STPA를 활용한 자율주행자동차의 시뮬레이션 기반 오류 주입 시나리오 및 안전조치 시간 연구

A Study on Simulation Based Fault Injection Test Scenario and Safety Measure Time of Autonomous Vehicle Using STPA

안 대 룡* · 신 성 근** · 백 윤 석** · 이 혁 기** · 박 기 홍*** · 최 인 성****

* 주저자 및 교신저자 : 자동차부품연구원 스마트운전제어연구센터
** 공저자 : 자동차부품연구원 스마트운전제어연구센터
*** 공저자 : 국민대학교 자동차공학과 교수
**** 공저자 : 교통안전공단 자동차안전연구원 자율주행실 책임연구원

Dae-ryong Ahn* · Seong-geun Shin** · Yun-soek Baek** · Hyuck-kee Lee** · Ki-hong Park*** · In-seong Choi****

* Smart Driving Contro R&D Center, Korea Automotive Technology Institute
** Smart Driving Contro R&D Center, Korea Automotive Technology Institute
*** School of Automotive Eng, Kookmin University
**** Autonomous Vehicle R&D Team, Korea Automobile Testing and Research Institute
† Corresponding author : Dae Ryong Ahn, drahn@katech.re.kr

Vol.18 No.2(2019)
April, 2019
pp.129~143

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2019.18.2.129

Received 4 March 2019
Revised 30 March 2019
Accepted 3 April 2019

요 약

자율주행자동차의 안전에 대한 중요성이 강조되면서 안전성 및 신뢰성 향상을 위한 개발 검증 지침인 ISO-26262의 적용과 자율주행자동차의 안전성 검증에 대한 중요성이 높아지고 있다. 특히 미국자동차공학회 기준 Level 3 이상의 자율주행자동차는 운전자 대신 주변 환경을 감지하고 판단한다. 따라서 자율주행 기능에 이상이 생기거나 오작동 발생 시 안전에 심각한 영향을 미칠 수 있으므로 자율주행자동차는 고장 및 오작동에 대비하여 안전개념을 적용하고 이를 검증해야 한다. 본 연구에서는 ISO-26262 Part3 프로세스와 시스템 이론적 프로세스 분석 방법론인 STPA를 활용하여 자율주행자동차의 안전성 평가 및 검증을 위한 오류 주입 시나리오를 연구하고 시뮬레이션 기반의 오류 주입 테스트를 통해 안전개념 설계를 위한 안전조치 시간을 연구하였다.

핵심어 : 자율주행자동차, 평가, 오류주입, 시스템 이론적 프로세스 분석, 안전조치 시간

ABSTRACT

As the importance of autonomous vehicle safety is emphasized, the application of ISO-26262, a development verification guideline for improving safety and reliability, and the safety verification of autonomous vehicles are becoming increasingly important, in particular, SAE standard level 3 or higher level autonomous vehicles detect and decision the surrounding environment instead of the human driver. Therefore, if there is and failure or malfunction in the autonomous driving function, safety may be seriously affected. So autonomous vehicles, it is essential to apply and verity the safety concept against failure and malfunctions.

In this study, we study the fault injection scenarios for safety evaluation and verification of autonomous vehicles using ISO-26262 part3 process and STPA were studied and safety measures for safety concept design were studied through simulation bases fault injection test.

Key words : Autonomous vehicle, Assessment, Fault injection, STPA, Safety measure time

Ⅰ. 서 론

1. 개요

자동차의 첨단 기술이 발전하면서 최근 자동차 업계 및 학계에서는 운전자 없이 주변 상황을 스스로 판단하여 차량을 제어하는 자율주행자동차 개발이 확대되고 있다. 또한, 세계 곳곳에서 자율주행자동차의 시범주행 및 법규를 개발하고 있다.(Chae et al., 2016) 미국, 영국, 일본 등 선진국에서는 자율주행자동차 관련 투자 계획 및 제도를 마련 중에 있으며 국내의 경우 국토교통부를 중심으로 ADAS 시스템 및 자율주행자동차의 평가 기준을 고도화 하고 자율주행자동차의 조기 상용화를 위한 정책을 활발히 마련하고 있다.(Kim et al., 2017) 또한, UNECE 산하 WP.29의 Regulation.79 Annex6에서는 복합 전자제어 시스템의 안전 설계 여부를 확인하고 평가를 수행하는 특별 요구사항을 포함시켰다.

현재 상용화되어 도로를 주행하고 있는 자율주행자동차는 미국자동차공학회(SAE) 기준으로 Level 2 수준이며 특정 구간에서만 자율주행을 허용하고 운전자는 전방 및 차량의 주변상황을 주시해야 하는 수준이다. 아래 <Table 1>은 SAE 기준 자율주행의 Level 별 수준을 정의한 표이다.(J3016, 2016)

<Table 1> Define of autonomous vehicle level (SAE)

Level	Dynamic Driving Task	Object and Event Detection and Response	Dynamic Driving Task Fallback
0	Driver	Driver	Driver
1	Driver-System	Driver	Driver
2	System	Driver	Driver
3	System	System	Fallback Ready Driver
4	System	System	System
5	System	System	System

DDT(Dynamic Driving Task)는 차량의 조향 및 감속, 가속의 행위를 통해 차량을 제어하는 것이고, OEDR(Object and Event Detection and Response)은 차량 주변의 물체 및 발생하는 이벤트에 대한 반응을 나타내는 것이다. Fallback은 시스템 이상이나 고장 등 돌발 상황 발생 시 누가 제어권을 가지고 있는지를 나타낸다. 자율주행자동차의 수준이 Level 3로 발전한다면 운전자는 전방 및 주변 상황을 주시해야하는 의무가 사라지며 자율주행시스템이 대신하여 전방 및 주변 상황을 검지하고 판단하여 제어를 수행하게 된다. 따라서 시스템 고장 또는 오류로 인한 위험 상황 발생 시 경고를 통해 운전자에게 차량의 상태를 알려야 하며 운전자에게 제어권을 넘길 때까지 시스템은 설계된 안전개념을 통해 안전한 동작을 보장해야한다. 안전개념의 적용 유무를 검증하기 위해 사용되는 시험 방법은 오류주입 시험으로 임의의 오류를 시스템에 주입하여 오작동을 일으키고 적용된 안전개념이 동작하여 차량의 안전한 주행을 보장하는지 검증하는 방법이다. 하지만 실제 자율주행자동차로 안전개념을 검증하는 방법은 매우 위험하고 어렵기 때문에 실차 시험 전 시뮬레이션을 통한 충분한 선행 시험이 효과적일 수 있다.

본 논문에서는 자율주행자동차의 자율주행시스템을 ISO-26262 Part3 프로세스와 STPA(Systems Theoretic Process Analysis) 기법을 이용하여 시뮬레이션 기반의 자율주행시스템의 안전개념 검증을 위한 오류주입 시험 시나리오에 대한 연구를 수행하고 시나리오 중 “의도치 않은 가속”과 “의도치 않은 조향”에 대한 오류주입 시뮬레이션을 통해 안전개념 설계 시 필요한 안전 조치 시간에 대한 연구를 수행하였다.

Ⅱ. 자율주행시스템의 기능 및 오작동 정의

자율주행시스템의 안전 분석을 위해서는 먼저 자율주행시스템의 기능을 정의해야 한다. 자율주행시스템은 차량에 장착된 센서 및 GPS 데이터를 바탕으로 주행환경을 인식하여 운전을 보조하거나 스스로 주행함으로써 주행 안전성 및 편의성을 향상시키는 차세대 지능형 자동차를 말한다.(Chu, 2011) 자율주행시스템을 구성하는 요소는 센서, 제어기, 액추에이터로 구분되지만 본 논문에서는 자율주행자동차의 기능제어기만을 고려하여 연구를 수행하였다.

1. 자율주행시스템 기능정의

차량 수준의 자율주행시스템 주 기능은 주변 환경 데이터를 기반으로 적절한 종방향 및 횡방향 제어를 수행하는 것이다. 따라서 본 연구에서는 자율주행시스템의 기능을 아래 <Table 2>와 같이 정리하였다.

2. 자율주행시스템 오작동 정의

자율주행시스템의 오작동 정의는 가이드 워드 기반의 분석 기법인 HAZOP 기법을 사용하여 도출하였다. HAZOP 기법에서 No or Not, More, Less 등과 같은 가이드워드들은 위험원을 도출하는 과정에서 시스템의 여러 상태와 결함되어 설계의도에서 벗어날 수 있는 이상 현상들을 식별하여 위험원의 발생을 찾게 되는 개념이다.(Hwang et al., 2010) 본 논문에서 자율주행시스템의 기능별 오작동을 도출하기 위해 사용된 가이드워드는 “No or Not, Incorrect”를 사용하였다. No or Not은 기능의 미수행을 의미하며 Incorrect는 기능의 잘못된 수행을 의미한다. 잘못된 수행은 정상적인 값이 아닌 잘못된 값을 출력하는 경우, 기능이 수행되지 않아야 하지만 기능이 수행되는 경우를 포함한다. 아래 <Table 3>은 가이드워드를 활용한 자율주행자동차의 기능별 오작동을 정리한 표이다.

<Table 2> ADS function definition

Function	Description
Acceleration	Accelerates the vehicle with appropriate acceleration
Deceleration	Decelerate the vehicle at the appropriate deceleration
Steering	Steering control for lane keeping

<Table 3> ADS malfunction

Function	Malfunction
Acceleration	Unintended acceleration
Deceleration	Unintended deceleration
	Not deceleration
Steering	Unintended steering
	No steering

Ⅲ. STPA 수행

STPA는 Systems Theoretic Process Analysis의 약어로 사고의 인과 관계를 분석하여 안전성 분석을 수행하기 위한 모델로 본 논문에서 수행하는 시스템의 고장안전성을 평가하는 시나리오를 도출하기 위해 사용하였다. STPA는 시스템의 요서간의 상호작용에 대한 고장 발생 시 일어날 수 있는 사고 상황과 위험원을 식별하고 사고를 발생시키는 부적절한 제어 명령을 찾아내는 것이 주된 목적이다. STPA의 수행 과정은 크게 준비 단계와 실행 단계로 나누어진다.(Yang and Kwon, 2017)

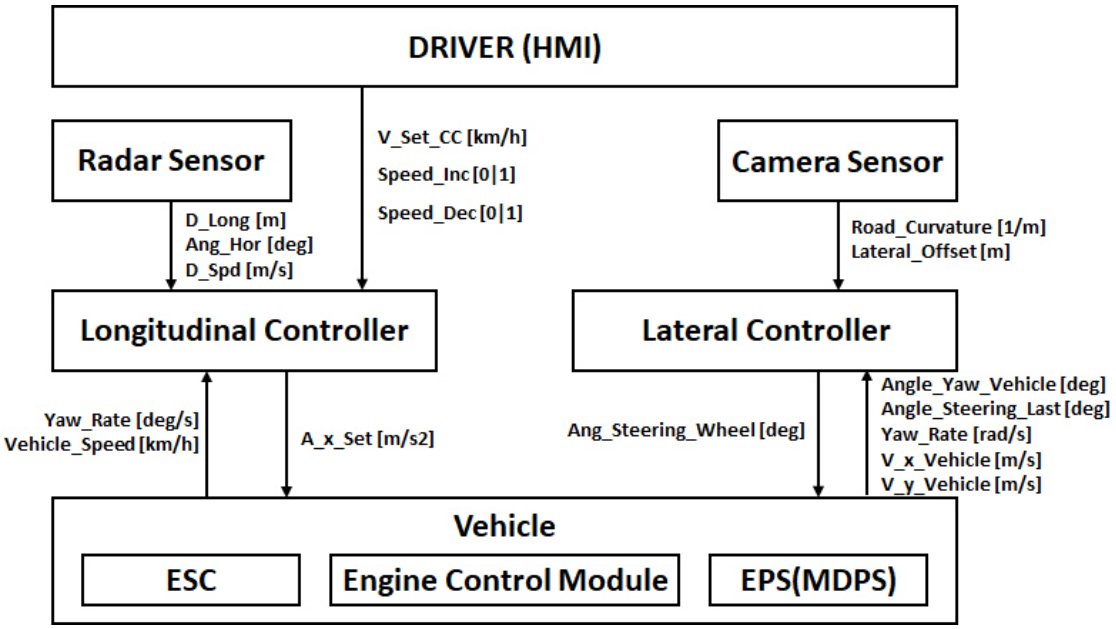
1. STPA 준비 단계

STPA를 진행하기 위한 준비 단계로는 사고 상황(Accident)과 위험원(Hazard)를 식별하고 시스템의 제어 구조도를 통해 제어 명령을 식별해야 한다. 사고 상황은 인명, 재산 손실, 환경오염, 임무 손실 등을 초래하는 바람직하지 않거나 예상치 못한 사건으로 정의되며 본 논문에서는 자율주행시스템의 오작동으로 인해 발생할 수 있는 사고 상황으로 설명된다. 위험원은 사고 상황을 초래하는 시스템의 상태를 나타낸다. 아래 <Table 4>는 자율주행시스템의 차량 수준의 위험원과 사고 상황을 정리한 표이다.

<Table 4> ADS Accident Definition

Index	Description	Vehicle Level Hazard and Accident	
A1	Rear-end-collision of the front vehicle	H1	Rear-end-collision of the front vehicle due to unintended acceleration
		H2	Rear-end-collision of the front vehicle due to not deceleration
A2	Rear-end-collision of the backward vehicle	H3	Rear-end-collision of the front vehicle due to unintended deceleration
A3	Lane departure (Crashes with vehicle or obstacle)	H4	Lane departure due to unintended steering
		H5	Lane departure due to no steering control (Curved road)

사고 상황 및 위험원을 식별한 다음 시스템의 제어구조도를 통해 제어 명령을 식별해야 한다. 아래 <Fig. 1>은 본 논문에서 사용된 자율주행 시스템의 제어 구성도를 간략하게 나타낸 그림이다. 크게 6가지 컴포넌트로 나뉘며 운전자의 설정 속도 입력과 인터페이스 스위치를 통한 속도 증감 값과 Radar 센서를 통해 주변 물체의 종/횡방향 수평각도(D_Long, Ang_Hor), 상대속도(D_Spd), 가속도(D_acc)의 시그널이 Longitudinal Controller로 입력된다. Camera 센서를 통해 출력되는 도로의 곡률(Road_Curvature)과 차선 중심으로 부터의 차량의 위치 값



<Fig. 1> ADS Control structure

(Lateral_Offset)은 Lateral Controller로 입력된다. 각 Controller로 입력된 데이터를 바탕으로 Longitudinal Controller는 가속도(a_x_Set)를 자동차에 요청하여 적절한 종방향 제어를 수행하며, Lateral Controller는 속도와 도로 곡률에 맞는 조향각을 자동차에 요청하여 적절한 횡방향 제어를 수행한다.

2. STPA 실행 단계

STPA의 실행 단계에서는 Unsafe Control Action(이하 UCA)을 정의하고 UCA가 발생되는 요인을 분석하는 Causal Factor 분석이 수행된다. 첫 번째로 UCA 분석은 안전하지 않은 제어 명령을 정의하는 단계로 앞에서 사용된 Guide Word 개념을 사용하는 HAZOP 기법(Whang et al., 2010) 과 유사한 형식으로 진행된다. STPA에서 UCA를 정의하는 방법은 아래 4가지 분류에 따라 진행된다.

1) 안전에 필요한 제어 미수행에 따른 위험
2) 안전하지 않은 제어 수행에 따른 위험
3) 안전에 필요한 제어가 “Too Early/Too Late/Wrong”하게 시작되는 것에 따른 위험
4) 안전에 필요한 제어가 “Too Early/Too Late/Wrong”하게 종료되는 것에 따른 위험

자율주행시스템의 제어 수행 별 4가지 분류에 따른 UCA 정의는 아래 <Table 5>와 같이 정리하였다.

<Table 5> ADS Accident Definition

Control Action	Not providing causes hazard	Providing caused hazard	Incorrect/Timing order	Stopped too soon/ applied too long
Acceleration	-	H1	Include in H1	
Deceleration	H2	H3	Include in H3	
Steering	H4	Include in H5	H5	Include in H4, H5

<Table 5>에서 표현된 H1은 “의도치 않은 가속” 상황을, H2는 “미감속” 상황, H3는 “의도치 않은 감속”, H4는 “조향 미수행”, H5는 “의도치 않은 조향”을 의미한다.

STPA 실행단계의 두 번째 내용은 UCA를 발생시키는 요인을 분석하는 Causal Factor를 분석하는 것이다. UCA의 발생 요인은 종방향 및 횡방향 제어기의 입력 및 출력 시그널의 값이 정상 상태의 값과 상이할 경우 발생하는 것으로 분석하였다. 아래 <Table 6>은 <Fig. 1>의 제어 구성도 입출력 시그널을 바탕으로 <Table 4, 5>에서 분석된 위험원 별 발생 요인 중 종방향 및 횡방향 제어기에 대한 Causal factor를 정리한 표이다.

<Table 6> Controller causal factor

Causal Factors		
H1	Input	Decision the **V_Set_CC** value as higher then the current speed
		Decision that the **Speed_Inc** signal is input
		Decision that the **D_Long** value of the radar sensor is longer than the actual relative distance
		Decision that the **D_Spd** value of the radar sensor is higher than the actual relative speed
		Decision that the current speed is lower than the **V_Set_CC** value
	Output	Output the calculated **A_x** of the controller to a value higher than the normal value
		Controller request invalid **+A_x** value

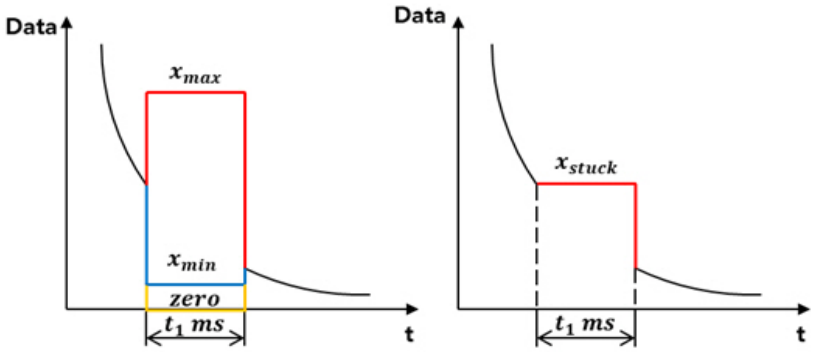
Causal Factors		
H2	Input	Decision that the **D_Long** value of the radar sensor is larger than the actual relative distance
		Although the actual relative distance is shortened, it is decided than the **D_Long** value does not change
		Although the actual relative speed is decreasing, the **D_Spd** value of the radar sensor
H3	Input	Decision the **V_Set_CC** value as lower then the current speed
		Decision that the **Speed_Dec** signal is input
		Decision that the **D_Long** value of the radar sensor is shorter than the actual relative distance
		Decision that the **D_Spd** value of the radar sensor is lower than the actual relative speed
	Output	Controller request invalid **-A_x** value
H4	Input	Decision that **Road_Curvature** value is 0
		Decision that **Ang_Yaw_Vehicle** is 0
		Decision that **Yaw_Rate** value is 0
	Output	Controller request **Steering_Wheel_Angle** is 0
H5	Input	Decided as an **Road_Curvature** value that does not fit the real road curvature
		Decided as an **Lateral_Offset** value that invalid
		Decided as an **Ang_Yaw_Vehicle** that invalid
		Decided as an **Yaw_Rate** that invalid
	Output	Controller request invalid **Steering_Wheel_Angle** value

Ⅳ. 오류 주입 시나리오

STPA 적용을 통해 도출한 Causal factor를 기반으로 자율주행자동차의 주요 위험원을 유발시킬 수 있는 제어기의 입출력 변수와 조건을 확인하였다. 도출된 입출력 변수 및 오작동 조건과 자율주행자동차의 주행 조건을 결합하여 오류 주입 사니리오를 연구하였다. 오류는 제어기가 입력값을 잘못 판단하는 경우를 모사하기 위해 제어기의 입력단에 변조된 센서 데이터를 주입하는 형식으로 수행하였고, 입력값은 정상적인데 제어기 내의 오류로 인해 제어기 출력 값이 잘못되는 경우는 제어기 출력단의 값을 변조시키는 방식으로 진행하였다.

1. 오류 Case 정의

오류 주입 시나리오를 도출하기 위해 주입을 수행할 오류에 대한 Case를 정의하였다. 일반적으로 오류 주입 Case는 Open Circuit, Short to GND, Short to VBAT, Short to signal measurement channel, Short to signal generation channel, Short to bus channel 등 전기적 신호에 의한 오류가 일반적이지만 본 논문에서는 위에 언급된 어떠한 오류로 인해 발생되는 Signal 수준의 오류 Case를 정의하여 시나리오를 도출하였다. 오류 Case는 아래 <Fig. 2>와 같이 크게 두 가지 경우로 나누었으며 첫 번째는 임의의 시간 동안 잘못된 데이터가 입력되는 오류로 입력 데이터는 출력 가능한 Max 값, Minimum 값, Zero(0), 그리고 임의의 시간 동안 이전 값이 고정되는 Stuck의 경우로 정의하였다.



<Fig. 2> Fault case

본 논문에서 도출한 시나리오에서 사용되는 오류 주입에 대한 변수는 센서-제어기-액추에이터 사이에서의 CAN을 통해 전달 가능한 데이터 값의 최소값(Min), 최대값(Max)으로 정하였으며 값에 대한 기준은 본 논문의 시뮬레이션 모델인 ASM과 보유하고 있는 시험 차량 및 실제 센서의 CAN 통신 프로토콜 자료를 참고하였고 아래 <Table 7>과 같이 정리하였다.

<Table 7> Signal min and max value

Signal	Min	Max	Unit
Curvature	-0.032768	0.032768	1/m
Lateral Offset	-20.5	20.5	m
D_Long	0	327	m
Hor_Angle	-7	7	deg
D_Spd	-51	51	m/s
A_x	-10	10	m/s2
Steering Wheel Angle	-450	450	deg
V_Set_CC	0	255	km/h

2. 종방향 오류 주입 시나리오

종방향 오류 주입 시나리오는 차량의 속도, 차간 거리, 주입 오류로 3가지 범주를 기반으로 도출하였다. 종방향 오류의 경우 횡방향 자율주행시스템은 정상적으로 작동하고 있는 것으로 가정하고 의도치 않은 가속 및 감속, 미감속과 같은 Hazard를 통해 사고가 발생하는데 주입 오류 별 차량의 속도와 차간 거리가 사고와 가장 연관된 범주라 판단하였다. 의도치 않은 가속인 경우 저속에서 높은 가속도에 의한 가속이 발생하는 경우도 고려하여 저속(30km/h), 중속(60km/h), 고속(100km/h) Case로 세분화 하였으며, 의도치 않은 감속과 미감속 시나리오의 경우는 중속과 고속만을 고려하였다. 또한 차간 거리는 ISO-22179(ISO-22179, 2009) 종방향 주행지원시스템(FSRA)의 최소 간격으로 설정되는 Time gap 1s로 설정하였다. 단, 의도치 않은 감속 의 경우 극단적인 케이스로 후방 차량과의 거리는 5m로 가깝게 추종하도록 설정하였다.

<Table 8> Longitudinal falut injection scenario

Index	Vehicle Speed [km/h]	Relative Distance	Forward Vehicle Deceleration	Injection Fault
H1	30, 60, 100	Time gap 1s	-	A_x : Max
				D_Long : Max
				D_Spd : Max
				Hor_Angle : Min/Max
		Single driving	-	V_Set_CC : Max
H2	60, 100	Time gap 1s	0.4g, 0,7g, 1.0g	D_Long : Max, Stuck
				D_Spd : Stuck
H3	80, 100	5m	-	A_x : Min
				D_Long : Min
				D_Spd : Min
		Signel driving	-	V_Set_CC : Min

3. 횡방향 오류 주입 시나리오

횡방향 오류 주입 시나리오는 종방향 오류 주입 시나리오의 3가지 범주 중 차간 거리 대신 도로의 곡선반지름을 범주에 추가하여 도출하였다. 횡방향 오류 주입의 경우 전방 및 후방 차량 보다는 차로 이탈로 인한 인접 차선의 차량이나 장애물과의 사고가 일어나는 경우를 고려하였다. 도로의 곡선 반지름은 고속도로 중 급격한 곡선로가 포함된 호남고속도로의 예를 들어 350m(Kang et al., 2002)로 결정하였다. 또한 차량의 주행속도는 저속 영역보다 고속 영역에서의 조향에 대한 위험도가 크므로 고속 주행상황 (100km/h)으로 설정하였다. 아래 <Table 9>와 같이 횡방향 오류 주입 시나리오를 정리하였다.

<Table 9> Lateral fault injection scenario

Index	Vehicle Speed [km/h]	Radius	Injection Fault
H4	100	350m	Steering Wheel Angle : 0
			Curvature : 0
H5		350m	Steering Wheel Angle : Min / Max
			Lateral Offset : Min / Max
		∞	Curvature : Min / Max

Ⅴ. 오류 주입 시뮬레이션

도출된 시나리오를 기반으로 본 논문에서는 종/횡방향 시스템의 대표적인 오류인 의도치 않은 가속(H1)과 의도치 않은 조향(H5)에 대한 오류 주입 시뮬레이션을 실시하였다. 횡방향 시스템은 Redundancy 구조로 되어 있으며 오류 주입 시간 이후 시스템은 정상 상태로 돌아오는 구조로 설계하였다.

1. 시뮬레이션 환경

시뮬레이션 환경은 독일의 dSPACE사의 ASM 모델을 사용했으며 ControlDesk 툴을 이용하여 모델의 입력 및 출력 단에 오류를 주입할 수 있게 구성하였다. 본 논문에서의 차선 이탈 판단여부는 차량의 전륜 바퀴의 측면이 차선을 넘어가는 순간으로 판단하였으며 차량의 폭은 1.8m, 도로의 폭은 3.5m로 설정하였다. 오류 주입 시험은 제어로직의 입출력 단에 사용자의 임의의 시간과 임의의 값을 넣을 수 있도록 모델 인터페이스를 구성하였고 dSPACE의 ControlDesk 툴을 활용하여 오류 주입을 수행하였다.

<Fig. 3> Simulation environment

2. 종방향 오류 주입 시뮬레이션 결과

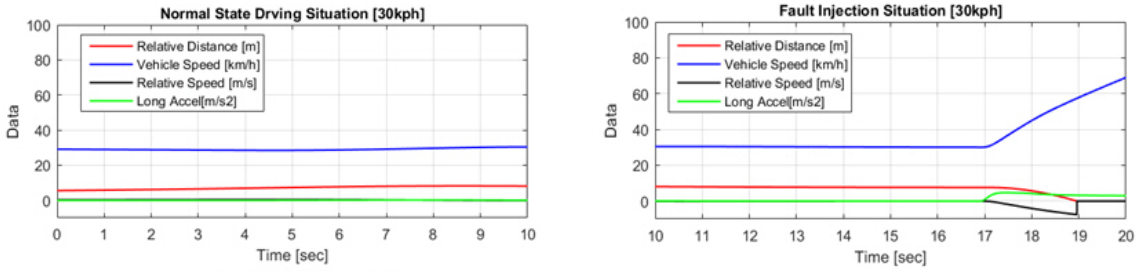
종방향 오류에 해당되는 항목 중 의도치 않은 가속(H1)에 대하여 오류 주입 시험을 수행하였다. 의도치 않은 가속에 대한 오류 주입 시험의 결과는 아래 <Table 10>과 같다. STPA 수행을 통해 선정된 변수들에 오류를 주입한 결과 D_Spd, Hor_Ang 외 모든 경우에서 기능에 대한 오작동이 발생하였다. <Table 10>의 차량 속도가 30km/h, 60km/h인 경우 원래의 설정된 속도는 100km/h로 주행인 상황이며 전방 차량의 속도에 Time gap 1s 의 차간 거리를 유지하다가 오작동이 발생되는 경우를 시험하였다. 100km/h인 경우 원래의 설정 속도는 130km/h로 주행 중 100km/h로 달리는 전방 차량을 Time gap 1s로 추종하는 시나리오이다.

<Table 10> Unintended acceleration simulation result (H1)

Speed	Injection Fault	Fault Occurrence	Collision Time	Collision Speed	Max Long. Accel
30km/h	A_x (Max)	O	2.5s	65km/h	4.7m/s^2
	D_Long (Max)	O	2.56s	55.3km/h	4.46m/s^2
	D_Spd (Max)	X	-	-	-
	Hor_Ang (Min or Max)	X	-	-	-
	V_Set_CC (Max)	O	(Single Driving)	-	4.48m/s^2
60km/h	A_x (Max)	O	4.0s	92.6km/h	2.1m/s^2
	D_Long (Max)	O	4.96s	86.3km/h	1.2m/s^2
	D_Spd (Max)	X	-	-	-
	Hor_Ang (Min or Max)	X	-	-	-
	V_Set_CC (Max)	O	(Single Driving)	-	2.2m/s^2
100km/h	A_x (Max)	O	7.27s	135km/h	1.29m/s^2
	D_Long (Max)	O	6.07s	127km/h	1.29m/s^2
	D_Spd (Max)	X	-	-	-
	Hor_Ang (Min or Max)	X	-	-	-
	V_Set_CC (Max)	O	(Single Driving)	-	2.0m/s^2

의도치 않은 가속에 대한 시나리오 결과 제어기의 출력 값인 A_x와 입력 값인 D_Long 값 각각의 Max 값을 입력한 결과 의도치 않은 가속이 발생하였으며 저속에서의 가속도가 높게 나온 것을 확인할 수 있었다.

아래 <Fig. 4>는 정상 주행 상태와 A_x Max 값 입력을 통한 Fault 상황을 비교한 그래프이다. 17초 경 Fault가 주입되어 차량이 가속하였고 약 19초에 충돌이 발생하였다. STPA 분석을 통해 도출된 D_Spd 변수는 오류 주입 결과 의도치 않은 가속이 일어나지는 않았다. 이는 D_Spd 변수 단독 오류 발생으로는 차량의 오작동이 발생하지 않음을 추측할 수 있다. 또한 전방 Object의 횡방향 위치를 판단하는 수평 각(Hor_Ang)은 ±7 (deg)로 좁은 영역이기 때문에 Time gap 1초의 차간 거리에서는 Min / Max 값을 주입해도 전방에 차량이 있는 것으로 인식하여 의도치 않은 가속이 일어나지 않았다. Time gap 2초의 경우 의도치 않은 가속이 일어났지만 전방 차량과의 상대거리가 줄어들면서 전방 차량을 인식하고 설정된 속도로 다시 감속하여 주행하는 결과를 확인하였다. 마지막으로 운전자가 설정하는 항속 속도 V_Set_CC 값에 오류를 주입한 결과 단독 주행 상황에서는 차량이 의도치 않은 가속이 발생하는 것을 확인하였다.



<Fig. 4> Comparison of normal state and unintended acceleration state

3. 횡방향 오류 주입 시뮬레이션 결과

횡방향 오류에 해당되는 의도치 않은 조향(H5)에 대하여 오류 주입 시험을 수행하였다. 제어기의 출력 값에 대한 오류 주입 시간은 100ms 단위로 올리면서 차로이탈 까지 걸리는 시간과 최대 횡 가속도를 측정하였다. 의도치 않은 조향에 대한 시뮬레이션 결과는 아래 <Table 11>과 같다. 시뮬레이션을 진행한 곡선로는 350m의 곡선반지름과 좌측 방향으로 선회하는 방향으로 설정되어있으며 100km/h의 속도로 주행 중 STPA 분석으로 도출된 변수에 오류를 주입하여 시뮬레이션을 진행하였다.

<Table 11> Unintended steering simulation result (H5)

Speed	Radius	Injection Fault	Fault Occurrence	Departure Time	Max Lat. Accel
100km/h	350m	Steering Wheel Angle (Min, Max)	O	Max: 0.85s after 300ms Injection Min: 0.76s after 200ms Injection	Min: 1.98m/s^2 Max: 5.79m/s^2
		Steering Wheel Angle (0)	O	1.08s	-
		Lateral Offset (Min, Max)	O	Min: 0.75s after 300ms Injection Max: 0.76s after 200ms Injection	Min: 3.37m/s^2 Max: 5.88m/s^2
		Curvature (Min, Max)	O	Min, Max: No Departure	-
	∞	Steering Wheel Angle (Min or Max)	O	0.56s after 300ms Injection	5.44m/s^2
		Lateral Offset (Min or Max)	O	0.61s after 200ms Injection	4.33m/s^2
		Curvature (Min, Max)	O	Min, Max: No Departure	-

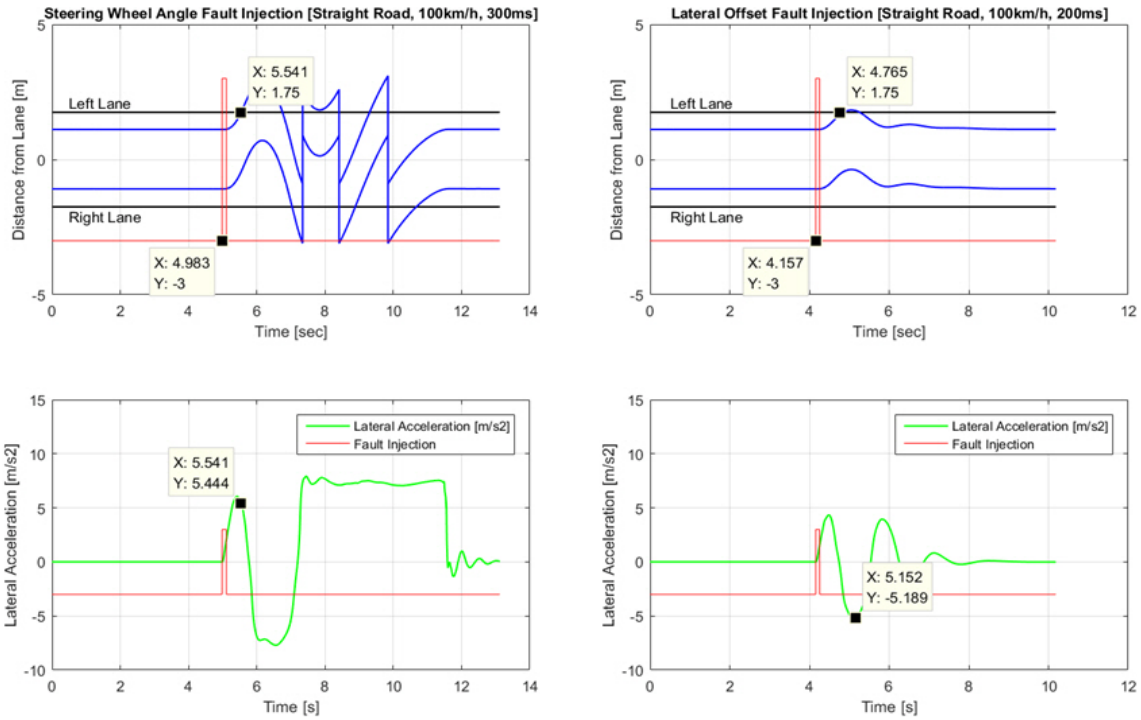
350R의 곡선반경에서 제어기의 출력 값인 Steering Wheel Angle 값에 대하여 오류를 주입한 결과 Max 값을 300ms 동안 주입 시 약 0.85s 후 차선을 이탈하였다. 시뮬레이션을 수행하는 도로 환경은 좌측으로 선회하는 형태의 곡선로이다. 따라서 좌측 선회 중 우측으로 진행되는 의도치 않은 조향의 경우가 좌측으로 진행되는 의도치 않은 조향의 경우보다 더 빠른 시간 내에 차선을 이탈하였다.

곡선로 주행 중 조향제어 미수행의 경우 오류 주입 후 약 1.08s 지난 시점에 차선을 이탈하였다. 제어기의 입력 값인 Later Offset의 경우 좌측으로 선회하는 도로 환경으로 인해 방향에 따라 차선 이탈 시간이 달라졌다. Curvature 값의 Min/Max인 경우 차선을 이탈하지는 않았지만 차로의 한쪽 방향으로 치우친 상태로 주행하는 결과가 나타났다.

직선로 상황에서는 오류 주입 변수의 Min, Max 값이 방향만 다르므로 Min, Max 값 별 차선 이탈시간은 같다. Steering Wheel Angle의 경우 300ms 동안 오류를 주입 시 약 0.56s 후 차선을 이탈하였다. Lateral Offset

의 경우 200ms 동안 오류 주입 시 0.61s 후 차선을 이탈하였으며 Curvature 값의 경우에는 곡선로에서의 결과처럼 차선은 이탈하지 않았지만 한쪽 방향으로 치우친 상태로 주행하는 결과가 나타났다.

아래 <Fig. 5>는 횡방향 오류 주입 시험의 결과 중 직선로 상황에서 Steering Wheel Angle 값과 Lateral Offset 값에 오류를 주입한 결과를 나타낸다. 그래프에서 검은색 선은 차선의 위치를 나타내며 파란색 선은 차선 내의 차량의 궤적을, 빨간색 선은 오류가 주입된 시점을 나타내고, 녹색 선은 차량의 횡 가속도를 나타낸다.

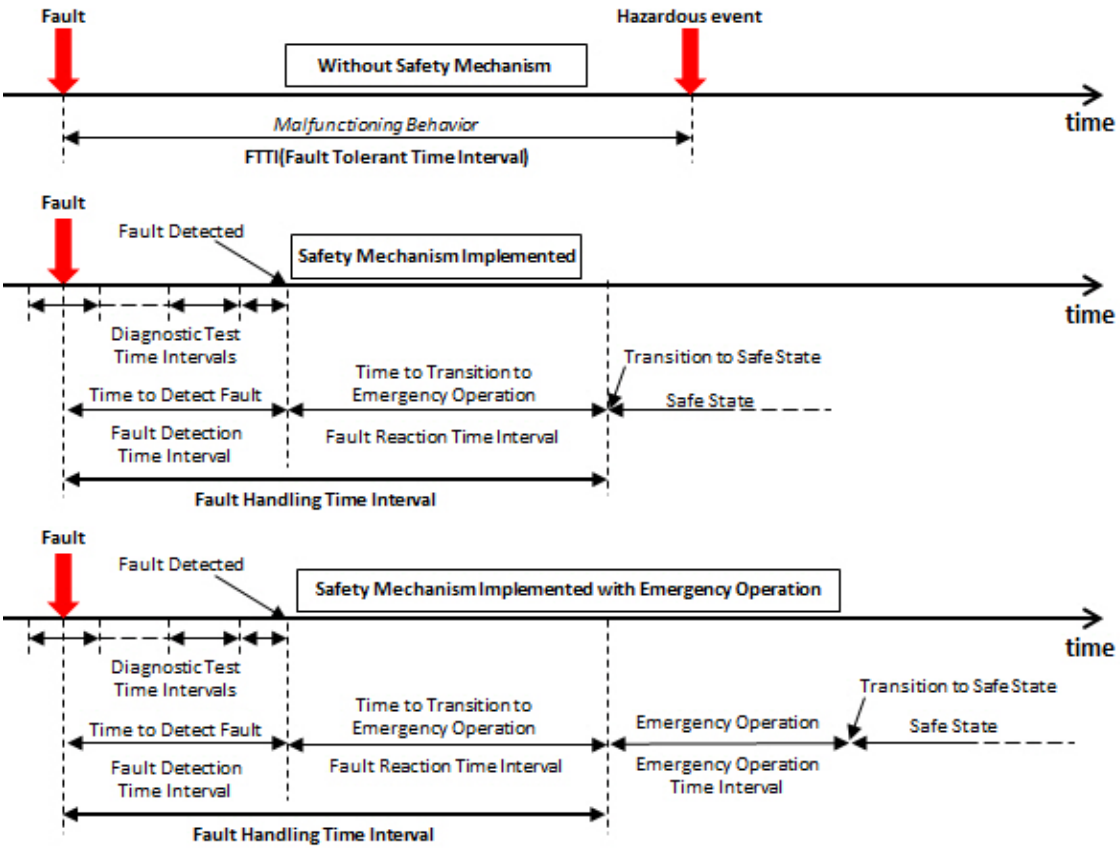


<Fig. 5> Unintended steering simulation in straight road

Ⅵ. 고찰

STPA에서 도출된 Causal Factor를 바탕으로 한 종방향 및 횡방향 오류주입 시뮬레이션 결과 자율주행자동차의 오작동으로 정의한 사항들이 나타났다. 하지만, 오작동 발생 여부가 중요한 것이 아니라 오작동이 발생되었을 때 자율주행자동차는 해당 오류를 검지하여 안전한 주행을 보장해야하는 것이 더욱 중요하다.

최근 개정된 ISO-26262 2판(ISO26262-1 2nd Edition)에서는 차량의 안전조치 시간에 대한 개념을 아래 <Fig. 6>과 같이 설명하였다. 안전 메커니즘이 없는 경우에는 오류로 인한 Malfunction 발생부터 위험(Hazard)이 발생하는 시간 까지를 Fault Tolerant Time interval(이하 FTTI)이라고 정의하고 있다. 안전 메커니즘이 적용된 경우는 오류 발생부터 오류를 감지하기 까지 걸리는 시간인 Fault Detection Time Interval과 오류를 조치하는 Fault Reaction Time Interval(이하 FRTI)이 포함되어 있으며 FRTI이후에 안전한 상태로 전환되거나 Emergency Operation(비상 동작)이 수행 후 Safe State로 전환된다.



<Fig. 6> Safety relevant time intervals(ISO-26262 2nd Edition Part1)

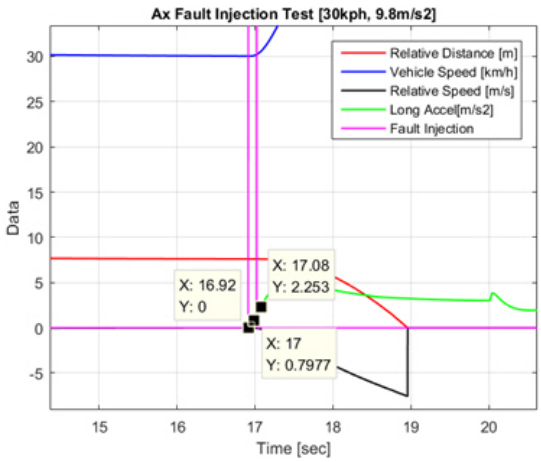
SAE 기준 Level3 이상의 자율주행자동차는 운전자가 전방주시 의무가 없기 때문에 오작동 상황에서의 Controllability는 모두 C3 등급으로 판단하는 것이 일반적이다. 아래 <Table 12>의 Controllability의 클래스 별 차량의 변수 범위를 살펴보면(Daniel Wanner et al., 2014) Q_z(차량의 안정성 변수)는 차량의 정상적인 Yaw rate 값과 오류 상황에서의 Yaw rate 값의 평균값을 더한 값으로 판단하였고, Q_y(차선 유지 변수), Q_x(충돌 회피 변수)의 기준을 바탕으로 Controllability의 산정 기준을 작성하였다.

<Table 12> Controllability class definition of the three indices

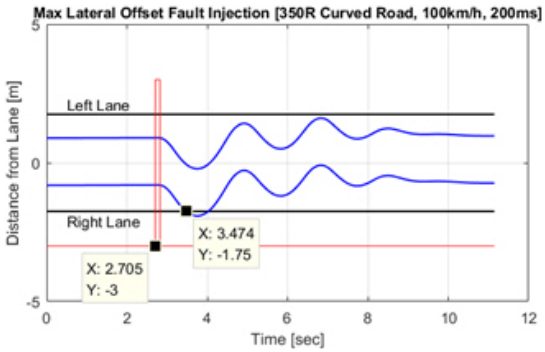
Controllability classes	C0	C1	C2	C3
Qz [°/s²]	< 2	2 - 3.5	3.5 - 5	> 5
Qy [s]	> 5	5 - 3	3 - 2	< 2
Qx [m/s²]	< 0.8	0.8 - 2.25	2.25 - 3	> 3

본 논문에서 수행된 종방향 오류 주입 시뮬레이션 결과 중에 저속 상황인 30km/h 상황에서 A_x(max), D_Long(Max) 오류 주입 시 종방향 가속도가 약 4.7m/s2이 발생되어 <Table 12>의 Q_x(충돌 회피 변수) 기준으로 C3에 해당 되는 것을 알 수 있다. 시스템의 오작동 발생 시 Controllability 등급을 C0-C1 수준으로 제한하

기 위해서는 아래 <Fig. 7>에서와 같이 오류 주입 후 0.08s ~ 0.16s 이내에 안전 조치를 통해 Safe State에 도달하여 가속을 억제하고 안전한 상태를 유지해야 한다.



<Fig. 7> Unintended acceleration simulation



<Fig. 8> Unintended steering simulation

또한, 본 논문에서 수행된 횡방향 오류 주입 시뮬레이션 중 Steering Wheel Angle 및 Lateral Offset 변수에 오류 주입을 수행한 결과를 보면 차선 이탈 시간이 1s 이내의 짧은 시간으로 <Table 12>의 Q_y(차선 유지 변수) 기준으로 C3에 해당되었다. 두 변수의 오류 주입 시 곡선로와 직선로에서 200ms~300ms 동안의 오류 주입에 차선이 이탈시간이 가장 짧은 경우는 0.56s 수준으로 매우 짧은 시간임을 알 수 있다. 횡방향 오류로 인한 차선 이탈을 방지하기 위해서는 적어도 오류 지속시간인 200ms 이전에 제어기가 오류를 감지 및 판단을 통해 안전 조치를 수행하여 Safe State에 도달하여 안전한 주행을 수행하도록 해야 한다.

Ⅶ. 결론 및 향후 연구

본 논문에서는 STPA 기법을 이용하여 자율주행자동차의 안전성 평가를 위한 종방향 및 횡방향 오류 주입 시나리오에 대한 연구를 수행하였다. 자율주행시스템의 Control Structure를 기반으로 제어기의 입출력 변수를 기반으로 오류 주입에 대한 시나리오를 구성하여 자율주행자동차의 5개의 주요 Hazard에 대한 오류주입 시나리오를 도출하였으며, 도출된 시나리오 중 자율주행자동차의 의도치 않은 가속 및 의도치 않은 조향 시나리오의 시뮬레이션을 통해 실제 오류 발생 여부 확인과 함께 안전 조치 시간에 대하여 연구하였다.

의도치 않은 가속의 경우 제어기의 출력 값인 A_x 값과 입력 값인 D_Long 값에 오류를 주입하여 오작동 발생 여부를 확인하였고, 이를 통해 Controllability를 C0-C1 수준으로 낮추기 위해서는 안전 조치 시간을 0.16초 이내에 의도치 않은 가속을 차단하고 Safe state에 도달하여 안전한 주행을 수행해야 함을 확인하였다.

의도치 않은 조향의 경우 제어기의 출력 값인 Steering Wheel Angle과 입력 값인 Curvature와 Lateral Offset 값에 오류를 주입하여 오작동 발생 여부를 확인하였고, 오류 주입 시 차선 이탈 시간을 도출하여 안전 조치 시간을 200ms 이내에 의도치 않은 조향을 차단하고 Safe state에 도달하여 안전한 주행을 수행해야 함을 확인하였다.

본 논문에서는 STPA를 통해 도출된 모든 경우의 시나리오를 바탕으로 시뮬레이션 진행을 수행하지 못하였지만, 향후 각 변수 별 오류 주입을 통한 오작동 여부 및 다양한 속도와 속도에 맞는 설계 곡률 별 시뮬레이션을 통한 안전 조치 시간을 연구할 예정이다.

ACKNOWLEDGEMENTS

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(18TLRP-B117133-03)으로 수행된 연구임.

REFERENCES

Chae H. S., Jeong Y. H., Yi K. S., Choi I. S. and Min K. C.(2016), "Safety Performance Evaluation Scenarios for Extraordinary Service Permission of Autonomous Vehicle," *Transactions of KSAE*, vol. 24, no. 5, pp.495-503.

Chu K. Y., Han J. H., Lee M. C., Kim D. C. and Sunwoo M. H.(2011), "Development of an Autonomous Vehicle: AI," *Transactions of KSAE*, vol. 19, no. 4, pp.146-154.

Hwang J. G., Jo H. J., Han C. H., Cho W. S., Ahn J. and Ha D. M.(2010), "A Study on the Hazop-KR for Hazard Analysis of Train Control Systems," *Journal of the Korean Society for Railway*, vol. 13, no. 4, pp.396-403.

ISO-22179(2009), *Intelligent transport systems - Full speed range adaptive cruise control(FSRA) systems - Performance requirements and test procedures*.

ISO-26262-1, "Road vehicles - Functional safety - Part 1: Vocabulary," 2018, 12.

J3016(2016), *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*.

Kang M. W., Son B. S., Dho C. U. and Kang J. K.(2002), "Development of Accident Prediction Models at Freeway Curve Section Based on Geometric Characteristics," *Journal of the Korean Society of Civil Engineers*, vol. 22, no. 6D, pp.1077-1088.

Kim D. Y., Lim J. H., Lee H. K., Choi I. S., Shin J. K., Hong Y. S. and Park K. H.(2017), "Development of Fault Injection Simulation Environment for ADAS Systems and Cases Studies of Fail-Safety Evaluation," *Transaction of KSAE*, vol. 25, no. 6, pp.767-777.

Wanner D., Drugge L. and Trigell A. S.(2017), "Fault Classification Method for the Driving Safety of Electrified Vehicles," *International Journal of Vehicle Mechanics and Mobility*, vol. 52, no. 5, pp.704-732.

Yang H. S. and Kwon G. H.(2017), "STAMP/STPA applied train software safety analysis case study," *Korea Software Conference Proceeding*, pp.607-609.