SOTIF
(Safety of The Intended Functionality)

SOTIF에서 운전자 오사용

안창남*

Driver Misuse in SOTIF

Changnam Ahn*

Key Words : Driver, Misuse, Functional Safety, Safety of Intended Functionality, Automotive Driving Assistant System, Performance, Limitations, Safety Analysis

ABSTRACT

유연성을 가진 사람은 긴급 상황에서 임기응변적 대응을 할 수 있어 자동화 시스템 대비 큰 장점을 가지고 있으나 때로는 그 유연한 행동이 위험한 상황을 유발할 수 있어 그 원인을 파악하고 적절한 시스템적 대응 설계를 통하여 방지할 필요가 있다. 이러한 설계를 위하여서는 자동화 제어기 속에서의 운전자의 역할 및 인적 오류에 대한 기본적인 이해가 필요하다. 일부 자동화 차량의 운전자와 같이 자동화 시스템에 지나치게 과신하는 경우에는 교육이나 사회적인 인식 변화가 우선 필요하겠지만 안전 설계 관점에서는 시스템에 대한 운전자의 지식과 신뢰를 실제 기능에 적절하게 맞추기 위하여 운전자 모니터링 경고와 같은 추가 정보를 주거나 긴급 상황 시 직관적인 조작으로 그들의 가설을 안전하게 테스트 할 수 있도록 보완해야 한다. SOTIF를 고려한 DCAS 법규 제정과 같이 자동차 안전 패러다임과 소비자 사용 조건 변화에 있어서 운전자의 오사용 대응 기술은 현재 자동차 안전 패러다임 변화에 있어서 핵심 안전 기술이다. 자동화는 사람을 대체하는 것이 아니라 사람의 능력을 증강 시키도록 설계 되어야 한다. 이를 위하여 자동화 프로세스 모델과 운전자 멘탈 모델이 조화 될 수 있도록 적절한 시점에 올바른 피드백을 제공하여 오사용을 방지하도록 해야 한다.

* 현대자동차/글로벌R&D마스터
E-mail : fedummy@hyundai.com

자율주행시스템의 SOTIF 안전성 검증 방안 연구

이혁기*·신성근**

A Study of Safety Validation Method of Automated Driving Systems

Hyuck-kee Lee*, Seong-geun Shin**

Key Words : SOTIF(Safety of the Intended Functionality, 운행안전), Virutal Validation(가상 검증), HILS(하드웨어인 더룹 시뮬레이션), Safety Assessment(안전성 평가), Scenario-based Safety Evaluation(시나리오기반 안전 검증)

ABSTRACT

Commercialization of Lv.3 Automated Driving Systems includes many kinds of verification and validation tests to assess the safety of the vehicles in hazardous scenarios. In that test, many kinds of Environment and traffic conditions shoud be considered to confirm the safe response of the automated vehicle. ISO 21448 includes the process and methods for the safety validation of Automated vehicles. The scenarios are too complex to execute experiments in a proving ground with real vehicles. UNECE also regulate the automated vehicles to be commercialized safely and published the guideline of New Assessment and Test Method for Automated Driving including scenario catalogue and virtual validation. In this paper, we deals with the overall SOTIF process and the validation method using HILS and simulation environments. Configuration of scenario space and realistic simulation environment would be essential to validate the safety of the automated driving in simulated space. the required simulation environment and detailed methodoloiges will also be discussed to meet the absence of unreasonable risk of automated driving.

* 한국자동차연구원/부문장
** 한국자동차연구원/책임연구원
E-mail : hlee@katech.re.kr

SOTIF Analysis 방법론

김정기*

SOTIF Analysis Methodology

Jeong-Kee Kim*

Key Words : ISO, Functional Safety, ISO21448, Safety of Intended Functionality, Automotive Driving Assistant System, Performance, Limitations, Safety Analysis

ABSTRACT

ISO TC22 / SC32 /WG은 기능안전(Functional Safety)을 다루는 표준화 기구이다. 여기서 지난 2023년 ISO21448을 제정하였다. ISO21448은 “Safety of Intended Functionality”를 다루는 표준으로 SOTIF 표준이라고 알려져 있다. 이 표준은 기능안전 보다 자율주행에 특화되어 있는 전기전자 시스템의 안전을 위해 제정된 표준으로 “의도된 기능을 수행함에 있어서도 안전을 유지”해야 하는 내용을 기반으로 발표되었다. 이는 자율주행 시스템에 속하는 ADAS(Automotive Driving Assistant System) 시스템이 올바르게 동작하더라도 안전에 위배되는 사항에 대한 분석과 이에 대한 위험성을 판단하여 이에 대응되는 설계를 보장할 수 있어야 한다. 이는 성능(Performance)이나 성능 한계(Limitations)에 대한 대응 설계가 필요함을 기반으로 하고 있다.

이를 위하여 모든 전기전자 시스템은 SOTIF에서 요구하는 수준의 분석을 통해 위험 요소를 식별하고, 이에 대한 위험도에 대한 평가를 수행해야 한다. 잘 알려진 기법으로 STPM이나 Safety Analysis등을 활용할 수 있으며, 본 세션에서는 복잡한 자율주행 시스템의 분석 방법에 대한 기본적인 요구사양과 개념을 전달하고자 한다.

* 씨엔비스/총괄사업본부장
E-mail : jkkim@cnbis.co.kr

실차 기반 SOTIF 시나리오 및 주행 실증 분석 연구 및 인지 기술 소개

현영진*

Introduction to Actual Vehicle-Based SOTIF Scenario and Driving Substantiation Analysis Research and Perception Technology

Young-Jin Hyun*

Key Words : Autonomous Vehicle, SOTIF, ISO 21448, Perception

ABSTRACT

OTIF(ISO 21448)는 기능안전(ISO 26262)과 달리 오작동, 고장, 결함에 관해 다루는 것이 아니라 의도된 설계 자체가 안전을 확보하기에 불충분/부적절한 경우를 다룬다. LV4 자율주행에 도전하고 있는 에스유엠에서는 “실차기반 unknown hazard 시나리오 도출, 안전대책 설계, 개발, 실차기반 SOTIF 시나리오 대응 검증”을 위한 연구를 추진하고 있다. 현재 자율주행 실증 테스트베드(상암, 시흥 등)에서 150km이상 주행데이터를 취득하여 실차 기반 주행 실증 분석을 통해 <모래, 염화칼슘에 의한 차선 미인지>, <버스 미인지(라이다)>, <차량 오인지(라이다)>, <나뭇가지 오인식>, <카메라 역광>, <라이다센서 버스 미인식>, <역광으로 사람 미인식> 등의 hazard 시나리오를 도출하였다. 도출된 시나리오를 기반으로 자율주행 실차의 센서을 다중다종 센서 및 시스템을 업그레이드 추진 및 실차 기반 unknown hazard 시나리오 도출 및 시뮬레이션 시나리오의 재현을 추진 중에 있다. 에스유엠에서는 도출한 hazard 시나리오를 기반으로 인지 알고리즘 개선을 진행 중에 있으며, 인지 기술에 대한 간략한 소개를 진행하고자 한다.

본 논문은 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구임 (과제번호 : 20018248, 과제명 : 주변 상황 인식 센서 성능 및 판단 기능 부족으로 인한 사고 위험 대응 기술(SOTIF) 개발)

* ㈜에스유엠/대표
E-mail : jyh@smobi.ai

SOTIF 기반 인식센서 성능 한계 시나리오 도출 및 평가

최경진*·문성준*·우승훈**

Derive and Evaluate SOTIF-Based Perception Sensor Performance Limit Scenarios

Kyungjin Choi*, Seongjoon Moon*, Seunghoon Woo**

Key Words : Functional safety(기능안전), Safety of the intended functionality(의도된 기능에 대한 안전 분석), Perception sensor(인지 센서), System theoretic process analysis(시스템 이론 프로세스 분석)

ABSTRACT

The purpose of this research is to derive and evaluate performance limit scenarios based on SOTIF for cognitive sensors used in autonomous driving.

This research is conducted through the combination of the limit factors of the cognitive performance of the sensor and the causal scenarios derived through the System Theoretic Process Analysis (STPA) method to derive the performance limit scenarios.

The performance limit factors of the sensor are derived from standard documents, hardware characteristics of the sensor, and accident case analysis. The derived performance limit factors are then implemented into the performance limit cognitive model for evaluation.

The STPA method derives causal scenarios in the order of defining the analysis purpose, modeling the control structure and defining control actions, identifying unsafe control actions, deriving causal factors, and defining causal scenarios. The causal scenario and the performance limit factor of the sensor are combined to form a performance limit scenario.

The performance limit scenario evaluation method evaluates the performance limit scenario implemented with IPG CarMaker through the risk evaluation indicator using the value of the sensor model in which the performance limit element of the sensor is implemented as the input value of the autonomous driving system implemented in Mathworks Matlab&Simulink in the environment.

* 국민대학교/박사과정
** 국민대학교/교수
E-mail : cart9535@kookmin.ac.kr

SOTIF 관점에서의 시나리오 기반 개발 및 검증 방법의 현황과 도전

서도현*·김승환*·송봉섭**

Survey and Challenges of Scenario-Based Development and Validation in the Viewpoint of SOTIF

Dohyun Seo*, Seunghwan Kim*, Bongsob Song**

Key Words : Scenario-based(시나리오 기반), Safety of the intended functionality(의도된 기능에 대한 안전 분석), Data-driven(데이터 기반), Safety-critical scenario(위험 시나리오), Generative model(생성형 모델)

ABSTRACT

The survey of safety-critical scenario generation methods is introduced to accelerate both development and validation of automated vehicles (AV) in the viewpoint of safety of the intended functionality (SOTIF). These safety-critical scenarios may be applied for various applications ranging from development of perception and decision algorithms to the corresponding test and validation. A systematic process for the scenario-based approach in the literature is in general composed of six steps: sources for scenarios, scenario generation, scenario database, selection of concrete scenarios, scenario execution, and AV assessment. While the knowledge-based scenario generation was suggested earlier for accident in-depth study, more attention has paid to the data-driven approach. On the other hand, as deep learning (DL) based approaches are used widely in AV applications, their systematic process for training and test becomes critical for scalability and commercialization. In consequence, it is discussed that the safety-critical scenario in the scenario generation has similarities with unknown unsafe events in SOTIF and a long-tailed problem in DL. It is proposed that the systematic process for the safety-critical scenario generation can be evolved to identify the unknown and unsafe event in field operation test (FOT) data as well as to augment training dataset for DL. Finally, it is demonstrated that DL can be applied to select a set of testable concrete scenarios in order to build up mutual collaborations between DL and scenario generation as a challenge in near future.

* 아주대학교/석사과정
** 아주대학교/교수
E-mail : bsong@ajou.ac.kr