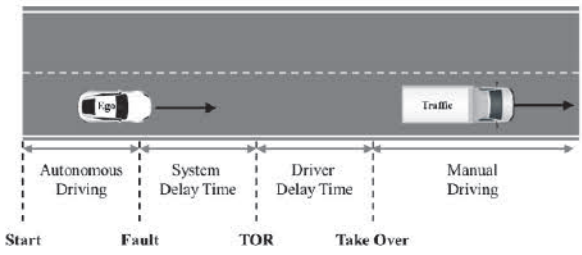


Fig. 16 Take over process in Level 3 AVs

시스템은 운전자에게 제어권 전환 요청을 발행해야 하는데, 이 요청을 운전자가 인지하는 지연 시간이 발생하며, 운전자가 요청을 인지한 후, 제어권을 수동으로 전환한다. 마지막으로, 운전자가 차량의 제어권을 완전히 인수하여 수동 주행 모드로 전환된다.

Jang 등[23]은 운전자의 인지 반응 시간을 정의하면서, 이를 운전자가 상황을 인지하는 시간, 발이 브레이크 페달까지 이동하는 시간, 그리고 브레이크 페달을 밟기 시작해 실제 제동력이 발휘되기까지의 시간을 고려하여 산정하였다. 또한, 현재 한국 도로 설계에 사용되는 인지 반응 시간인 2.5초가 비용-효율 측면에서 재검토될 필요가 있으며, 실제로는 속도에 따라 더 짧은 인지 반응 시간이 타당하다고 주장하였다. 예를 들어, 60 km/h 이하에서는 2초, 80 km/h에서는 1.8초, 100 km/h에서는 1.6초, 그리고 120 km/h 이상에서는 1.4초가 적절하다고 제안하였다.

본 논문에서는 이 연구를 참고하여 보수적인 관점에서 운전자 인지 반응 지연 시간을 정의하였다. 60 km/h에서는 2초, 100 km/h에서는 1.7초로 설정하여, 실제 도로 상황에서의 안전성을 높이는 데 중점을 두었다. 이러한 설정은 다양한 주행 속도에서 운전자의 반응 시간이 중요한 영향을 미친다는 점을 반영한 것이다.

5.1.2.3 안전 요구 사항 도출

FTTI와 제어권 전환 시간, 그리고 운전자 인지 반응 지연 시간을 정의하였으며, 이를 바탕으로 제어권 전환 가능 여부(Take over possibility)를 평가한다. 본 논문에서는 제어권 전환이 이루어지기 위한 최소 시간을 산정하기 위해 다음과 같은 수식을 도출하였다. 제어권 전환 시간은 FTTI보다 앞서 이루어져야 하므로, 이를 기반으로 식 (4)를 도출하였다. 제어권 전환 시간은 제어권 전환 요청 시간과 운전자 인지 반응 지연 시간을 합산한 값으로 정의하며, 이는 식 (5)로 표현된다. 이때, 최소 제어권 전환 시간은 FTTI로 정의되며, 이는 식 (6)에서 제시된다. 최종적으로, 제어권 전환 요청 시간은 식 (7)을 통해 도출되었다.

$$FTTI \geq TOT \tag{4}$$

$$TOT = TOR + T_{Delay} \tag{5}$$

$$\min TOT = FTTI \tag{6}$$

$$\min TOR = FTTI - T_{Delay} \tag{7}$$

Table 7 Identify take over possibility

Causal scenario	Driving condition	FTTI [s]	Time delay [s]	TOR [s]	TOP
CS-1 [TC-1][TC-2]	60CD	1	2	-1	X
	60DD	1	2	-1	X
	100CD	1	1.7	-0.7	X
	100DD	1	1.7	-0.7	X
CS-2 [TC-3][TC-4]	60CD	1	2	-1	X
	60DD	1	2	-1	X
	100CD	1	1.7	-0.7	X
	100DD	1	1.7	-0.7	X

따라서 Table 7에서 도출된 FTTI와 정의한 Time delay를 바탕으로 TOR을 정의하였으며, 제어권 전환 요청 시간이 너무 짧거나 0 또는 음수인 경우에는 제어권 전환이 불가능하다는 결론을 내렸다. 본 논문에서는, 정의된 FTTI 내에서 제어권 전환이 이루어지도록 하기 위해 결함 대응 시간(Fail Operation Time)을 사용한다. 따라서, FTTI 내에서 제어권 전환이 불가능할 경우, FOT를 통해 이를 해결하는 것을 목표로 한다. 이 과정은 식 (8)로 표현할 수 있다.

$$FTTI + FOT \geq TOT \tag{8}$$

정의한 수식에 의해 제어권 전환이 불가능 할 때의 FOT는 TOR로 정의할 수 있다. 즉, 시스템의 안전 요구사항으로 제어권 전환이 가능하도록 FOT를 만족해야 한다는 것을 도출하였다. Fig. 17은 앞서 정의한 방법론에 따라 Controllability를 산정하기 위해 정의된 FTTI와 TOR, FOT에 대해 정리한 그림이며, y축은 Driver's readiness으로 운전자의 주의력을 의미한다.

이를 통해 제어권 전환이 FTTI 내에 이루어질 수 없다고 판단되어, 4가지 위험 시나리오 모두에서 C>0 상황으로 평가되었으며 Table 8에 정리하였다.

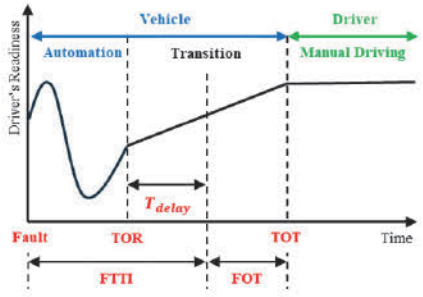


Fig. 17 FTTI, TOR, and FOT for Controllability Assessment

Table 8 Risk Assessment Analysis Controllability

Causal scenario	Driving condition	Controllability
CS-1 [TC-1][TC-2]	60CD	>C0
	60DD	>C0
	100CD	>C0
	100DD	>C0
CS-2 [TC-3][TC-4]	60CD	>C0
	60DD	>C0
	100CD	>C0
	100DD	>C0

5.2 안전 메커니즘 설계

앞선 절에서는 안전 요구 사항을 FOT로 정의하였다. 이를 만족시키기 위해 위험 상황을 극복할 수 있는 대응 기술 개발이 필요하다. 안전 메커니즘은 ISO 26262 표준에서 매우 중요한 개념 중 하나이다. 안전 메커니즘은 시스템에 결함이 발생할 경우 이를 감지하고, 시스템이 안전한 상태로 유지되도록 하는 일련의 절차와 방법을 의미한다. Fig. 18은 ISO 26262에서 정의하는 안전 메커니즘이 적용되었을 때의 안전 관련 시간 간격을 나타내며, Fault Detection Time Interval(FDTI), Fault Reaction Time Interval(FRTI), Fault Handling Time Interval(FHTI)라는 개념이 사용된다. FDTI는 결함 검출 시간 간격으로, 결함의 발생부터 검출까지의 시간 간격을 의미한다. FRTI는 결함 반응 시간 간격으로 결함 검출부터 안전 상태에 도달하기까지의 시간을 의미하며, FHTI는 FDTI와 FRTI의 합으로 정의된 FTTI보다 적어도 같거나 작아야 한다.[24]

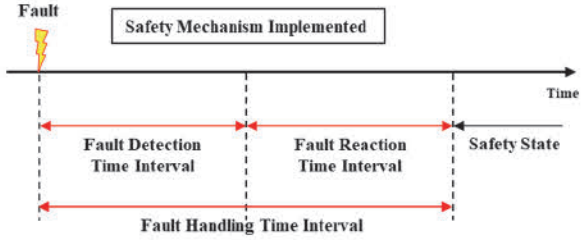


Fig. 18 FDTI, FRTI, FHTI as defined in ISO 26262

해당 개념들을 도입해 본 논문에서는 시스템의 결함을 찾기 위한 방법론으로 신호 처리 기반의 이상 감지 알고리즘을 사용한다. 이후 결함에 대응하기 위해 속도 단계별 감속 제어 시스템을 적용하여 Fail-Safe 전략을 통해 위험 상황을 극복하고자 한다.

5.2.1 Anomaly Detection Algorithm

본 절에서는 자율주행 시스템에서 외란을 감지하기 위해 사용된 Anomaly detection algorithm에 대해 설명한다. 시스템은 실시간으로 차량의 상대 거리 데이터를 분석하여 수신된 데이터 간의 변화율을 계산한다. 변화율은 현재 데이터와 이전 데이터 간의 차이를 통해 산출되며, 계산된 변화율이 설정된 임계 값을 초과할 경우, 시스템은 이를 즉시 이상 상태로 간주하지 않고 일정 기간 동안 모니터링을 진행한다. 이 기간 동안 지속적으로 임계 값 이상의 변화율이 감지될 경우, 시스템은 이를 이상 상태로 판단하여 Flag를 전송한다. 반대로, 이상 상태가 감지된 후 변화율이 임계 값 이하로 떨어지면, 시스템은 이를 이상 상태가 해제된 것으로 간주하지만, 이 경우에도 즉시 해제를 수행하지 않고 일정 기간 동안 추가 모니터링을 진행한다. 이 모니터링 기간 동안 임계 값 이하의 변화율이 지속적으로 감지되면, 시스템은 이상 상태를 해제하고 정상 상태로 전환되었음을 알린다. Anomaly detection algorithm은 Python으로 구현하였으며, 검증환경에 따라 입출력은 ROS message로 정의된 토픽을 송·수신한다. Fig. 19는 이상 감지 알고리즘을 Flow chart로 시각화한 것으로, 입력 값과 임계 값 파라미터가 함께 포함되어 있다. 임계 값은 반복적인 실험을 통해 최적화된 값으로 설정되었으며, 사용자의 특정 요구 사항에 맞게 조정될 수 있다.

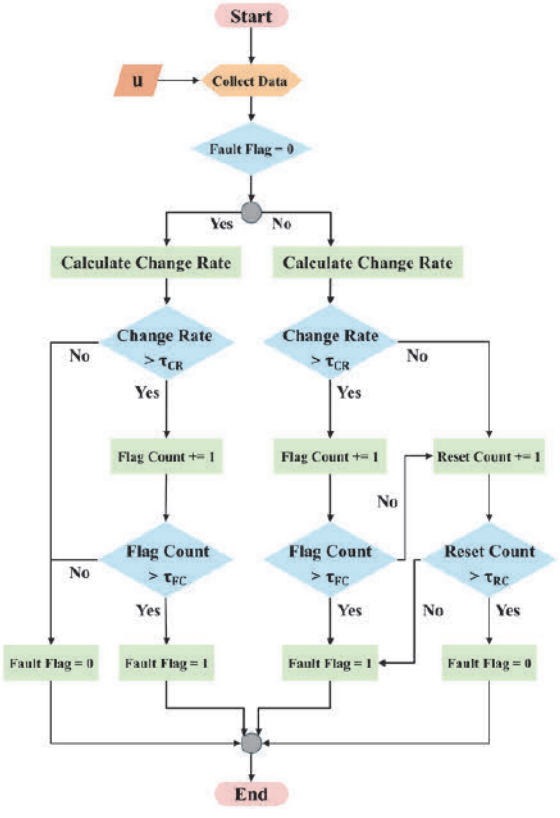


Fig. 19 Flow chart of anomaly detection algorithm

- u : Relative Distance Data
- τ_{CR}: Change Rate Threshold
- τ_{FC}: Flag Count Threshold
- τ_{RC}: Reset Count Threshold

5.2.2 Risk Mitigation Algorithm

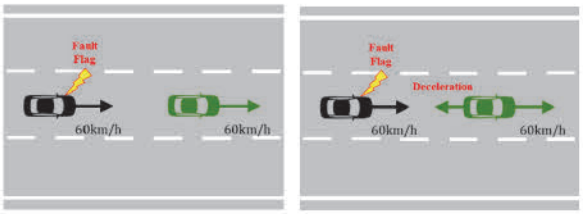
본 절에서는 앞서 이상 감지 알고리즘을 통해 시스템이 외란임을 판단한 경우, Flag가 1일 때 위험 대응 알고리즘이 활성화되어 시스템의 안전 요구 사항을 만족하는 과정을 설명한다. 기존의 안전 메커니즘이 적용되지 않은 상태에서는 제어권 전환이 불가능했던 동일한 위험 시나리오를 대상으로, Fail-Safe 전략을 통해 FOT 안전 요구 사항을 충족시켜 제어권 전환이 가능해지는 것을 목표로 한다.

본 논문에서는 Fail-Safe 전략으로 Minimum Risk Maneuver(MRM) 관점의 위험 대응 알고리즘을 설계한다. Fail-Safe란 하나의 결함이 발생한 뒤, 시스템을 외부 동력원 없이 안전 상태에 머물게 하거나, 외부 동력원을 통해 시스템을 안전 상태로 유지함으로써 결함으로부터 시스템을 보호하는 전략이다.

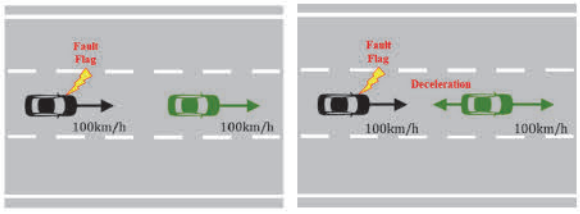
본 논문에서는 전방 차량을 추종하며 주행하는 종방향 SCC 자율주행 시스템을 분석 대상으로 선정하였다. 제어기 관점에서 정확한 객체 상대거리 정보를 알지 못하는 상황에서 잘못된 입력 값을 이용한 제어는 사고로 이어질 가능성이 매우 크다. 본 시스템은 LiDAR 센서만을 이용한 제어 시스템으로 설계되었기 때문에, 현재 시스템의 작동을 유지하면서 결함으로부터 시스템을 보호하는 것은 불가능하다. 이 제어 시스템에서 발생할 수 있는 주요 위험으로는 전방 차량과의 충돌이 있으며, 이는 충분한 안전거리를 유지함으로써 회피할 수 있다고 판단하였다.

현재 주행 조건에서 전방에 단일 차량만 존재하지만, SCC 시스템의 특성상 전방 차량이 급감속할 경우 운전자에게 불편함을 초래할 뿐만 아니라, 후방 차량과의 충돌 위험도 증가할 수 있다. 따라서 시스템이 외란임을 감지한 시점부터 전방 차량과의 충돌이 발생하지 않는 범위 내에서 일정 시간 동안 차량의 현재 속도를 기반으로 단계별 감속을 수행할 수 있는 제어 시스템을 제안한다.

Fig. 20은 4가지 Driving condition에 대한 그림이며, Fig. 21(a)는 100DD에 미인지 외란을 주입한 시나리오를 대상으로 안전 메커니즘이 적용된 상황에서 외란 검출

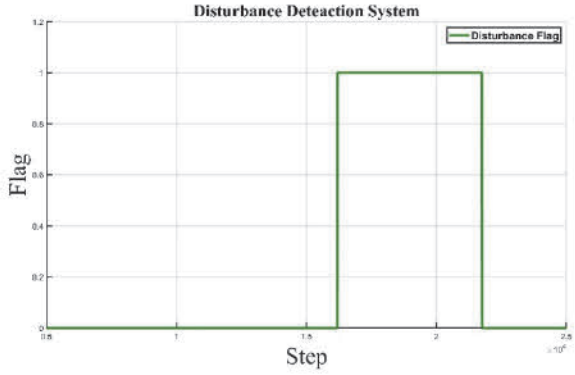


(a) 60CD (b) 60DD

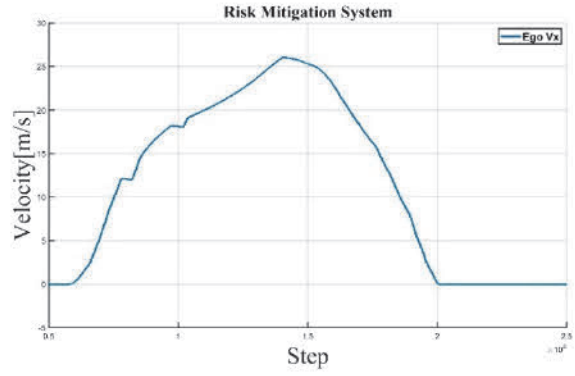


(c) 100CD (d) 100DD

Fig. 20 Driving Condition 4-Case Scenario



(a) Disturbance detection system

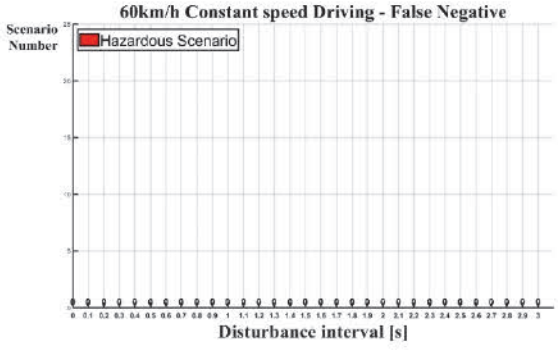


(b) Risk mitigation system

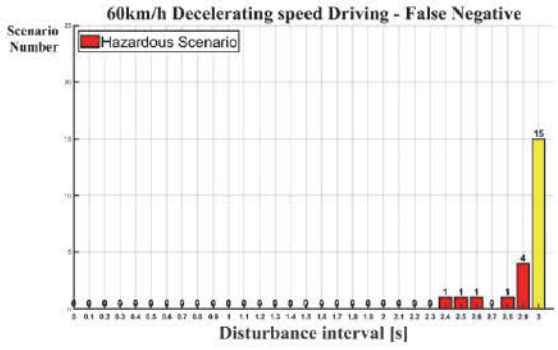
Fig. 21 Safety mechanism assessment

알고리즘을 통해 검출된 결과이며, Fig. 21(b)는 위험 대응 알고리즘을 통한 감속 제어가 자차량의 속도에 미친 영향을 시각적으로 보여준다. 자차량의 속도가 거의 100 km/h에 도달하는 순간 외란이 발생하였고, 이에 따라 안전거리를 유지하기 위해 강한 감속이 이루어지고 있음을 확인할 수 있다.

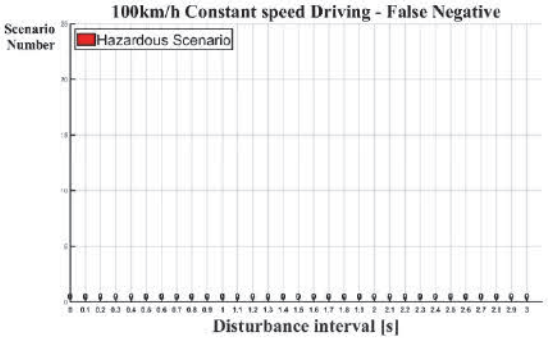
이와 같은 안전 메커니즘을 설계함으로써, 시스템이 안전 요구 사항을 충족하는지 확인하기 위해 8개의 위험 시나리오를 대상으로 재평가를 수행하고, 새로운 FTTI를 도출하였다. 실험은 동일한 조건으로 진행되며, Fig. 22와 Fig. 23에서 실험 결과를 확인할 수 있다.



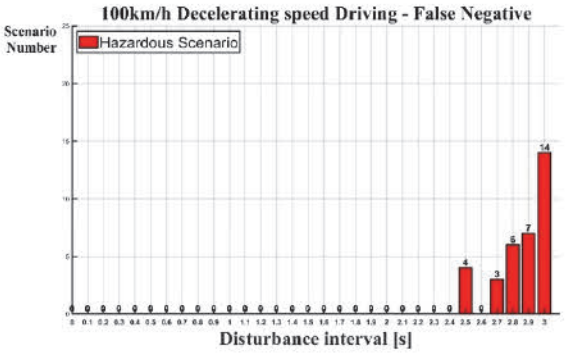
(a)



(b)

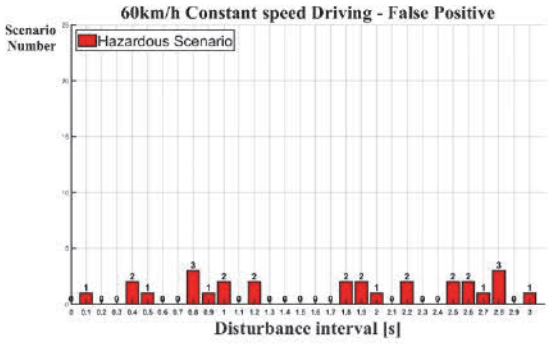


(c)

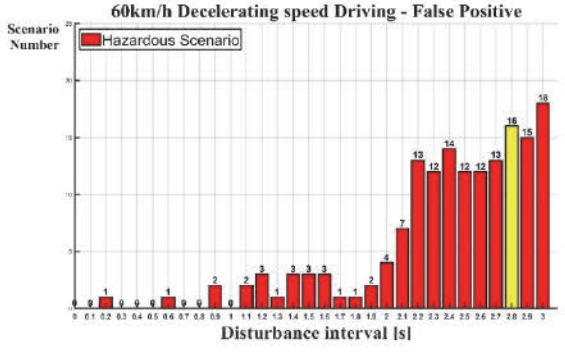


(d)

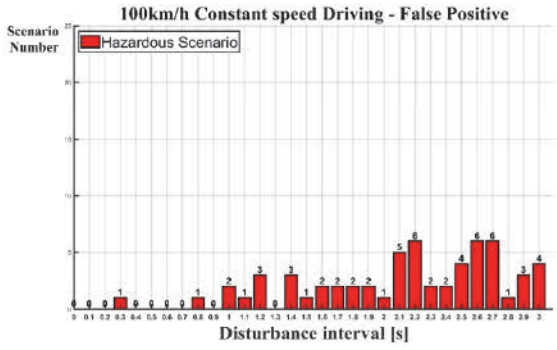
Fig. 22 Results of FTTI by False Negative with Safety Mechanism



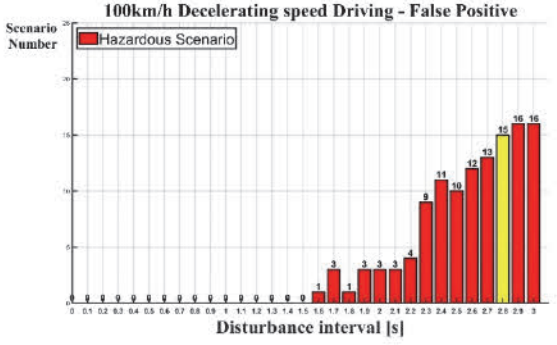
(a)



(b)



(c)



(d)

Fig. 23 Results of FTTI by False Positive with Safety Mechanism

Table 9의 실험 결과를 보면, 미인지 외란이 주입되었을 때, 안전 메커니즘이 작동한 시스템의 FTTI는 60 km/h에서 감속 주행 시 2.1초, 100 km/h에서 감속 주행 시 2.2초로 측정되었다. 본 연구에서는 위험 시나리오가 발생하지 않은 상황에서 FTTI를 3초로 설정하였다. 따라서, 나머지 두 시나리오에서의 FTTI는 3초로 측정되었다.

오인지 외란의 경우, 60 km/h에서 감속 주행 시 FTTI는 2.9초, 100 km/h에서 감속 주행 시 FTTI는 2.9초로 측정되었으며, 위험 시나리오가 나타나지 않은 60 km/h 및 100 km/h의 등속 주행 시 FTTI는 3초로 측정되었다. 이러

Table 9 Evaluation of the achievement of the SOTIF

Causal scenario	Driving condition	FTTI [s]	Time Delay [s]	TOR [s]	TOP	Severity	Controllability
CS-1 [TC-1][TC-2]	60CD	3	1.7	1.3	O	S=0	C=0
	60DD	2.1	1.7	0.4	O	S=0	C=0
	100CD	3	2	1	O	S=0	C=0
	100DD	2.2	2	0.2	O	S=0	C=0
CS-2 [TC-3][TC-4]	60CD	3	1.7	1.3	O	S=0	C=0
	60DD	2.9	1.7	1.2	O	S=0	C=0
	100CD	3	2	1	O	S=0	C=0
	100DD	2.9	2	0.9	O	S=0	C=0

한 FTTI를 바탕으로 운전자의 인지 반응 지연 시간을 고려할 때, 제어권 전환이 시간 내에 가능함을 확인할 수 있었으며, 추가적인 결함 대응 시간이 필요하지 않음을 도출하였다.

안전 메커니즘이 적용됨으로써 운전자 상해 및 차량 충돌이 방지되었고, 이에 따라 Severity는 0으로 평가되었으며, Controllability 또한 주어진 FTTI 내에서 제어권이 전환될 수 있으므로 0으로 평가되었다. 이러한 결과를 통해 SOTIF 관점에서의 불합리한 위험이 더 이상 존재하지 않음을 확인할 수 있었으며, 따라서 자율주행 시스템의 SOTIF 확보를 확인하였다.

6. 결 론

본 논문에서는 STPA 안전 분석 기법을 SOTIF 위험 분석 프로세스에 적용하여 SCC 시스템의 위험을 분석하고, 이를 가상 환경에서 평가하였다. STPA 기법을 통해 LiDAR 센서 기반 SCC 시스템에서 발생할 수 있는 운전자 관점의 위험 요소와 사고 시나리오를 정의하고, Control structure를 이용하여 시스템 제어 구조를 분석한 뒤, 발생 가능한 UCA를 식별하였다.

LiDAR 센서가 객체 인식 정보를 제공하지 않거나 잘못된 정보를 제공하는 두 가지 경우를 대표 UCA로 선정하여 위험 평가 대상으로 설정하였다. 성능 한계 상황 분석에는 ISO 34502 표준 문서를 참고하여 LiDAR 센서의 미인지 및 오인지 원인을 분석하였다. 이를 바탕으로 UCA 발생 원인을 분석하고, Triggering condition과 Causal scenario를 도출하였다.

MATLAB/Simulink와 CarMaker 시뮬레이션 툴을 활용하여 위험 평가 환경을 구축하였으며, 외란 상황을 모방하기 위해 Point cloud 데이터에 Random dropout과 Gaussian noise를 적용하여 시스템이 객체를 미인지 또는 오인지하도록 구현하였다.

본 연구에서는 기존 연구를 참고하여, 시나리오는 Severity와 Controllability를 기준으로 평가되었으며, Controllability를 0으로 만드는 전략을 사용하여 위험 시나리오를 안전 시나리오로 개선하고자 하였다. Controllability는 TTC 관점에서 평가되었으며, 운전자가 적절한 시간 내에 제어권을 인수할 수 있도록 TOR을 설계 목표로 설정하였다. Time budget 내에 제어권 전환이 불가능한 상황에서는 FOT를 추가적인 시스템 개선 가이드라인으로 제시하였다. 기존 연구에서 도입된 Time budget 대신 FTTI 개념을 새롭게 도입하여 시스템의 위험 평가를 더욱 정교화 하였다. 이를 기반으로, 안전 요구 사항을 만족하기 위한 외란 판단 및 위험 상황 발생 시 Fail-Safe 관점에서의 MRM 알고리즘을 개발하였다. 이 알고리즘은 위험 시나리오에서 시스템이 안전하게 대응할 수 있도록 설계되었으며, 최종적으로 SOTIF 관점에서 위험 상황이 발생했을 때 시스템의 안전성을 확보하였다.

본 연구는 STPA와 가상 시뮬레이션을 활용하여 SOTIF 관점에서의 위험 분석 및 평가 프로세스를 제시함으로써, SAE Level 3 이상의 자율주행 시스템 개발에 기여할 수 있는 중요한 참고 자료를 제공하였다. 특히, STPA 기법을 적용함으로써 기존 FMEA/FTA 기반 분석에 비해 더 복잡한 상호작용과 시스템 오류를 체계적으로 분석할 수 있는 장점을 확보하였다. 이를 통해 인지 센서의 성능 한계에 따른 차량 레벨의 위험을 효과적으로 도출하였으며, 외란으로 인한 위험 상황 발생 시 감속을 수행하는 안전 메커니즘을 설계하였다. 이를 통해 운전자가 제어권을 전환하기 위한 충분한 시간을 확보하였고, 최종적으로 자율주행 시스템의 SOTIF 관점에서 위험이 안전한 수준으로 평가되었다.

다만, STPA 기법은 분석의 복잡성과 주관적 해석 가능성이라는 한계를 지니고 있다. 이러한 한계를 줄이기 위해 STPA 분석 소프트웨어 툴이 개발되고 있으며, 이는 FMEA/FTA 방식에서 사용되는 툴과 유사한 역할을 한다. 그러나 STPA는 최신 안전 분석 기법으로, 비교적 널리 사용되는 FMEA/FTA와 비교했을 때 관련 연구와 프로그램 개발이 상대적으로 적다. 그 결과, STPA 분석 소프트웨어 툴은 아직 완전한 자동화를 이루지 못하고, 분석 과정에서 많은 사용자의 주관적 판단과 수작업이 여전히 요구된다. 따라서, STPA 기법을 적용하는 과정에서는 이러한 불완전한 자동화로 인해 시간과 비용이 추가로 소요되는 Trade-off가 존재한다. 또한, 사용한 SCC 시스템은 상용화된 차량에 탑재된 SCC 시스템과 성능상의 차이가 있기 때문에 정합성 부분에서 실험 결과에 제한이 있다는 한계점이 있다. SCC 시스템의 제약된 기능 내에서 제한된 시나리오와, 인지 센서의 데이터 신호에 외란을 주입하는 방식으로 구현된 외란 모델에는 여전히 보완해야 할 부분이 존재한다. 현실과 정합성이 높은 차량 시스템 모델을 사용하고, 실제 외란과 유사한 고도화된 외란 모델을 적용하여 다양한 시나리오에서 테스트를 진행한다면, 보다 안전하고 신뢰성 있는 SAE Level 3 이상의 자율주행 시스템 구현에 기여할 수 있을 것으로 기대된다.

본 연구는 STPA를 적용한 SOTIF 프로세스를 통해 이해도를 높이고, 안전성 확보를 위한 중요한 가이드라인을 제시하였다. 향후에는 다양한 시나리오와 복잡한 외란 요소를 포함한 분석을 통해 범용적인 안전 메커니즘을 개발하고 평가할 계획이다.

후 기

본 연구는 산업통상자원부 자율주행기술혁신사업의 연구비지원(과제번호: 20018248, 주변 상황 인식 센서 성능 및 판단 기능 부족으로 인한 사고 위험 대응 기술(SOTIF) 개발)의 지원으로 수행된 연구임.

References

1) B. Y. Lee, "Domestic and International Trends and Prospects in Autonomous Vehicle Technology Development," Information and Communications Magazine, Vol.33, No.4, pp.10-16, 2016.
2) R. Mariani and K. Greb, "Recent Advances and Trends on Automotive Safety," 2022 IEEE International Reliability Physics Symposium (IRPS), IEEE, 2022.
3) ISO 26262 vs. SOTIF (ISO/PAS 21448): What's the Difference?, Retrieved from https://www.ptc.com/en/blogs/alm/iso-26262-vs-sotif-iso-pas-21448-whats-the-difference.
4) The Impact of Automotive SPICE and ISO 26262 on Your Engineering Process, Retrieved from https://lembergsolutions.com/blog/impact-automotive-spice-and-iso-26262-your-engineering-process.
5) Why SOTIF (ISO/PAS 21448) Is Key For Safety in Autonomous Driving, Retrieved from https://www.perforce.com/blog/qac/sotif-iso-pas-21448-autonomous-driving.
6) International Organization for Standardization, ISO 21448 - Road Vehicles - Safety of the Intended Functionality, ISO 21448, International Organization for Standardization, 2022.
7) S. P. Hong, A Study on the Application of Product Liability Act for Defect of Autonomous Vehicles, M. S. Dissertation, Hanyang University, Seoul, 2019.
8) H. S. Choi, S. J. Han, J. W. Jeon, S. M. Ahn and J. W. Yoo, "Simulation-Based SOTIF Hazard Analysis and Risk Assessment Methodology for Autonomous Driving System," Transactions of KSAE, Vol.32, No.4, pp.331-347, 2024.
9) Digital Today, Volkswagen CEO: Lidar is an Essential Device for Autonomous Driving, Retrieved from https://www.digitaltoday.co.kr/news/articleView.html?idxno=435336.
10) S. J. Kim and D. H. Shim, "Modeling and Analysis of IGLAD Traffic Accident Case Using Prescan for SOTIF Standard Development," Transactions of KASA, Vol.15, No.3, pp.53-58, 2023.
11) M. J. Kim, T. H. Kim and Y. M. Kim, "On the Integrated Process of RSS Model and ISO/DIS 21448 (SOTIF) for Securing Autonomous Vehicle Safety," Transactions of KOSSE, Vol.17, No.2, pp.129-138, 2021.
12) N. Leveson and J. Thomas, STPA Handbook, Cambridge, 2018.
13) K. Qin, Y. Wang, L. Liu, X. Xia, Q. Wang and Z. Zhang, "Analysis and Research on SOTIF of Typical L3 Autopilot System," International Conference on Cyber Security and Information Engineering, pp.82-86, 2022.
14) J. Barkovic, A Fault-Aware Sensor Fusion System for Autonomous Vehicles, M. S. Dissertation, McMaster University, Hamilton, 2020.
15) International Organization for Standardization, "ISO 34502 - Road Vehicles - Test Scenarios for Automated Driving Systems Scenario-Based Safety Evaluation Framework," ISO 34502, International Organization for Standardization, 2022.
16) J. H. Kim, Model Predictive Control Based ACC Controller Design to Avoid Abnormal Driving Vehicles, M. S. Dissertation, Hanyang University, Seoul, 2022.
17) H. S. Roh, Development of the Longitudinal Control for Truck Platooning, M. S. Dissertation, Kookmin University, Seoul, 2020.
18) R. B. Rusu and S. Cousins, "3D Is Here: Point Cloud Library (PCL)," International Conference on Robotics and Automation, pp.1-4, 2011.
19) Y. Zhang, J. Hou and Y. Yuan, "A Comprehensive Study of the Robustness for LiDAR-Based 3D Object Detectors Against Adversarial Attacks," International Journal of Computer Vision, Vol.132, No.5, pp.1592-1624, 2024.
20) J. Li, Y. Zhang, S. Zho, C. Chen and Z. Du, "A Research on SOTIF of LKA Based on STPA," 2022 IEEE International Conference on Real-Time Computing and Robotics (RCAR), pp.396-400, 2022.
21) SAE International, SAE J2980 Surface Vehicle Recommended Practice, SAE J2980, SAE International, 2023.
22) H. G. Park, Y. S. Park and S. W. Park, "A Study on the Correlation Between Effective Impact Speed and the Severity of Collision Accidents with Fishing Vessels," Transactions of KINPR, Vol.47, pp.202-211, 2023.
23) M. S. Jang, S. K. Lee, J. S. Kim, S. M. Hong and K. J. Lee, "The Chronological Evolution of Driver's Perception Reaction Time," Korean Society of Transportation, Vol.8, No.6, pp.55-61, 2011.
24) D. Denomme, S. Hooson and J. Winkelman, "A Fault Tolerant Time Interval Process for Functional Safety Development," SAE 2019-01-0110, 2019.