Transactions of KSAE, Vol. 26, No. 2, pp.149-158 (March, 2018)

pISSN 1225-6382 / eISSN 2234-0149
DOI https://doi.org/10.7467/KSAE.2018.26.2.149

자율주행자동차의 종방향 주행지원시스템 기능안전 컨셉 설계 및 검증

안 대 룡[*1] · 신 성 근[1] · 박 기 홍[2] · 최 인 성[3] · 이 혁 기[1]

자동차부품연구원 스마트운전제어연구센터[1] · 국민대학교 자동차공학과[2]
교통안전공단 자동차안전연구원 자율주행연구팀[3]

Functional Safety Concept Design and Verification for Longitudinal Driving Assistance System of an Autonomous Vehicle

Daeryong Ahn[*1] • Seonggeun Shin[1] • Kihong Park[2] • Inseong Choi[3] • Hyuckkee Lee[1]

[1]Smart Driving Control R&D Center, Korea Automotive Technology Institute, 303 Pungse-ro, Pungse-myeon, Dongnam-gu, Cheonan-si, Chungnam 31214, Korea
[2]School of Automotive Engineering, Kookmin University, Seoul 02707, Korea
[3]Autonomous Vehicle R&D Team, Korea Automobile Testing & Research Institute, Korea Transportation Safety Authority, 200 Samjon-ro, Songsan-myeon, Hwaseong-si, Gyeonggi 18247, Korea
(Received 13 October 2017 / Revised 15 November 2017 / Accepted 11 December 2017)

Abstract : Recently, an autonomous vehicle, which is issued in the automobile market, is a combination of a high-level driver assistance system. Therefore, the safety and reliability of the driver assistance system is directly connected to autonomous vehicle safety and reliability. For an improved vehicle safety and reliability, emphasis is placed on the development and verification guidelines, such as the ISO-26262. In this paper, we studied the functional safety analysis method of Full Speed Range(FSRA) ACC, which is a typical longitudinal driver assistance system based on the ISO-26262 Part 3. We conducted a Hazard Analysis and Risk Assessment(H&R) to derive the safety objectives, as well as proposed a functional safety concept(FSC) and monitoring concepts for the typical malfunctions of the FSRA system. Finally, we verified the proposed concept in a simulated environment and proposed an index for the functional safety evaluation.

Key words : ACC(적응 순항 제어), FSRA(전 속도 영역 대응 ACC), Functional safety(기능안전), Malfunction(오작동), H&R(위험원 분석 및 리스크 평가), Safety goal(안전 목표), FSC(기능안전 컨셉), ISO-26262(자동차 기능안전 표준), Functional safety evaluation index(기능안전성 평가 지표)

1. 서 론

자율주행자동차 개발을 위해서는 현재 상용화되고 있는 지능형 자동차의 기술보다 더욱 안정성이 뛰어나고 악의적 환경에서 보다 강인한 성능이 보장되어야 한다. 따라서 안정성을 보장하기 위해 안전에 관련된 시스템은 테스트를 통해 안정성을 검증해야 한다.[1] 이에 따라 차량의 소프트웨어 및 전기 전자장치의 기능 오작동으로 인한 안전문제를 개선하기 위해 ISO-26262가 제정되었다.[2]

ISO-26262는 개발하는 아이템의 SW뿐만 아니라 HW 수준의 안전성을 위해 안전 컨셉 설계부터

*Corresponding author, E-mail: drahn@katech.re.kr

검증까지 아우르는 하나의 프로세스이다. 전기, 전자 기능안전 표준인 IEC-61508을 자동차 개발 프로세스에 맞게 보완하였다. ISO-26262 1판에서는 3.5톤 이하의 양산 차량에 한정하여 SW가 탑재된 전기 및 전자 부품 개발에만 해당되었지만 현재는 버스, 트럭, 모터사이클까지 차종이 확장되었으며 반도체의 기능안전까지 포함된 2판이 발표될 예정이다. ISO- 26262의 중요성이 커지면서 유럽뿐만 아니라 미국, 일본, 우리나라의 OEM에서도 이 개발 프로세스에 대한 요구사항을 준수하기 위해 노력하고 있다.

미국 자동차공학회(SAE)에서 정의한 자율주행 차량 등급[4]에 따르면 현재 상용화된 자율주행의 기술은 다중 기능 자율화에 해당하는 Level2에 해당한다. 예를 들면 종방향 운전자 지원 시스템인 ACC와 횡방향 운전자 지원 시스템인 LKAS(Lane Keeping Assistance System)가 동시에 동작하는 제어능력을 갖는 레벨이라고 볼 수 있다. 일반적인 차량은 운전자가 직접 차량을 제어하여 사고의 위험을 줄이거나 회피가 가능하지만 센서를 통해 주변을 인식하고 판단하는 자율주행자동차의 경우, 센서의 미인식, 오인식, 시스템의 오작동 또는 유기적 관계에 있는 하드웨어 또는 소프트웨어에서 고장이 발생하면 전제 시스템에서 판단 오류가 발생할 수 있으며 해당 오류로 인해 큰 사고로 이어질 수 있다.[11] 따라서 자율주행자동차의 주행지원 시스템의 기능안전 또는 고장 안전 분석이 꼭 필요하다.

본 논문에서는 종방향 주행지원시스템인 FSRA 시스템의 기능 안전성 평가를 위한 평가 지표를 도출하기 위해 ISO-26262 Part3 기반의 프로세스를[3] 수행하여 위험원 분석(H&R)을 실시하고, 도출된 위험원에 대한 안전 목표(Safety goal)를 도출하였다. 안전 목표를 준수하기 위해 FSRA 시스템의 주요 오작동인 “의도치 않은 가속”과 “의도치 않은 감속”에 대한 간단한 기능안전 컨셉을 설계하고 시뮬레이션을 통한 컨셉 검증 과정을 통해 자율주행자동차의 종방향 주행지원시스템의 기능안전성 평가 지표를 제안하였다. FSRA 시스템의 예비 아키텍처에는 센서와 액추에이터가 포함되어있지만 센서와 액추에이터의 기능은 정상 작동한다는 가정 하에 FSRA 기능 제어기만 고려하여 작성되었으며 센서와 액추에이터의 기능안전 요구사항 정도만 간략하게 작성되었다. 본 논문에서 수행된 과정을 통해 향후 자율주행자동차의 종방향 주행지원 시스템의 안전성 평가를 위한 평가 지표를 제안하였다.

2. FSRA 시스템 기능 및 오작동 정의

ISO-26262 Part3의 위험원 분석을 실시하기 위해서는 먼저 시스템의 기능과 기능에 대한 오작동을 정의해야 한다. FSRA 시스템은 Full Speed Range ACC의 약어로 대표적인 종방향 주행지원시스템이다. ACC는 전방 차량과의 거리, 차량의 거동, 운전자 명령 등의 정보를 바탕으로 엔진 동력전달계 및 브레이크를 제어하여 전방 차량과 적당한 거리를 유지하며 전방 차량을 추종하는 기능을 수행한다.[9] FSRA 시스템은 ACC 기능에 더하여 차량 정지부터 설정 속도까지 전 속도를 대응할 수 있으며 차량의 각종 센서와 주로 CAN을 통해 정보를 주고받는다. 본 연구에서는 대표적인 충돌 경감 및 회피 기능인 AEB 시스템의 기능이 포함된 FSRA 시스템으로 정의하여 분석 하였으며 센서 및 액추에이터보다는 제어기 기능을 중심으로 분석하였다. 아래 그림은 FSRA 시스템의 예비 아키텍처를 나타낸다. 본 장에서는 FSRA 시스템의 기능 및 기능별 오작동을 정의하고 오작동 시뮬레이션을 실시하여 Severity 및 Controllability 등급 산정에 참고하였다.

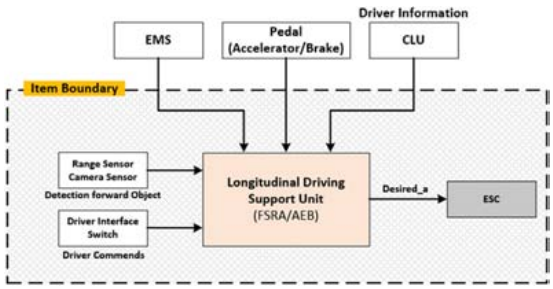

Fig. 1 Longitudinal driving assistance system preliminary architecture

2.1 FSRA 시스템 기능 정의

FSRA 시스템은 차량의 전체 속도 구간을 대응할 수 있는 ACC 시스템이며 FSRA 기능에 포함된 AEB

Table 1 FSRA system subfunction define

Function	Description
Speed increase	Accelerate for the set speed
Speed decrease	Deceleration for the set speed

시스템은 전방 차량 또는 보행자와의 충돌 상황에서 운전자가 반응하지 못하는 위급한 상황에 자동으로 급제동을 수행하는 시스템이다. 종방향 주행지원시스템의 대표 기능은 “차량의 속도 제어”, “차간 거리 제어”가 있지만 본 논문에 분석한 기능으로 “차량 속도 증가”와 “차량 속도 감소”기능에 집중하여 분석하였다.

2.2 FSRA 시스템 오작동 정의

FSRA 시스템의 오작동 정의는 위험원 도출을 위해 사용되는 대표적 기법인 HAZOP(Hazard and Operability Studies)를 사용하였다. HAZOP 기법은 위험원 도출을 위한 형식화된 시스템적 기법으로서 안내어(Guide word)라는 개념을 사용한다. More, No, Less 등과 같은 안내어들은 위험원을 도출하는 과정에서 시스템의 여러 상태와 결합되어 설계의도에서 벗어날 수 있는 이상 현상들을 식별하여 위험원의 발생을 찾게 되는 개념이다.[5)]

HAZOP Guide words 기반의 분류를 통해 “차량 속도 증가”, “차량 속도 감소”기능에 대한 오작동은 총 4개로 아래 표는 FSRA 시스템의 오작동을 정리한 것을 나타낸다.

Table 2 FSRA system malfunction

Malfunction	Description
Wrong increase of vehicle speed	Not a acceleration condition, but acceleration is performed
Excessive increase of vehicle speed	Acceleration to system maximum acceleration
Wrong decrease of vehicle speed	Not a deceleration condition, but deceleration is performed
Excessive decrease of vehicle speed	Deceleration to a higher deceleration rate than the normal deceleration rate

3. 위험원 분석

위험원 분석은 시스템의 오작동으로 인해 발생될 수 있는 Hazard(위험원) 분석과 도로, 노면, 주변 차량의 움직임, 교통량 등 환경적 요인이 적용되어 차량 수준의 Hazardous event를 생성하고 각 Event 별 Severity(S), Exposure(E), Controllability(C) 등급을 할당하여 ASIL 등급을 산정하고 안전 목표를 설정하는 일련의 과정이다. 본 논문에서 위험원 분석 시 오작동이 일어나는 각 상황에 대하여 S, E, C 등급 할당에 필요한 주행 속도는 고속(100 km/h), 중속(70 km/h), 저속(30 km/h)으로 설정하여 적용하였고 오작동 시뮬레이션을 통해 얻은 결과를 바탕으로 S 등급과 C 등급 할당에 참고하였다.

3.1 상황 분석

상황 분석은 Hazardous event를 생성할 때 고려되는 환경적인 요인으로, 차량 운전 조건 및 상황을 분석하기 위한 단계이다. 오작동이 일어나는 장소, 환경을 가정하여 오작동에 의해 일어나는 위험 상황을 일련의 시나리오 형태로 작성하게 된다. 본 논문에서 Hazardous event 생성을 위한 상황 분석 시 고려한 환경적 요인은 Location(고속도로, 국도, 시내), Road shape(직선로, 곡선로, 로터리, 합류지점, 분기점), Traffic(보통, 혼잡, 정체), Vehicle action(차선 유지, Time gap 추종, 전방 차량 감속/급감속)을 고려하였다.

3.2 S, E, C 등급 산정

Situation analysis와 Malfunction의 조합을 통해 도출된 Hazardous event에 S, E, C 등급을 산정하여 시스템의 ASIL 등급을 산출한다. S 등급 산정의 기준은 ISO-26262 Part3 및 SAE J2980[6)] 문서를 참고하였다. E 와 C 등급의 기준도 ISO-26262 Part3의 부록의 예시를 참고하였으며 상태 심각도인 S 등급과 제어 가능성을 나타내는 C 등급의 산정은 FSRA 시스템의 오작동 시뮬레이션과 통계자료를 바탕으로 산정하였다.

3.2.1 오작동 시뮬레이션

FSRA 시스템의 오작동 시뮬레이션 환경에서 차량 동역학 모델은 TESIS사의 veDYNA를 이용한 YF 쏘나타 모델이며 아래 그림과 같이 시뮬레이션 환경을 구성하였다.

시뮬레이션 시나리오는 Host vehicle이 전방 차량

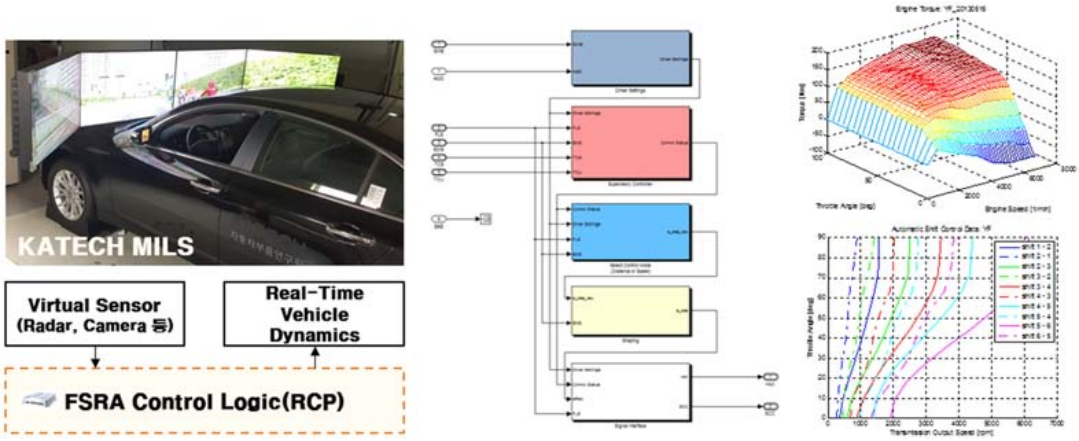

Photo. 1 Simulation environment

을 Time gap 추종 중 Host vehicle의 의도치 않은 감속 및 가속을 수행하는 시나리오로 구성하였다. Time gap 추종 시 전방 차량과의 차간 거리는 Time gap 1.0 s, 1.5 s, 2.0 s에 따른 거리로 설정하였으며 전방 차량의 일반적인 감속도는 0.4 g, 급제동 시 감속도는 0.8 g로 설정하였다. 또한 시뮬레이션에서 추돌 및 피 추돌 차량의 질량은 같다고 가정하여 충돌속도를 계산하였다. 충돌속도는 아래 식 (1)[10]과 같다.

$$\Delta v = \frac{m1}{m1+m2}(v1-v2) \quad (1)$$

여기서 Δv는 속도 변화를 나타내고, m1은 추돌 차량의 질량, m2는 피추돌 차량의 질량, v1은 추돌 차량의 추돌 시 속도, v2는 피추돌 차량의 추돌 시 속도를 나타낸다.

Host vehicle의 감속 시나리오 시 제동력은 국제표준인 ISO-22179[7]에서 제안한 FSRA 시스템의 최대 감속도인 0.5 g, 가속도는 4 m/s^{2}으로 설정하였다. Controllability를 산정하기 위해 운전자의 Reaction time을 약 1.2 sec[8]로 가정하고 오작동 발생 후 급제동하여 종방향 충돌 회피 유무를 확인하였다.

첫 번째 시험 시나리오는 주행 중 FSRA 오작동으로 시스템의 최대 감속도(0.5 g)로 감속하여 후방 차량이 추돌하는 시나리오이다. 시나리오 조건 및 시뮬레이션의 결과는 아래 Table 4와 같다.

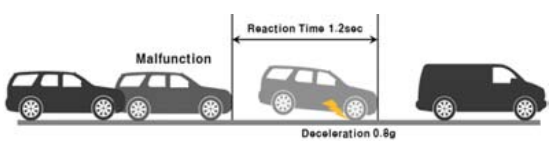

Fig. 2 Driver brake reaction time and deceleration

Table 3 FSRA system malfunction simulation 1

Velocity	Distance	Col_v	Δv
High (100 km/h)	50 m	81.5 km/h	40.75 km/h (S2)
	30 m	64.6 km/h	32.3 km/h (S2)
Mid (70 km/h)	50 m	70 km/h	35 km/h (S2)
	30 m	65 km/h	32.5 km/h (S2)
Low (30 km/h)	30 m	30 km/h	15 km/h (S1)
	5 m	25.1 km/h	12.55 km/h (S1)

Table 3의 시나리오 조건 별 충돌 속도를 이용하여 Severity 등급 산정에 활용하고자 운전자 반응 시간 후 회피를 위한 제동은 들어가지 않은 채 시뮬레이션이 실시되었다. Fig. 3은 첫 번째 시나리오 중 전방 차량과 상대 거리 50 m, 속도는 100 km/h의 고속으로 주행 중 전방 차량의 FSRA 시스템의 오작동으로 인해 0.5 g로 감속할 때 Host vehicle이 제동 없이 충돌하는 시뮬레이션 결과를 나타낸다.

Fig. 4는 두 번째 시나리오는 전방 차량을 Time gap 추종 중 FSRA 시스템의 최대가속도인 4 m/s^{2}으로 가속하는 시나리오 결과이다. 차량 속도 및 Time gap 별 충돌 속도와 Severity 산정 값은 Table 4와 같다. 충돌 속도는 작지만 고속도로에서의 2차사고 등을 고려하여 모두S3로 산정하였다.

세 번째 시나리오는 Controllability 등급 산정을 위해 본 논문에서 설정한 운전자 Reaction time인 1.2 s

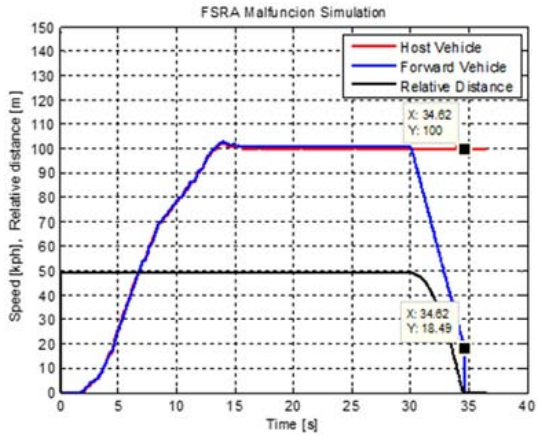

Fig. 3 Malfunction simulation example 1 (100 km/h, 50 m)

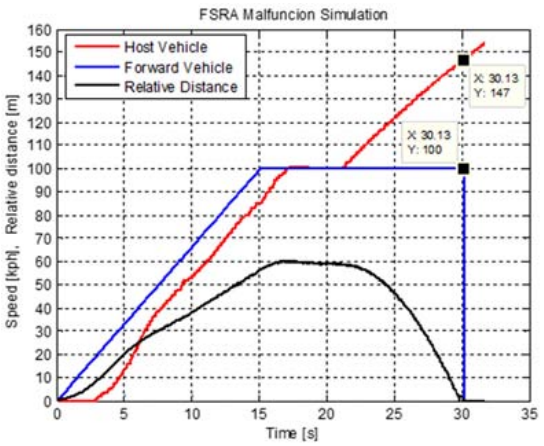

Fig. 4 Malfunction simulation example 2 (100 km/h, t-gap2.0 s)

Table 4 FSRA system malfunction simulation 2

Velocity	Time gap	Col_v	Δv
High (100 km/h)	1.0 s	36 km/h	18 km/h
	1.5 s	41 km/h	20.5 km/h
	2.0 s	47 km/h	23.5 km/h
Mid (70 km/h)	1.0 s	39 km/h	14.5 km/h
	1.5 s	45 km/h	22.5 km/h
	2.0 s	49 km/h	24.5 km/h
Low (30 km/h)	1.0 s	38 km/h	19 km/h
	1.5 s	43 km/h	21.5 km/h
	2.0 s	45 km/h	22.5 km/h

후 제동을 통해 충돌 회피가 가능한지 여부를 확인하기 위해 실시하였다. 전방 차량을 Time gap 추종 중 전방 차량의 감속(0.4 g) 또는 급 감속(0.8 g) 시 과도한 가속(4 m/s^2)으로 인해 전방 차량을 추돌하는 시뮬레이션을 실시한 결과 전방 차량의 일반적인 감속(0.4 g) 상황에서의 과도한 가속 시나리오에서는 충돌을 모두 회피하였으며 0.8 g로 급 감속 시 과도한 가속으로 인한 충돌 속도는 아래 표 Table 5와 같이 정리하였다.

Table 5 FSRA system malfunction simulation 3

Velocity	Time gap	Δv	Col_t	C
High (100 km/h)	1.0 s	32.25 km/h	3.02 s	C2
	1.5 s	31.5 km/h	3.75 s	
	2.0 s	22.5 km/h	4.45 s	
Mid (70 km/h)	1.0 s	32.5 km/h	2.48 s	
	1.5 s	27 km/h	2.01 s	
	2.0 s	19 km/h	3.69 s	
Low (30 km/h)	1.0 s	17 km/h	2.03 s	
	1.5 s	17 km/h	2.35 s	
	2.0 s	11.5 km/h	2.81 s	

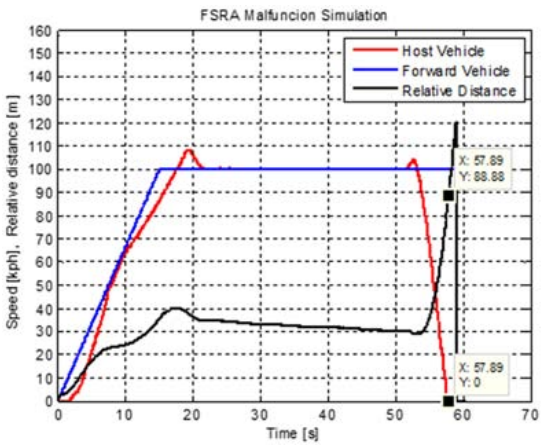

Fig. 5 Malfunction simulation example 3 (100 km/h, t-gap1.0 s) collision avoidance

Table 5에서 Col_t는 오작동이 발생된 시점부터 충돌까지 걸린 시간을 나타내며, 전방 차량 급감속 시뮬레이션 Case에서는 모두 충돌하였고 그 외의 시나리오에서는 충돌을 모두 회피하였다. 시뮬레이션의 결과로 판단하면 전방 차량의 급감속 및 AEB 시스템의 긴급제동 오수행 시 후방 차량에 의한 추돌이 일어나 Controllability가 높을 것으로 보이지만 본 논문에서 구성한 시나리오가 실제 전체 사고 시나리오를 대표할 수 없으며 실제 운전자라면 전방 차량이 갑자기 급제동을 수행 하더라도 실제 운전

자 역시 급제동 또는 조향을 통해 회피가 가능할 것을 고려하여 C2 정도로 판단하였다.

3.3 Worst Case 선별

진행된 시뮬레이션 결과를 바탕으로 시나리오 별 Severity, Exposure, Controllability를 산정하여 위험원 분석을 실시하였다. 위험원 분석 결과 약 1000개 수준의 Malfunction case가 도출되어 ASIL 등급이 할당되었다. 아래 그림은 분석시나리오 중 ASIL 등급이 높은 위험도 있는 Worst case를 선별하여 나타낸 것이다.

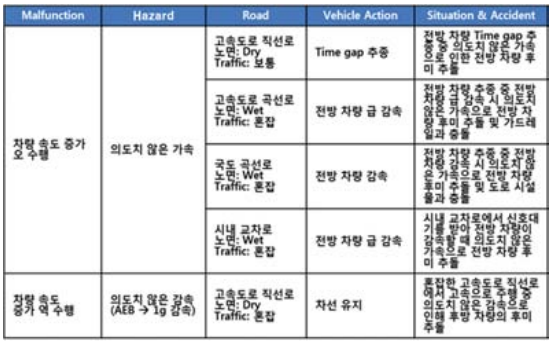

Fig. 6 Worst case speed increase/decrease malfunction

3.4 Safety Goal 도출

Safety goal은 Malfunction에 의한 Hazard를 방지하는 형태로 작성하였다. 본 논문에서 도출된 Safety goal을 달성하기 위한 Safe state는 제어기를 “Shut-off” 시켜 의도치 않은 감/가속이 일어나지 않도록 설계하였다. 아래 표에 도출된 FSRA 시스템의 Safety goal을 정리하였다.

Table 6 FSRA system safety goal

ID	Safety goal
G001	Prevents unintended acceleration due to an increase in the speed of the vehicle
G002	Prevents unintended deceleration due to an decrease in the speed of the vehicle

4. 기능안전 컨셉 설계 및 검증

기능안전 컨셉은 자율주행자동차의 안전성 평가 시 중요한 평가 대상이라고 볼 수 있다. 예를 들면

Table 7 Safety requirement of each component

Component	Safety requirement
Forward sensor	A plausibility check can be applied to the forward sensor signals
Driver control switch	A plausibility check can be applied to the driver control switch
Actuator	Actuator a plausibility check can be applied to the actuator signals
Controller	The controller unit detects faults in the forward sensor
	The controller unit detects faults in the actuator
	The control unit, which detects and confirm the setting of an impermissible acceleration and deceleration, brings the system into a safe state as a fault reaction

시스템의 오작동을 어떻게 감지하고 어떻게 조치할 것인가에 대한 해결방안이 기능안전 컨셉 설계에 포함되기 때문이다. Safety goal을 달성하기 위한 기능안전 컨셉은 모니터링을 통해 오작동 발생 시 허용 시간 내에 적절한 조치를 수행하여 차량을 제어 가능한 안전한 상태로 전환하는 컨셉이다. Safety goal 달성을 위해 설계한 컴포넌트 별 안전 요구사항은 유럽의 주요 완성차 업체에서 발표한 가솔린/디젤 엔진 제어 유닛의 모니터링 컨셉인 E-GAS 모니터링 컨셉[8]을 참고하여 아래 표에 작성하였다. E-GAS 모니터링 컨셉에서 엔진 제어 유닛의 오작동으로 인한 의도치 않은 가속 부분에 대하여 모니터링 해야 하는 시그널과 오작동 여부를 판단하는 안전 컨셉 예시를 본 논문의 내용과 유사한 부분이 있어 참고하였다.

4.1 오작동 대응을 위한 안전 컨셉

본 논문에서 다루고자 한 것은 안전 컨셉을 설계하는 것이 아닌 기능안전성을 평가하기 위한 평가항목을 도출하는 것으로 제어기의 Level2 수준의 기능 모니터링 컨셉 정도로 구현하여 진행하였다. Safety goal을 달성하기 위한 안전 컨셉은 아래 그림과 같다. 입출력 센서의 타당성 확인과 차량의 가속도를 결정하는 기능제어기(Level1)의 가속도를 모니터링하는 모니터링제어기(Level2)로 구성하였다.

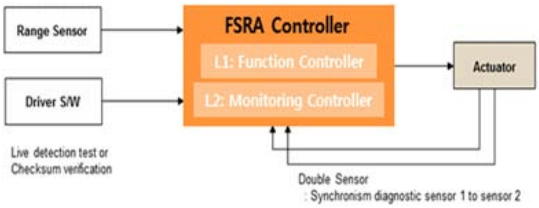

Fig. 7 Safety Concept of malfunction prevention

4.2 모니터링 컨셉

기능 제어기의 가속도 결정 오류를 검출하기 위한 모니터링 컨셉은 시스템에서 허용 가능한 가속도를 계산하고, 실제 가속도와 비교하는 컨셉으로 기능 안전성 평가 시 오작동을 검출 전략에 해당되는 내용이다.

가속도 모니터링을 통해 기능 제어기의 가속도 결정에 대한 타당성을 검증하였다. 의도치 않은 가속 및 감속 발생 시의 Safe state로 정의한 Shut-off(감/가속 명령 차단)하는 안전 조치를 수행하였다. Fig. 8은 가속도 모니터링 컨셉의 구조를 나타낸 그림으로, 좌측에서 허용 가능한 가속도를 계산하여 입력을 받고, 우측에서는 ESC를 통해 현재 출력되고 있는 실제 가속도를 입력 받아 비교하는 컨셉이다.

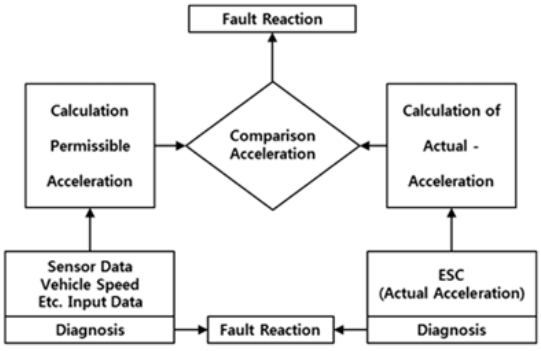

Fig. 8 Acceleration monitoring concept

4.3 안전 컨셉 검증

4.3.1 검증 환경

설계한 안전 컨셉 검증을 위해 시뮬레이션 기반 안전 컨셉 검증 환경을 구성하였다. dSPACE 사의 ASM(차량 모델)을 이용해 FSRA 시스템과 Fig. 8의 가속도 모니터링 알고리즘을 구현하였고, ASM에서 지원하는 가상 Radar 센서를 통해 전/후방 차량의

Fig. 9 Simulation based verification environment

데이터를 취득하였다. 아래 그림은 시뮬레이션 기반의 검증 환경을 나타낸다.

4.3.2 검증 시나리오

검증 시나리오는 Subject vehicle이 FSRA 시스템을 사용하여 주행 중 의도치 않은 가속 및 감속이 발생하는 시나리오로 상세 시나리오는 Fig. 10과 같다.

의도치 않은 감속 시나리오에서 후방 차량은 Time gap 1.0 s로 추종 중 전방 차량 감속에 대한 반응 시간을 1.5초 후 -4 m/s^{2}으로 감속하는 운전자 모델을 적용하였다. 각 오작동 시나리오를 기반으로 의도치 않은 가속과 감속을 위한 오류를 주입하여 컨

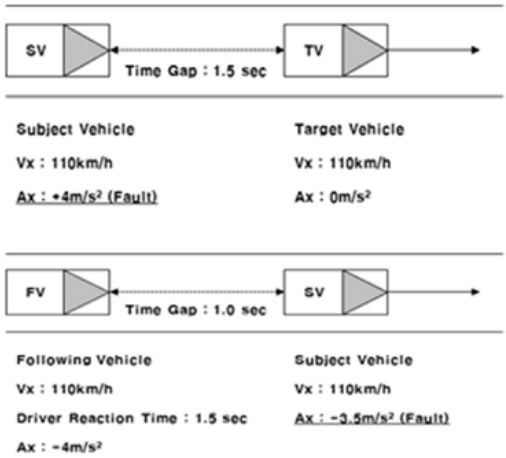

Fig. 10 Unintended acceleration/deceleration scenario

셉 검증을 실시하였으며, 오류주입은 FSRA 제어기의 요청 가속도 값을 직접 입력하는 형식으로 진행하였다.

4.3.3 검증 결과

의도치 않은 가속 및 감속에 의한 안전 컨셉 검증 결과는 Fig. 11과 같다. 의도치 않은 가속 시뮬레이션의 경우 시뮬레이션 시간 기준 약 2.2초 경 4 m/s^{2}의 가속도 요청 값을 임의로 입력하였으며, 모니터링 제어기는 허용 가능한 가속도와 실제 가속도를 비교하여 제어기 Shut-off를 수행 2.6초에 차량의 의도치 않은 가속 명령을 제한하여 전방 차량과의 충돌을 회피하였다. Fig. 11 좌측 하단 그래프에서 파란색 선은 요청된 가속도로, 시스템의 최대 가속도인 4 m/s로 요청되었고 초록색 선은 제어기에서 Shut-off 명령이 출력된 그래프이다. 여기서 제어기 Shut-off 수행은 기능안전성 평가 시 오작동에 대하여 어떻게 조치를 취했는지에 대한 전략의 예로 사용될 수 있다.

의도치 않은 감속에 대한 시뮬레이션의 경우 시뮬레이션 시간 기준 약 4.99초에 -3.5 m/s^{2}의 감속도 요청 값을 임의로 입력하였으며, 모니터링 제어기는 허용 가능한 가속도와 실제 가속도를 비교하여 제어기 Shut-off를 수행하여 약 5.33초에 차량의 의도치 않은 감속 명령을 제한하여 충돌을 회피하였다.

4.4 기능안전성 평가 지표

본 논문에서 진행한 일련의 과정은 종방향 자율주행지원시스템의 기능안전과 관련된 평가대책을 작성하고 시스템의 기능안전 평가 시 참고자료로 활용될 수 있는 평가지표를 도출하는 것이다.

본 논문에서 진행한 ISO-26262 Part3 프로세스를 통해 도출된 평가 지표는 아래 표와 같이 정리하였다.

첫 번째 평가 항목은 오작동 감지에 대한 적정성이다. 이는 오작동 발생 시 시스템은 오작동 검지 유무를 판단하는 지표로 볼 수 있다. 본 논문에서 작성한 Level2 모니터링 컨셉을 평가하는 지표로 오작동 감지에 효과적인지 여부를 평가한다.

두 번째 평가 항목은 오작동 조치에 대한 적정성이다. 이는 오작동 발생 시 시스템이 오작동에 대한 조치를 잘 수행하는지 평가하기 위한 지표이다. 오작동 조치에 대한 적정성은 조치 여부, 조치 방법, 조치 시간의 세부 항목으로 나눌 수 있다. 본 논문에

Table 8 Derived evaluation index

Evaluation index	Evaluation item
Appropriateness of malfunction detection	- Check for malfunction detection
Appropriateness of malfunction measures	- Whether malfunction is measures - Solution of malfunction - Measure time of malfunction

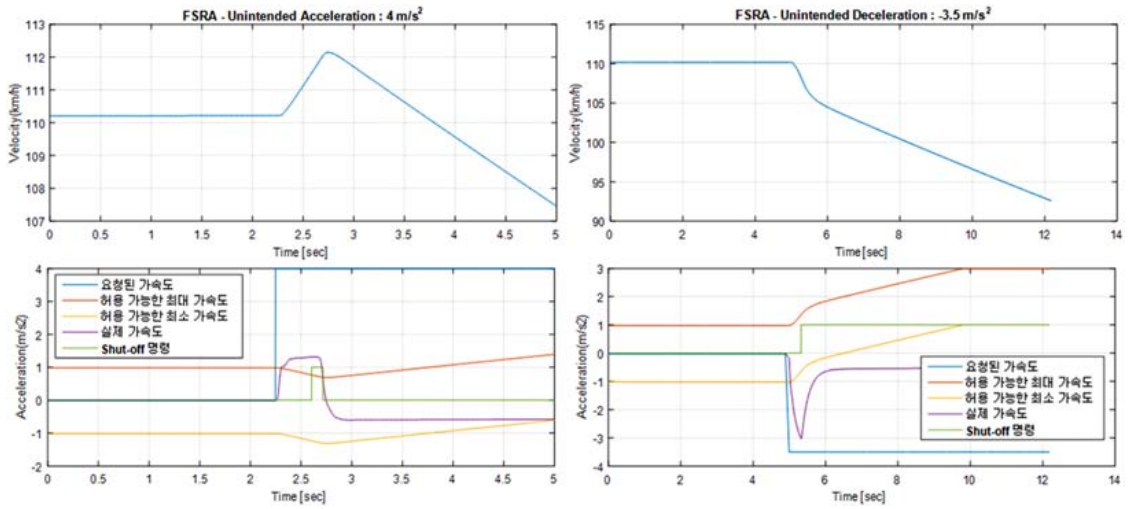

Fig. 11 Unintended acceleration and deceleration simulation result

서 수행된 조치여부와 조치 방법은 Shut-off 방식을 사용하여 오작동에 대한 조치를 수행한 것이 이에 해당된다. 조치 시간은 오작동이 발생한 시점부터 조치까지 걸린 시간으로 본 논문에서는 500 ms의 시간을 예시로 적용하였지만 오작동 발생 상황 및 센서 지연시간, 제어 지연시간, 액추에이터 반응 시간, 통신 지연 등 여러 가지 요인에 따라 달라지며 추가적인 연구를 통해 최적화가 필요한 부분이다.

5. 결 론

본 논문에서는 대표적인 종방향 자율주행지원시스템인 FSRA 시스템의 기능 제어기에 대하여 기능안전성을 평가하기 위한 평가 항목을 제안하고자 ISO-26262 Part3 프로세스의 기능안전 분석을 통해 위험원 분석을 수행하였다. 분석 수행 시 Hazardous event에 S, E, C 등급을 할당하기 위해 FSRA 시스템의 오작동 시뮬레이션을 진행하여 ASIL 등급 산정에 이용하였고 이를 바탕으로 FSRA 시스템의 Safety goal을 도출하였다. 도출된 Safety goal을 준수하기 위해 “의도치 않은 가속”, “의도치 않은 감속”에 대한 간단한 안전 컨셉을 설계하고 시뮬레이션을 통해 검증하였다.

본 연구에서 제안한 기능 안전성 평가 지표는 “오작동 감지에 대한 적정성”과 “오작동 조치에 대한 적정성”으로 오작동을 감지하기 위해 시스템에서 허용 가능한 감/가속도와 ESC를 통해 출력되는 실제 감/가속도를 모니터링 하는 컨셉의 예를 들었으며 “오작동 조치에 대한 적정성”의 예로 감/가속도 모니터링 중 일정 Margin 이상의 차이를 보이게 되면 시스템 Shut-off를 수행하여 충돌을 방지하도록 했다. 또한 오작동 조치 시간에 대한 추가적 연구를 통해 최적화가 필요하지만 본 논문에서 시뮬레이션 한 결과 500 ms 이내로 안전 조치 수행 시 충돌을 회피하여 안전한 상태를 유지하는 것으로 확인되었다.

본 논문에서 진행된 일련의 과정은 종방향 자율주행지원시스템의 오작동에 대한 감지 방법 및 조치 방법, 조치 시간을 도출하기 위한 예시라고 볼 수 있다.

자율주행 자동차의 도입 요구와 적용의 필요성이 증대되고 있는 시점에 자율주행기술 도입 시 가장 큰 위험요소로 주행 안전성 등의 논란이 제기되고 있다. 따라서 자율주행 자동차의 안전성을 평가하기 위한 기준 및 방법에 대한 연구도 지속되어야 한다.

후 기

본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(17TLRP-B117133-02)으로 수행된 연구임.

References

1) D. Gruyer, S. Pechberti and S. Glaser, “Development of Full Speed Range ACC with SiVIC, a Virtual Platform for ADAS Prototyping, Test and Evaluation,” IEEE Intelligent Vehicles Symposium, pp.100-105, 2013.
2) K. H. Roh and K. S. Lee, “An Ontology-Based Hazard Analysis and Risk Assessment for Automotive Funtional Safety,” Journal of the Korea Society of Computer and Information, Vol.20, No.3, pp.9-17, 2015.
3) ISO 26262-3:2011, Road Vehicles – Functional Safety - Part 3: Concept Phase, 2011.
4) Automated Driving-levels of Driving Automation are Defined in New SAE International Standard J3016, 2015.
5) J. G. Hwang, H. J. Jo, C. H. Han, W. S. Cho, J. Ahn and D. M. Ha, “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, 2010.
6) SAE-J2980, Considerations for ISO 26262 ASIL Hazard Classification, 2015.
7) ISO 22179, Intelligent Transport Systems - Full Speed Range Adaptive Cruise Control(FSRA) Systems - Performance Requirements and Test Procedures, 2009.
8) Standardized E-Gas Monitoring Concept for Gasoline and Diesel Engine Controls Units, Version 6.0, 2015.
9) B. J. Yong, S. J. Shim and K. H. Yoon, “Safety Evaluation of the Adaptive Cruise Control

System," Transactions of KSAE, Vol.15, No.2 pp.159-164, 2007.
10) D. B. Kim, D. K. Yun, J. H. Park, S. Y. Ha and J. C. Park, "A Case Study on Speed Analysis of the Rear-end Collision Accident," Transactions of KSAE, Vol.24, No.6, pp.724-729, 2016.
11) B. H. Bae, J. H. Kim and B. W. Kim, "Design of Fail-safe System Architecture for Robust Autonomous Unmanned Ground Vehicle," KSAE Annual Conference Proceedings, pp.1368-1373, 2011.