교차로 시나리오 기반 V2X를 활용한 자율주행차량의 위험성 분석 및 고장안전성 검증 연구

A Study on the Risk Analysis and Fail-safe Verification of Autonomous Vehicles Using V2X Based on Intersection Scenarios

백 윤 석* · 신 성 근** · 박 종 기*** · 이 혁 기**** · 엄 성 욱***** · 조 성 우****** · 신 재 곤*******

* 주저자 및 교신저자 : 한국자동차연구원 ICT융합연구센터 선임연구원
** 공저자 : 한국자동차연구원 ICT융합연구센터 선임연구원
*** 공저자 : 한국자동차연구원 ICT융합연구센터 연구원
**** 공저자 : 한국자동차연구원 ICT융합연구센터 센터장
***** 공저자 : 한국교통안전공단 자동차안전연구원 자율주행실 선임연구원
****** 공저자 : 한국교통안전공단 자동차안전연구원 자율주행실 실장
******* 공저자 : 한국교통안전공단 자동차안전연구원 자율주행실 수석위원

Yunseok, Baek* · Seong-Geun Shin* · Jong-ki Park* · Hyuck-Kee Lee* · Sung-wook Eom** · Seong-woo Cho** · Jae-kon Shin**

* ICT Convergence R&D Center, Korea Automotive Technology Institute
** AutomatedVehicle Division, Korea Automobile Testing & Research Institute, Korea Transportation Safety Authority

† Corresponding author : Yunseok Baek, ysbaek@katech.re.kr

Vol.20 No.6(2021)
December, 2021
pp.299~312

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2021.20.6.299

Received 12 November 2021
Revised 22 November 2021
Accepted 7 December 2021

요 약

V2X를 활용한 자율주행차량은 기존의 자율주행차량보다 더욱 많은 정보를 바탕으로 자율주행차량의 센서 커버리지 밖의 영역의 정보를 통하여 안전한 주행이 가능하다. V2X 기술이 자율주행차량의 핵심 구성 요소로 부각되면서 V2X 보안 문제에 대해 연구가 활발히 진행되고 있지만 자율주행차량이 V2X의 의존도가 높은 자율주행시스템에서 V2X 통신의 고장으로 인한 위험성에 대한 부분은 상대적으로 부각되고 있지 않으며 관련 연구도 미진한 편이다. 본 논문에서는 자율주행차량의 교차로 시나리오를 제시하여 V2X를 활용한 자율주행시스템의 서비스 시나리오를 정의 하였으며 이를 기반으로 기능을 도출하고 V2X의 위험 요인을 분석하여 오작동을 정의하였다. ISO26262 Part3 프로세스를 활용하여 HARA 및 고장 주입 시나리오의 시뮬레이션을 통해 V2X 모듈의 고장으로 인한 위험성과 이를 확인하는 검증 과정을 제시하였다.

핵심어 : V2X, 신호 교차로, 위험성 분석, 안전성 검증, 고장 주입

ABSTRACT

Autonomous vehicles using V2X can drive safely information on areas outside the sensor coverage of autonomous vehicles conventional autonomous vehicles. As V2X technology has emerged as a key component of autonomous vehicles, research on V2X security is actively underway research on risk analysis due to failure of V2X communication is insufficient. In this paper, the service scenario and function of autonomous driving system V2X were derived by presenting the intersection scenario

of the autonomous vehicle, the malfunction was defined by analyzing the hazard of V2X. he ISO26262 Part3 process was used to analyze the risk of malfunction of autonomous vehicle V2X. In addition, a fault injection scenario was presented to verify the fail-safe of the simulation-based intersection scenario.

Key words : V2X, Intersection, HARA, Fail-safe verification, Fault Injection

Ⅰ. 서 론

1. 개요

교차로 도심로에서 자율주행차량이 운행되기 위해서는 카메라, 라이다 (Lidar) 및 레이더 (Radar) 등의 센서를 통해 신호등, 전방의 객체 등을 검출하여 현시 정보에 따른 주행을 판단한다. 교차로와 같은 혼합류 도심 환경에서는 각종 도로시설물, 주정차 차량 등이 혼재하며 사각지대가 발생하여 차량 센서만으로는 위험상황을 인지하기 어려움이 있다. 특히 미국의 자동차 통계조사 기관인 DMV에 보고된 자료를 보면, 66건 중 58건이 교차로에서 발생하였고 자율주행차량 전체 사고의 88%로 교차로 사고 비율이 높음을 알 수 있다. (Grembek et al., 2018) 이를 보완하기 위해 V2X (Vehicle to everything) 통신 시스템을 적용하여 차량과 차량 (V2V, Vehicle to Vehicle) 및 차량과 인프라 (V2I, Venice to Infrastructure) 등으로 주변 차량, 신호등과 같은 교통 인프라와 소통이 가능해지고 교통 효율, 연비 개선 및 안전을 위한 기술들이 개발되어 지고 있다. 또한 V2X를 활용한 자율주행차량은 일반 자율주행차량보다 더욱 많은 정보를 바탕으로 자율주행차량의 센서 커버리지 밖의 영역에 대해 긴급 상황, 공사 구간 정보, 정제 구간 정보 및 신호등 정보 등을 통해 안전한 주행이 가능해졌다.(Ahn et al., 2019)

V2X 기술이 자율주행차량의 핵심 구성 요소로 부각되면서 V2X 보안 문제에 대해 연구가 활발히 진행되고 있다. 차량 네트워크에서 보안과 프라이버시 (신원 및 공개 키 기반 암호화 등)에 사용되는 다양한 기법에 대한 연구가 진행되고 (Biswas et al., 2010) V2X 통신의 다양한 공격과 보안 방식을 연구하고 (Karagiannis et al., 2011) 보안을 보장하기 위해 다양한 접근 방식을 분류하지만 (Amrita and Mauro, 2019; Weise, 2011) 자율주행차량이 V2X의 의존도가 높은 자율주행시스템에서 V2X 통신 모듈의 고장으로 인한 위험성 문제에 대해 연구가 미진하다.

V2X의 의존도가 높은 자율주행시스템에서 V2X 고장으로 활용할 수 없는 경우 교차로 도심로에서 기존의 위험이 그대로 노출될 수 있고 잘못된 정보 혹은 정보의 미제공 등의 V2X 기능 오작동으로 인한 잠재적 위험이 존재할 수 있다. 따라서 고장 시 발생할 수 있는 위험 요인 분석과 시스템의 위험성 평가에 대한 연구가 수행되어야 한다.

본 논문에서는 자율주행차량의 교차로 시나리오를 제시하여 V2X를 활용한 자율주행시스템의 서비스 시나리오를 정의 하였으며 이를 기반으로 기능을 도출하고 V2X의 위험 요인을 분석하여 오작동을 정의하였다. ISO26262 Part3 프로세스를 활용하여 HARA 및 고장 주입 시나리오의 시뮬레이션을 통해 V2X 모듈의 고장으로 인한 위험성과 이를 확인하는 검증 과정을 제시하였다.

Ⅱ. 신호 교차로 시나리오 정의

1. 대상 차량 정의

자율주행차량이란 운전자의 개입 없이 주변 환경을 인식하고 주행 상황을 판단하여 차량을 제어함으로써 스스로 주어진 목적지까지 주행하는 차량을 말하며, 본 연구에서는 모든 상황을 대처할 수 있는 차량이 아닌 센서와 V2X의 동일한 정보가 가졌을 때 V2X 통신을 고의존한다고 가정하여 Lv.4 수준의 자율주행시스템을 정의하였다.

충돌회피시스템은 환경 센서를 통해 감지된 정보를 기반으로 충돌 위험을 감지하여 사고를 방지하기 위한 경고를 제공하거나 능동적인 조치를 수행하는 시스템으로 충돌 위험도를 판단하였다. 충돌 위험도를 판단을 통해 예측되는 충돌 상황의 충돌 회피 가능성을 판단하여 이에 대한 적절한 조치를 수행함으로써 충돌을 완벽히 회피하거나 충돌을 회피할 수 없는 경우에는 경감을 위한 조치를 결정할 수 있다. 이러한 조치로는 제동이 가장 일반적인이며, 자동 조향을 통해서도 충돌을 회피할 수 있다. 기존 연구에서 다양한 주행 상황에서 충돌 위험도를 정확하게 산출하기 위한 알고리즘이 제안되었다. (Ararat et al., 2006; Lee and Peng, 2005)

이 중에서도 대상 차량과 전방 오브젝트와의 상대 거리와 속도를 주요 인자로 사용하여 시간 관점에서 충돌 위험도를 판단하는 방법이 일반적이다. 시간 관점에서 충돌 위험도를 판단하기 위한 대표적인 방법은 THW (Time HeadWay)와 TTC (Time-To-Collision)이고 본 논문에서는 TTC를 통하여 충돌 위험도를 판단하였다. TTC는 대상 차량과 전반 차량 도는 장애물과의 충돌이 발생하기까지 남은 시간을 나타내는 파라미터로써 TTC 값이 작은 경우 충돌이 임박한 높은 위험 상황을 의미한다.

$$TTC = \frac{d_{rf}}{v_r} \quad \cdots\cdots (1)$$

여기서 v_r은 충돌 대상과의 종방향 상대 속도이며 d_{rf}은 종방향 상대거리이다. 현재 차량이 완전히 정지시키기 위한 소요시간이 TTC 보다 큰 경우에는 제동을 통해 충돌 회피가 가능하지만 TTC보다 작을 경우에는 제동만으로는 충돌을 회피할 수 없다.

센서의 한계를 극복하기 위한 방안으로 기존의 충돌회피시스템이 동작하기 어려운 상황을 V2X 통신을 활용한 자율주행시스템으로 보완하는 형태로 구성되었다. LV.4 수준의 자율주행시스템은 V2X 통신을 활용하여 전방의 신호 정보 (SPaT, Signal Phase And Timing) 및 이동체 정보 (BSM, Basic Safety Message / PVD, Probe Vehicle Data / RSA, Road Side Alert) 등을 제공받아 신호 교차로를 주행할 때 자율주행시스템에서 판단, 제어 및 명령함을 가정하였다. 신호 정보 (SPaT)는 실시간 신호 정보를 전달받아 현재 신호 그리고 다음 신호와 남은 시간을 기반으로 자율주행시스템에서 주행 여부를 판단, 제어 및 명령을 하고 충돌 위험 정보 (RSA)는 충돌 위험 정보를 전달받아 사고를 회피할 수 있도록 자율주행시스템에서 주행 여부를 판단, 제어 및 명령을 하며 기본 안전 메시지 (BSM)는 주변 차량의 위치를 기반으로 교차로까지의 TTC (Time To Collision)를 판단하여 사고를 회피할 수 있도록 자율주행시스템에서 주행 여부를 판단, 제어 및 명령함을 가정하였다.

2. 신호 교차로 상충회피 시나리오 정의

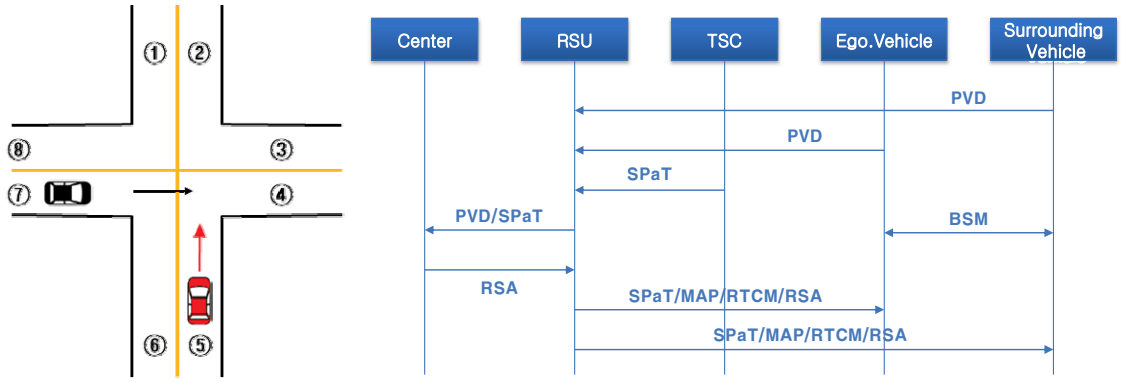
도심로는 자율주행을 하기에 매우 어려운 구간과 상황이 많이 존재한다. 빌딩숲 및 고가 도로 등의 영향

으로 음영구간이 존재하고 시시각각 변화하는 공사구간이 존재하며 차도로 갑자기 통행하는 보행자, 차량의 사각지대에서 출현하는 차량, 딜레마존이 존재하는 교차로 등으로 자율주행시스템의 즉각적인 대처가 어렵다.

그 중 사고 위험이 높고 운행 중 노출 빈도가 높은 도심지의 신호 교차로를 주행하는 상황을 제시하였으며 교차로에 진출입하는 모두 차량은 V2X를 활용한 자율주행차량이고 도로 밖은 빌딩숲으로 센서로 다른 차선의 주변을 감지할 수 없지만 V2X 통신을 통해 차량간 OBU (On Board Unit) 통신 (V2V, Vehicle-to-Vehicle)을 하며 신호 정보는 RSU (Road Side Unit) 통신 (V2I, Vehicle-to-Infra)을 통해 전달하여 차량간 상충 회피하는 신호 교차로 시나리오 및 사각지대 충돌 위험 교차로 시나리오를 선정하였다.

신호 교차로 시나리오의 프로세스는 다음과 같다.

1. 교차로 (⑤)에서 교차로 (②)로 직진하려는 자차가 교차로에 진입
2. 교차로 내 위치한 자차를 포함한 주변 차량에 BSM을 전송하며 OBU는 수신하고 PVD를 전송하며 RSU는 수신
3. TSC에서는 실시간 신호운영 정보를 RSU로 송신
4. RSU는 PVD 정보 및 신호 정보를 센터에 전달
5. 센터는 위험상황을 검지하고 충돌을 판단하는 충돌 알고리즘은 수신된 지도 정보, 차량 위치 및 속도 정보 등으로 TTC (Time To Collision)을 계산하여 충돌 위험 발생시 RSA 메시지를 생성하여 RSU에 제공
6. RSU는 RSA를 수신하고 SPaT/MAP/RTCM/RSA를 자차를 포함한 주변 차량에 전송
7. 자차는 RSU로부터 수신된 정보를 통해 주행 속도 등을 판단, 제어 및 명령하여 상충 회피



<Fig. 1> The intersection scenario and the service scenario procedure

3. V2X 메시지셋 정의

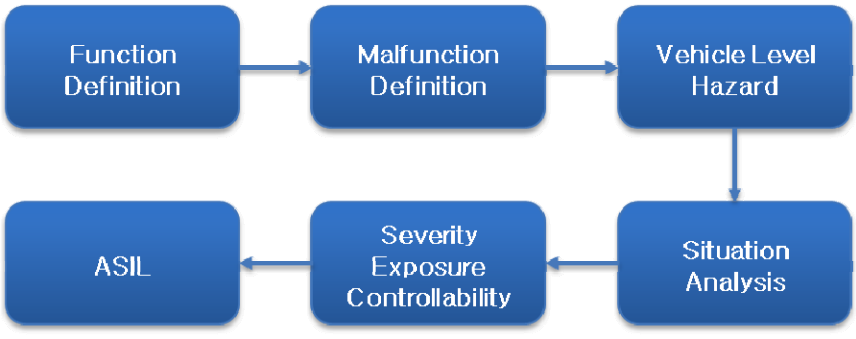
미국자동차기술협회 SAE J2735 표준을 기반으로 메시지 셋을 분석하면 메시지의 종류에 따라 V2V와 V2I의 기능 구분이 가능하며, V2V 메시지의 경우 차량 상태 정보 위주이고 V2I 메시지의 경우 주변 상황 정보를 포함한다. (SAE, 2016) V2V와 V2I 메시지 간의 동일/유사한 정보를 가지는 경우도 있으며, 어느 메시지의 고장 상황에 따라 위험도 분석이 달라질 수 있다. 아래 표에 메시지 셋과 V2X와의 관계를 정의하였다.

<Table 1> The definition of Message set

Message Set	Description	V2V	V2I	I2V
Basic Safety Message (BSM)	Safety data related to vehicle status information	O		
Map Data	Conveying different types of geographic road information			O
Signal Phase And Timing (SPAT)	Conveys the current status of one or more signal intersections			O
Emergency Vehicle Alert (EVA)	Sending a warning message that caution is required in case of an accident with a nearby vehicle	O		
Probe Vehicle Data (PVD)	Used to exchange vehicle status with other segment (typically RSU) DSRC units to gather information about general vehicle driving behavior along road segments.		O	
Road Side Alert (RSA)	Alerts users to surrounding dangers			O
RTCM corrections (RTCM)	Messages related to the Radio Technical Committee (RTCM) standard for maritime services			O
Signal Request Message (SRM)	Messages sent by DSCR-equipped equipment to the RSU at a signal intersection			O
Traveler Information Message (TIM)	This message is used for communication between the roadside base station and the vehicle, and includes information such as the condition of the surrounding road (construction, cleaning, advertisement), and is a message used when the roadside base station informs the adjacent vehicle terminal of the condition of the surrounding road.			O

Ⅲ. 오작동 정의 및 차량 수준 위험원 도출

ISO26262 Part3 프로세스를 활용한 HARA (Hazard Analysis and Risk Assessment) 방법은 기능에 대한 정의와 오작동, 차량 수준의 위험원을 도출하고 Situation Analysis를 통해 어떤 주행 환경에서 위험원이 도출되는지 분석하고 최종적으로 자동차 안전 무결성 수준인 ASIL (Automotive Safety Integrity Level)을 결정한다.



<Fig. 2> HARA Process

본 장에서는 ISO26262 Part3 Concept Phase 프로세스를 활용하여 V2X 통신 기반의 자율주행차량의 신호교차로 상충회피 시나리오에 대한 기능을 정의하고 No or Not, Incorrect, More, Less 등과 같은 가이드워드를

기반으로 시스템의 여러 상태와 결합되어 설계 의도에서 벗어날 수 있는 이상 현상들을 식별하여 위험원의 발생을 찾게 되는 개념인 HAZOP 기법을 활용하여 오작동을 도출하였다.

1. 신호 교차로 상충회피 시나리오에 대한 기능 정의

신호 교차로 상충회피 시나리오를 통해 V2X의 기능을 다음 표와 같이 정의하였다.

<Table 2> The Definition of V2X Function Based on Intersection Scenario

Service	Function	Description
Cooperative Intersection Control Service	[F001] Providing signal information for collision avoidance	Providing signal information (SPaT) to avoid collisions with vehicles using signal intersections
	[F002] Providing collision risk information in blind spots	When entering an intersection with a blind spot, the center provides collision risk information (RSA) with other vehicles using the intersection to surrounding vehicles including the ego-vehicle.

2. 신호 교차로 상충회피 시나리오에 대한 기능의 오작동 정의

오작동 정의는 HAZOP 기법을 활용하였으며 도출한 기능 중 주요 위험원을 내포하고 있는 기능에 대한 오작동 도출을 수행하였다. HAZOP의 Guide words 중 미수행을 의미하는 No or Not 과 오수행 및 잘못된 수행을 의미하는 Incorrect를 이용하여 아래 표와 같이 주요 오작동을 도출하였다.

<Table 3> The Definition of V2X Malfunction Based on Intersection Scenario

Malfunction	Hazard	Description
[MF01] Not provided signal information for collision avoidance	-	Collision avoidance is possible by avoiding collisions with nearby vehicles from V2V BSM messages (vehicle status information) even if I2V signal information is not provided while driving at a constant speed at an intersection with city signals in clear weather
[MF02] Incorrectly provided signal information for collision avoidance	Side impact hazard	When driving at a constant speed at a city intersection in clear weather, the red light signal is incorrectly provided as a green light signal as an SPaT message (signal information), and after entering the intersection at a constant speed instead of stopping, the safety system of the autonomous vehicle and V2V BSM message (vehicle status information) to avoid collision with surrounding vehicles, but collided with slow deceleration
[MF03] Not provided with collision risk information in blind spots	Side impact hazard	When a vehicle with a risk of collision from another direction within the intersection does not provide collision risk information when approaching, after entering the intersection, the autonomous vehicle safety system and V2V BSM message (vehicle status information) avoid collision with nearby vehicles, but due to slow deceleration crashed
[MF04] Incorrectly provided with collision risk information in blind spots	-	At an intersection with blind spots in the city in clear weather, there is no vehicle entering at a cruising speed, but an I2V RSA message (collision risk information) is delivered to decelerate unintentionally, but the autonomous driving system avoids an accident with a vehicle following from the rear

3. 고장 유형 분석

ISO 26262 및 일반 IEC 61508과 같은 기능 안전에 대한 표준을 기준으로 무선 통신에 적용할 수 있는 고장 모드를 분석하였다. ISO26262 파트 5에서 온 칩 통신 및 데이터 전송에 대한 고장 모드를 정의하였고

(ISO-26262-5, 2011) IEC 61508-2에서 무선 통신의 고장 모드를 정의하였다. (IEC 61508-2, 2010)

NHTSA를 참고하여 V2X 모듈의 송수신부 (안테나)는 잘못된 데이터 수신이나 누락, 타이밍 관련 입력이 잘못되었거나 누락으로 발생하는 외부 외란 (External disturbance), 하드웨어 고장에 따른 고장 모드를 정의하였다. 프로세서 모듈은 전원 공급부 고장, 소프트웨어 결함, 하드웨어 고장으로 고장 모드를 정의하였다. 이에 대한 위험 요인 (Casual factor)으로 전원 공급부 고장은 하이/로우/외란에 의해 발생하며, 소프트웨어 결함은 부적절한 신호 처리 알고리즘 혹은 소프트웨어 코드 생성의 결함으로 발생하고, 하드웨어 고장은 마이크로컨트롤러의 기계적 고장, 메모리 오류, 내부 타이밍 클럭 오류, 신호 변환 오류 (신호 필터)로 정리하였다. 차량 통신단의 위험 요인은 통신 버스 고장, 하드웨어 고장으로 고장 모드를 정의하였다. 이에 대한 위험 요인 (Casual factor)으로 통신 버스 고장은 버스 과부하 (overload) 혹은 버스 오류, 메시지 송수신기 고장으로 정리하였다. (Baek et al., 2020)

<Table 4> Failure mode

Component	Failure mode	Causal factor
Transceiver	External control input or information wrong or missing and external disturbance	Message Corruption
		Message delay
		Message loss
		Unintended message repetition
		Resequencing
		Insertion of message
		Incorrect addressing
		Asymmetric information
		Blocking access to a communication channel
	Hardware fault	Internal hardware failure
Processor	Hardware fault	Convert different Encoding/Deconding method
		Timing clock fault (GPS)
		Power supply off
External Interface Bus (Ethernet or CAN)	Hardware fault	Failure of the message transmitter, receiver
		Short circuit to battery voltage
		Short circuit to ground
		Broken wire

4. 고장 주입 시나리오

송수신부, 프로세서 및 인터페이스로 구분하여 고장 유형을 정의하였다. 프로세서와 인터페이스는 하드웨어의 고장 유형이 주를 이루며 고장을 주입하면 V2I와 V2V의 구분과 관계없이 미제공의 오작동 경우만 발생하여 본 연구에서는 V2X의 V2I와 V2V 메시지 셋에 대한 상호 보완 관계를 기반으로 기능의 오작동으로 인한 위험도를 분석하기 위해 송수신부 고장 요인에 대한 고장 주입 시나리오를 제시하였다.

송수신부의 고장 유형 중 하드웨어 고장에 대해서는 직접적인 고장 주입이 가능하지만 재현반복성과 시험 안전성 등의 이유로 V2X 메시지에 접적으로 고장 주입하기엔 한계가 존재하며 정상 메시지 패킷 (Packet) 혹은 헤더 (Header)에 고장을 주입하여 송신한 메시지를 수신하는 방식으로 송수신부의 고장을 모사하였다. 제시한 고장 유형을 다음과 같이 정의하여 고장을 주입하고 기능의 오작동과의 관계를 정의하였다.

1) Message Corruption

수신된 메시지가 의도치 않은 메시지가 제공된 경우로 메시지 페이로드 (Payload)에 다른 정보가 포함된 형태의 고장이다. 신호 교차로를 이용하는 차량과의 충돌 사고 회피를 위한 신호 정보 (SPaT)에서 빨간불 상태 정보를 초록불 상태 정보로 메시지를 변경하여 고장 주입을 하였으며, 사각지대가 존재하는 교차로 진입 시 교차로를 이용하는 다른 차량과의 충돌 위험 정보 (RSA)가 없지만 충돌 위험이 있다고 메시지를 변경하여 고장 주입을 하였다. 오작동 유형 중 잘못된 정보 (Incorrect) 제공의 형태이다.

2) Message Delay

수신 주기보다 늦게 메시지가 제공되는 경우로 메시지 패킷에 의도치 않은 지연이 발생하는 고장이다. 메시지 전송 주기는 10Hz이고 정해진 주기의 보다 늦게 전송하도록 지연을 설정하여 고장 주입을 하였다. 오작동 유형 중 정보 미제공 (No)의 형태이다.

3) Message Loss

메시지 손실의 경우, 수신된 메시지의 일부 혹은 전체를 손실되는 경우로 메시지 패킷 전체에 대해 신호 정보 (SPaT) 및 충돌 위험 정보 (RSA)를 수신하지 않도록 하여 고장을 주입하였다. 오작동 유형 중 정보 미제공 (No)의 형태이다.

4) Unintended message repetition

의도치 않은 메시지의 반복하는 경우로 메시지 패킷이 업데이트 되지 않고 신호 정보 (SPaT)의 이전 값이 계속하여 반복하는 형태와 다른 차량과의 충돌 위험이 없어졌지만 이전의 값인 충돌 위험이 있다는 충돌 위험 정보 (RSA)를 반복하여 고장을 주입하였다. 오작동 유형 중 잘못된 정보 (Incorrect)의 제공의 형태이다.

5) Resequencing

잘못된 시퀀스 넘버 (Sequence Number)가 포함된 메시지의 경우로 메시지 헤더 부분 중 시퀀스 넘버가 순차적이지 않게 고장을 주입하였으며 신호 정보 (SPaT)와 충돌 위험 정보 (RSA)가 미수신되어 오작동 유형 중 정보 미제공 (No)의 형태이다.

6) Insertion of message

의도치 않은 메시지가 추가되어 기존의 데이터 항목과 값이 달라지는 경우로 메시지 헤더 정보의 데이터 길이 (Length)와 실제 데이터의 길이가 맞지 않도록 고장 주입을 하였고 디코딩이 되지 않아서 신호 정보 (SPaT)와 충돌 위험 정보 (RSA)가 미제공되어 오작동 유형 중 정보 미제공 (No)의 형태이다.

7) Incorrect addressing

송수신부의 잘못된 식별인자가 전달된 경우로 메시지 헤더의 타입 (Type)을 메시지 수신을 메시지 송신으로 타입을 변경하여 고장을 주입하였다. 작동 유형 중 정보 미제공 (No)의 형태이다.

8) Asymmetric information

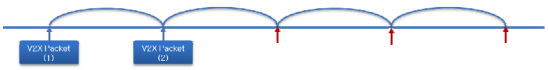
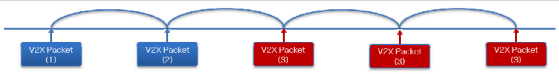
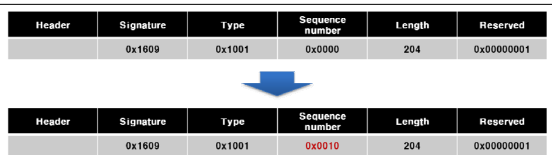
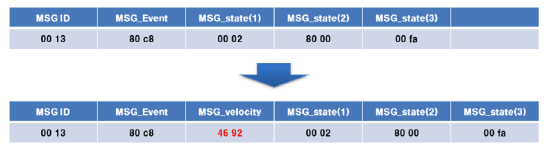
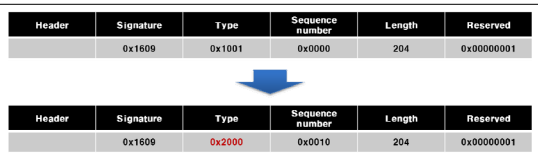
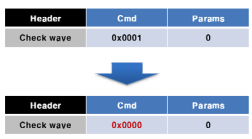
송신한 메시지와 수신한 메시지가 비대칭 형태의 경우로 송신한 메시지 헤더의 메시지 길이와 수신한 메

시지 헤더의 메시지 길이를 변경하여 고장을 주입하였고 헤더 정보와 데이터 정보가 일치하지 않아 디코딩이 되지 않아 신호 정보 (SPaT)와 충돌 위험 정보 (RSA)가 미제공되어 오작동 유형 중 정보 미제공 (No)의 형태이다.

9) Blocking access to a communication channel

통신 채널의 접근이 차단되는 경우로 동작 시퀀스 중 상태 정보 확인의 응답이 되지 않도록 고장을 주입하여 메시지셋이 송수신되지 않도록 구현하였으며 작동 유형 중 정보 미제공 (No)의 형태이다.

<Table 5> Fault injection

	Casual Factor	Fault Injection
Transceiver	Message Corruption	
	Message delay	
	Message loss	
	Unintended message repetition	
	Resequencing	
	Insertion of message	
	Incorrect addressing	
	Asymmetric information	
	Blocking access to a communication channel	

5. ASIL 산정 근거

ASIL은 상해 심각도, 노출 빈도, 제어 가능성의 등급을 조합하여 산정하였다. 상해 심각도를 나타내는 등급은 S0, S1, S2, S3로 나타내며 S0는 사고 시 상해가 없는 것을 뜻하며 S3는 생명이 위독하거나 사망에 이르는 치명적인 상해를 나타낸다. 상해 심각도를 판단하기 위해 SAE J2980 (SAE, 2015)의 속도 변화(ΔV) 별 상해 심각도 산정법을 참고하여 상해 심각도 산정을 위한 충돌 속도는 아래 식 (1)과 같다. 여기서 Δv는 충돌 차량의 속도 변화를 나타내고, m1은 충돌 차량의 질량, m2는 피충돌 차량의 질량, v1은 충돌 차량의 충돌 시 속도, v2는 피충돌 차량의 충돌 시 속도를 나타낸다. 충돌 시 반발계수 등의 조건은 고려하지 않았으며 충돌 속도 및 아래 식 (2)의 속도 변화만을 고려하였다.

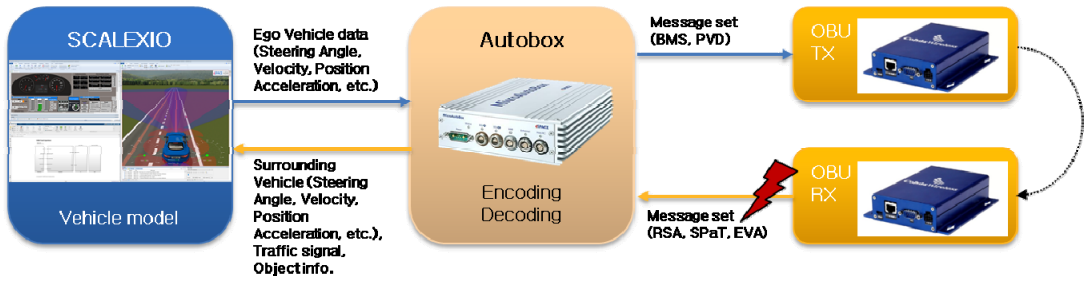
$$\triangle v = \frac{m_1}{m_1 + m_2}(v_1 - v_2) \quad \cdots\cdots (2)$$

노출 빈도 등급은 E1, E2, E3, E4로 구분되며 E1은 매우 낮은 발생 빈도를 나타내고 E4는 매우 높은 발생 빈도를 나타내며 ISO-26262 파트 3 문서 (ISO-26262 Part3, 2018)의 부록에 포함되어있는 노출 빈도 예시를 참고하였다. 제어 가능성은 오작동이 발생했을 시 제어 가능성을 나타내는 지표로 C0, C1, C2, C3로 구분되며 C0는 누구나 제어가 가능한 상태를 나타내며 C3는 제어가 불가능한 상태를 나타내며 본 논문에서는 자율주행차로 가정하여 운전자가 직접적으로 관여를 하지 않으므로 모두 C3로 산정하였다.

Ⅳ. 시뮬레이션 환경 및 결과

1. 시뮬레이션 환경

3장에서 분석한 V2X 기능의 고장을 주입하여 고장안전성을 검증하기 위한 HILS 환경 및 결과를 정리하였다. HILS 환경은 dSPACE사의 차량 모델 (ASM) 및 센서 모델, 환경 모델 등과 V2X 모듈 (OBU, RSU), 프로세서 ECU 장비 (ASN.1을 준수한 인코딩/디코딩)로 구성되며, 고장주입을 위해 Matlab/Simullink와 ControlDesk를 연동하여 송수신부의 고장을 모사하였다. 비쥬얼 시뮬레이션 기능을 수행하는 MotionDesk를 통하여 시뮬레이션 결과를 확인하였다.



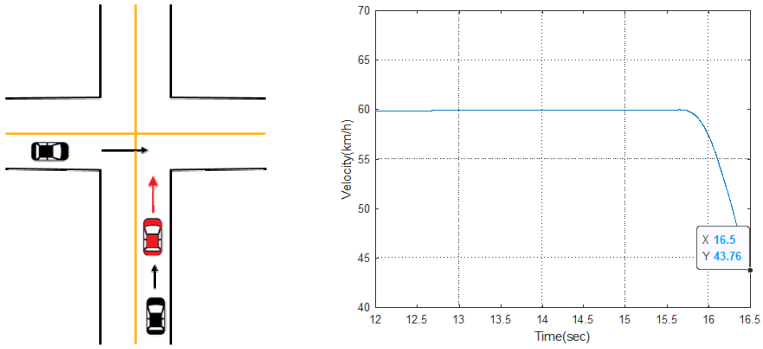
<Fig. 3> Simulation Environment

2. 시뮬레이션 결과 분석

1) 상충 회피를 위한 신호 정보 제공의 오작동 시나리오

상충 회피를 위한 신호 정보 미제공 (MF01)의 경우 편도 1차로의 신호 교차로로 시나리오를 구성하였으며 V2X로 전달받은 신호 정보가 없기 때문에 대상 차량의 자율주행시스템은 비신호 교차로로 인식하여 V2V 기반의 BSM 메시지를 통하여 주변 차량의 상태 정보를 통하여 충돌이 발생하지 않았다.

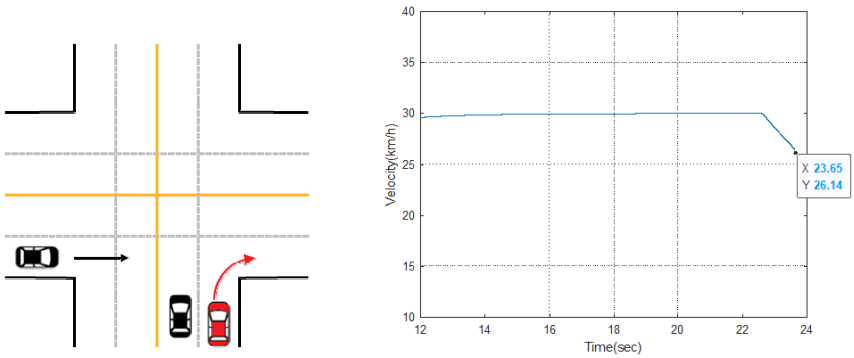
상충 회피를 위한 신호 정보 오제공 (MF2)의 경우 주변 차량은 V2X 신호등 정보를 신뢰하여 교차로에 진입하고 대상 차량에 잘못된 정보 (빨간불 상태인데 초록불로 잘못 제공)를 제공하여 충돌 위험이 존재하며 교차로를 진입 이후 센서 및 V2V 기반의 BSM 메시지를 통하여 충돌지점으로부터 3.6m에서 위험 상황을 판단하여 사고회피를 위한 0.98g로 늦은 시점의 감속이 발생하였다.



<Fig. 4> Scenario and simulation results of Function (F001)

2) 사각지대 충돌위험 정보 제공의 오작동 시나리오

사각지대 충돌위험 정보 미제공 (MF03) 시나리오는 도심의 편도 2차로 교차로에서 1차선에 정지 차량으로 사각지대가 존재하고 우회전하는 차량과 측면 차로에서 직진하는 차량과의 충돌상황을 모사하는 시나리오로 충돌 오프셋은 직진 차량의 50%로 설정하고 주행속도는 우회전 차량이 저속인 30km/h, 직진 차량은 60km/h의 속도로 설정하였다.



<Fig. 5> Scenario and simulation results of Function (F002)

사각지대 충돌위험 정보 오제공 (MF04) 시나리오는 도심 교차로에서 60km/h의 속도로 주행 중 교차로 진

입하는 주변 차량이 없지만 있다고 잘못 제공되어 의도치 않은 감속이 발생하여 후방에서 추종하는 차량의 충돌 위험이 발생할 수 있다.

3) 시뮬레이션 결과 분석

상충 회피를 위한 신호 정보 미제공 (MF01)의 경우 신호 정보가 제공되지 않았지만 충돌을 회피하였으며 상해 심각도는 QM으로 산정하였으며 상충 회피를 위한 신호 정보 오제공 (MF2)의 경우 교차로를 진입하고 위험 상황을 판단하여 늦은 감속으로 충돌 속도를 줄였지만 델타 v는 43.76 km/h로 충돌하여 상해 심각도는 S2으로 산정하였다. 사각지대 충돌위험 정보 미제공 (MF03)의 경우 차량이 교차로 충돌 위험 정보를 제공받지 못했지만 교차로를 진입하고 V2V 기반의 BSM 메시지를 통하여 충돌지점으로부터 3.6m에서 위험 상황을 판단하여 사고회피를 위한 0.98g로 늦은 감속으로 충돌 속도가 경감하여 델타 v는 26.14 km/h로 충돌하여 상해 심각도는 S1으로 산정하였다. 사각지대 충돌위험 정보 오제공 (MF04)의 경우 선행 차량이 충돌 위험 정보로 최대 감속도 0.98g로 제동을 하여도 후행 차량은 센서 기반 자율주행차량의 안전시스템으로 제동을 하여 충돌하지 않아 상해 심각도는 S0로 산정하였다.

<Table 6> Simulation results for malfunctions

Malfunction	Collision speed	Delta v	Severity
MF1	0 km/h	0 km/h	S0
MF2	43.76 km/h	21.88 km/h	S2
MF3	26.14 km/h	13.07 km/h	S1
MF4	0 km/h	0 km/h	S0

시뮬레이션 결과로부터 산정된 상해 심각도를 기반으로 ASIL 등급을 산정하면 다음과 같다.

<Table 7> The result of HARA (Hazard Analysis and Risk Assessment)

Malfunction	Hazard	S	E	C	ASIL
[MF01] Not provided signal information for collision avoidance	-	S0	E4	C3	QM
[MF02] Incorrect provided signal information for collision avoidance	Side impact	S2	E4	C3	C
[MF03] Not provided with collision risk information in blind spots	Side impact	S1	E4	C3	B
[MF04] Incorrect provided with collision risk information in blind spots	-	S0	E4	C3	QM

MF02와 MF03 오작동 시나리오의 시뮬레이션 결과를 보면, 고장 주입을 통해 V2I 메시지 결함으로 오작동이 발생하였지만 V2V 메시지를 통해 위험을 인지하고 사고 회피하기 위해 감속으로 상해 심각도가 낮아졌다. 하지만 V2X 모듈의 고장으로 인하여 V2I와 V2V 모두에 영향을 미치는 경우, 아래 정의한 결과의 위험성 평가보다 위험한 상황이 발생할 것이다.

<Table 8> Simulation results according to failure mode in the intersection scenario

Service	Function	Failure mode		Malfunction	ASIL
Cooperative Intersection Control	[F001] Providing signal information for	Transceiver	Message delay	No or Not	QM
			Message loss		
			Resequencing		

Service	Function	Failure mode		Malfunction	ASIL
Service	collision avoidance		Insertion of message		
			Incorrect addressing		
			Asymmetric information		
			Blocking access to a communication channel		
			Message Corruption	Incorrect	C
			Unintended message repetition		
	[F002] Providing collision risk information in blind spots		Message delay	No or Not	B
			Message loss		
			Resequencing		
			Insertion of message		
			Incorrect addressing		
			Asymmetric information		
			Blocking access to a communication channel		
			Message Corruption	Incorrect	QM
			Unintended message repetition		

Ⅴ. 결 론

본 연구에서는 도심로 교차로 상황에서 V2X를 활용한 자율주행차량의 시나리오를 제시하였고 Lv.4 수준의 자율주행차량을 정의함으로써 V2X의 고의존도 자율주행시스템으로 한정하였다. SAE J2735 메시지 셋을 분석하여 메시지 셋의 종류에 따라 차량과 차량 통신 (V2V)과 차량과 인프라 통신 (V2I)으로 구분하였다. 도심 신호 교차로의 시나리오로부터 기능에 대한 오작동 정의를 수행하고 차량 수준의 위험원 (Hazard)를 도출하였으며, 시뮬레이션을 통해 고장 유형별로 고장 주입 시나리오를 제시하여 오작동의 결함으로 발생되는 차량의 거동을 확인하고 위험성을 평가하였다.

신호 정보의 오작동으로 인해 잘못된 정보 제공되는 경우와 충돌 위험 정보의 오작동으로 인해 정보가 제공되지 않는다면 교차로 주행시 사고로 이어질 수 있으며 위험성이 높은 것으로 분석되었지만 V2V의 대표 메시지 셋인 기본 안전 메시지 (BSM)가 주변 차량을 파악하고 충돌 전에 감속하여 사고의 위험도를 낮출 수 있음을 알 수 있었다.

V2X 통신의 V2V와 V2I 메시지 간의 동일 혹은 유사한 차량 정보를 가지고 있기 때문에 교차로 상충 회피 시나리오의 기능에 대해 특정 메시지만을 활용하는 것이 아니라 이종의 메시지를 이용하여 위험 수준이 낮아질 수 있다. 하지만 앞서 다루지 않은 하드웨어 고장 등의 위험성은 여전히 존재하며 사고의 경감만을 할 수 있으므로 안전성 확보를 위한 V2X 모듈 기능안전 적용의 필요성을 식별하고 메시지 전송의 이중화, 내부 모니터링 및 고장 진단 등의 안전 컨셉이 적용되어 V2X 모듈의 고장 상황에서 사고를 방지하거나 상해를 줄일 수 있다. 이를 통하여 자율주행차량의 안전한 협력주행 구현이 가능할 것으로 보인다.

ACKNOWLEDGEMENTS

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(21PQOW-B152473-03)으로 수행하였습니다.

REFERENCES

Ahn D. R., Shin S. G., Baek Y. S. and Lee H. K.(2019), "Hazard Analysis of Autonomous Vehicle due to V2I Malfunction," *The Journal of the Korea Institute of Intelligent Transport Systems*, vol. 18, no. 6, pp.251-261.

Amrita G. and Mauro C.(2019), "Security issues and challenges in V2X: A Survey, Computer Networks," *Computer Networks Science Direct*, vol. 169, 107093.

Ararat O., Kural E. and Guvenc B. A.(2006), "Development of a Collision Warning System for Adaptive Cruise Control Vehicles Using a Comparison Analysis of Recent Algorithm," *2006 IEEE Intelligent Symposium*.

Baek Y. S., Shin S. G., Ahn D. R., Lee H. K., Moon B. J., Kim S. S. and Cho S. W.(2020), "A Study of Hazard Analysis and Monitoring Concepts of Autonomous Vehicles Based on V2V Communication System at Non-signalized Intersections," *The Journal of the Korea Institute of Intelligent Transport Systems*, vol. 19, no. 6, pp.222-234.

Biswas S., Haque M. M. and Misic J. V.(2010), "Privacy and Anonymity in VANETs: A Contemporary Study," *Ad Hoc & Sensor Wireless Networks*, vol. 10, pp.177-192.

Germbek O., Kurzhanskiy A. A., Medury A., Varaiya P. and Yu M.(2018), *Introducing an Intelligent Intersection*, ITS-Berkeley.

IEC 61508-2(2010), *Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*.

ISO-26262(2011), *Road vehicles-Functional safety-Part5: Product development at the hardware level*.

ISO-26262(2018), *Road vehicles-Functional safety-Part3: Concept Phase*.

Karagiannis G., Altintas O., Ekici E., Heijenk G., Jarupan B., Lin K. and Weil T.(2011), "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, pp.584-616.

Lee L. K. and Peng H.(2005), "Evaluation of automotive forward collision warning and collision avoidance algorithms," *Vehicle System Dynamics*, vol. 43, no. 10, pp.735-751.

SAE J2735(2016), *Dedicated Short Range Communications (DSRC) Message Set Dictionary*.

SAE J2980(2015), *Considerations for ISO 26262 ASIL Hazard Classification*.

Weise C.(2011), "V2x communication in Europe-from research projects towards standardization and field testing of vehicle communication technology," *Computer Networks*, vol. 55, pp.3103-3119.