ISO 26262를 활용한 V2X 통신시스템의 위험 분석 및 안전성 검증 전략에 관한 연구

임성묵, 정서현, 성경모

한국정보통신기술협회

seongmook.lim@tta.or.kr, shjeong@tta.or.kr, skm@tta.or.kr

Recearch on risk analysis and safety verification strategy for V2X communication system using ISO 26262

Seongmook Lim, Seohyun Jeong, Sungkyung Mo

Telecommunications Technology Association

요 약

V2X(Vehicle to Everything) 통신 기술은 차량이 주변 환경과 통신하여 교통 효율성과 도로 안전을 향상하게 하는 기술로, 다른 차량(V2V), 보행자(V2P), 인프라(V2I), 그리고 네트워크(V2N)와 정보를 교환한다. 기존의 V2X 통신시스템 검증은 메시지 전송의 신뢰성과 지연 문제 등 통신에 초점을 맞추고 있다. 본 논문은 ISO 26262의 위험 분석과 위험 평가를 적용하여 V2X 통신시스템의 안전성을 검증하고 기능 안전 요구사항을 만족하는 검증 전략을 수립하는 것을 목적으로 한다.

Ⅰ. 서 론

V2X 통신시스템을 통해 차량은 도로를 구성하는 주변 환경 및 다른 요소와 통신 작용할 수 있다. 이러한 통신은 차량이 셀룰러 네트워크 등 다양한 통신 채널을 사용하여 차량, 보행자, 인프라 및 네트워크 등과 메시지를 교환함으로써 교통 효율성과 도로 안전성을 향상한다.

V2X 통신시스템에 관한 기존 검증은 주로 메시지 전송의 신뢰성 및 지연 문제와 같은 통신 측면에 중점을 두고 있지만 ISO 26262와 같은 기능 안전 표준을 적용하는 측면에도 더 많은 연구가 필요해 보인다. ISO 26262에서 요구하는 위험 분석 및 위험 평가를 V2X 통신시스템에 체계적으로 적용한 연구는 위험을 식별하고 완화하는 데 매우 중요하다. 본 논문에서는 ISO 26262의 위험 분석 및 위험 평가 프로세스를 적용하여 V2X 통신시스템의 위험 분석 및 기능 안전성 검증 전략에 관한 연구를 하였다.

Ⅱ. V2X 통신시스템의 위험 분석

2.1 ISO 26262 목적

ISO 26262는 도로 차량 내 전기 및 전자(E/E) 시스템의 기능 안전을 다루는 국제 표준이다. 이 표준은 광범위한 IEC 61508 안전 표준에서 파생되었으며 자동차 산업 요구사항에 맞게 특별히 조정되어 개발, 생산, 운용, 서비스 및 폐기를 포함한 자동차 E/E 시스템의 수명 주기 전반에 걸쳐 안전을 보장하기 위한 위험 기반 접근 방식을 개괄적으로 설명한다.[1]

2.2 ISO 26262의 위험 분석 및 위험 평가의 주요 원칙

위험 분석 및 위험 평가는 ISO 26262의 핵심 구성요소로, E/E 시스템 장애와 관련된 잠재적 위험을 식별하고 분류하는 기초 역할을 하며 이 프로세스에는 몇 가지 주요 단계가 포함된다. [3]

가) 위험원 분석 및 위험 평가 착수: 위험원 분석 및 위험 평가는 아이템 정의에 기반을 두어야 하며, 내부 안전 메커니즘이 없는 아이템은 위험원 분석 및 위험 평가 동안에 평가되어야 함[3]

나) 상황 분석 및 위험원 식별: 올바르게 사용될 때와 합리적으로 예측하는 방법으로 올바르지 않게 사용될 때, 두 경우에 대해서 아이템의 오동작 행위로 인하여 위험 사건이 발생할 운용 상황 및 운용 방식 기술[3]

다) 위험 사건의 분류: 식별된 모든 위험 사건은 ISO 26262의 범위를 벗어나는 것을 제외하고는 모두 분류되어야 하며, 심각도(S), 노출 확률(E) 또는 제어 가능성(C)과 관련하여 주어진 위험원에 대해 분류

- 심각도(S): 한 명 이상의 사람들에게 잠재적으로 위험 사건에서 발생할 수 있는 위해 정도의 추정[1][3]

	등급			
	S0	S1	S2	S3
설명	상해 없음	가볍고 보통의 상해	심각하고 생명을 위협하는 상해	치명적 상해

- 노출 확률(E): 각 운용 상황에 대한 노출 확률[3]

	등급				
	E0	E1	E2	E3	E4
설명	거의 불가능	매우낮은확률	낮은 확률	중간 확률	높은 확률

- 제어 가능성(C): 관련된 사람의 시기적절한 대응을 통해 규정된 위험 또는 손상을 회피하는 능력[1][3]

	등급			
	C0	C1	C2	C3
설명	일반적으로 제어 가능	간단히 제어 가능	보통의 경우 제어 가능	제어하기 어렵거나 제어 불가능

라) 안전 목표 결정: 심각도, 노출 확률 및 제어 가능성의 분류에 기초하여 각 위험 사건에 관해 결정 [3]

심각도 등급	노출도 등급	제어가능성 등급		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

- QM: ISO26262 표준 준수에 대한 요구사항이 없음
- A는 가장 낮은 안전 무결성 수준이며 D는 가장 높은 안전 무결성 수준

Ⅲ. V2X 통신시스템의 안전성 검증 전략

3.1 ISO 26262의 주요 검증 기법

가) 결함 주입 테스트: 결함 주입 테스트는 실행시간 동안에 시험 대상에 결함을 주입하기 위해 특별한 방법을 사용하며, 이것은 준비된 HW를 통해 SW 안에서 실행 [4]

나) 고장 모드 및 영향 분석(FMjEA): 설계된 시스템이나 기기, 부품의 잠재적인 고장 모드를 찾아내고, 시스템이나 기기의 가동 중에 고장이 발생하였을 경우 목표 달성에 미치는 영향을 평가하여, 영향이 큰 고장 모드에 대해서는 적절한 대책을 세워 고장을 미리 방지 [5]

라) 인터페이스 테스트: 인터페이스 테스트는 호환성, 타이밍 및 기타 규정된 정격을 시험하기 위해서 아날로그와 디지털의 입력과 출력, 경계 테스트 및 동치 클래스 테스트를 포함하며, ECU의 SPI, IC 통신 또는 엘리먼트 사이의 다른 인터페이스의 동적 테스트뿐만 아니라 SW와 HW의 호환성에 대한 테스트를 수행 [4]

3.2 시나리오 기반의 테스트

가) 비상 전기 브레이크 라이트: 전방 차량이 운전자 실수나 도로 위험으로 인해 급제동하는 경우, 뒤를 따르는 운전자가 너무 늦게 반응하여 더 많은 차량에 영향을 미칠 수 있으며 이 경우에 안전 목표는 제어 가능성은 간단하고(C1), 심각성은 생명을 위협하며(S3), 노출 확률이 높으므로(E4) 안전 목표 B로 결정할 수 있음[6]

나) 좌회전 지원: 도로에서 신호등에 따라 직진과 좌회전을 동시에 허용하는 경우, 경우에 따라 차량의 시야를 가릴 수 있으며, 이 경우에 안전 목표는 제어할 수 없으며(C3), 심각도는 생명을 위협하며(S3), 노출 확률은 낮으므로(E1) 안전 목표 A로 결정할 수 있음[6]

다) 측면 충돌: 도시 환경의 교차로에서는 시야가 구조물로 인하여 제한되는 경우가 많으며, 이 경우 V2X를 사용하면 카메라와 레이더 등의 센서가 감지하기전에라도 다른 차량의 의도 등을 판단할 수 있음. 하지만 교차로에서 정당한 이유 없이 정지할 가능성이 있는 경우, 제어는 불가능하며(C3), 심각도는 생명을 위협하고(S3), 노출 확률은 낮으므로(E1) 안전 목표는 A로 결정할 수 있음[6]

라) 고속도로 차선 변경: 고속도로의 차선 변경은 향상할 방법이나, V2X 장애 등으로 인하여 두 대의 차량이 동시에 같은 지점에 잘못 도달할 가능성이 매우 크며, 이 경우 심각도는 생명을 위협하는 수준(S3), 주행 협상에 실패하여 제어가 어려우며(C3), 한 차량이 다른 차량의 예정 경로를 알지 못할 가능성이 크므로(E4) 안전 목표는 D여야 하며, V2X 통신시스템의 구성이 안전 목표 D에 도달해야 함을 의미함 [6]

Ⅳ. 결론

ISO 26262 위험 분석 및 위험 평가 방법론을 적용하여 V2X 통신시스템을 평가한 결과, ISO 26262를 통해 위험 분석 및 안전성 검증이 필요함을 확인하였다. 이 연구는 위험 완화 조치와 테스트를 통해 다양한 조건에서 중요한 기능의 안전성을 확인하는 전략을 확인하였으며, 안전 조치의 효율적인 통합과 기능 안전 표준의 준수는 V2X 통신시스템 개발에 필수적인 요소임을 확인하였다. 앞으로 V2X 기술이 자율주행 산업에 널리 도입될 것으로 예상되며, 이에 따라 V2X 통신시스템의 안전성을 높이기 위한 지속적인 연구가 중요해질 것으로 보인다.

ACKNOWLEDGMENT

※ 본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원의 “초고속 V2X 통신기반 자율주행 서비스 기술 개발” 지원으로 수행되었음 (과제번호 : 2021-0-01140)

참 고 문 헌

[1] KS R ISO 26262-1:2018, 도로 차량 - 기능 안전 - 제1부: 용어

[2] KS R ISO 26262-2:2018, 도로 차량 - 기능 안전 - 제2부: 기능 안전 관리

[3] KS R ISO 26262-3:2018, 도로 차량 - 기능 안전 - 제3부: 개념단계

[4] KS R ISO 26262-4:2018, 도로 차량 - 기능 안전 - 제4부: 시스템 수준에서의 제품 개발

[5] 이경호. "자동차 브레이크에 적합한 공정 FMEA에 관한 사례 연구." 국내석사학위논문 금오공과대학교, 2015. 경상북도

[6] Autotalks(2021), Funtional Safety for Enabling Present and Future V2X Use-Cases