Transactions of KSAE, Vol. 34, No. 11, pp.1353-1371 (November, 2026)

Check for updates

Copyright © 2026 KSAE / 252-12
pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2026.34.11.1353

〈응 용 논 문〉

순차형 AEB/AES 사고회피 시스템의 천이 오작동에 대한 기능안전 분석 및 안전 메커니즘 검증

백 윤 석[1,2] · 이 형 철[*2]

한국자동차연구원 주행안전연구센터[1] · 한양대학교 전기공학과[2]

Functional Safety Analysis and Safety Mechanism Verification for Transition Faults in a Sequential AEB/AES Collision Avoidance System

Yunseok Baek[1,2] · Hyeongcheol Lee[*2]

[1]*Autonomous Driving Technology Research Division, Korea Automotive Technology Institute (KATECH), 303 Pungse-ro, Pungse-myeon, Dongnam-gu, Cheonan-si, Chungnam 31214, Korea*

[2]*Department of Electrical Engineering, Hanyang University, Seoul 04763, Korea*

(Received 6 July 2026 / Revised 18 July 2026 / Accepted 11 August 2026)

Abstract : This study presents an STPA-HARA-based functional safety analysis and a safety mechanism design for a sequential AEB/AES collision avoidance function. In time-critical cut-in scenarios, safety-critical mode-transition faults may occur because the target function prioritizes AEB and considers AES only when braking alone is insufficient. STPA is applied to identify unsafe control actions involving AEB request omission, AES request omission or delay, and AEB-to-AES transition failure, which converge into a common transition fault set. The identified results are mapped to hazardous events and safety goals in accordance with ISO 26262 Part 3, and the dominant events are evaluated as ASIL D. At the software level, a logical gate is designed to monitor transition-violation precursors and conditionally correct AES requests under a steering-feasibility guard. R157 cut-in fault injection is used for verification by comparing nominal cases, fault-injected cases, and cases with safety mechanism applied.

Key words : Functional safety(기능안전), Sequential AEB/AES(순차형 자동긴급제동/자동긴급조향), STPA-HARA(시스템 이론 기반 프로세스 분석 및 위험성 평가), Safety mechanism(안전 메커니즘), Fault injection(고장 주입)

Nomenclature

BTN	: braking threat number
STN	: steering threat number
TTC	: time to collision, s
R_{crit}	: collision-risk critical flag
B_{inf}	: braking-insufficiency flag
S_{feas}	: steering-feasibility flag
C_2	: condition where braking is insufficient but steering is feasible under critical risk
$C_{2,\mathrm{valid}}$	: validated C2 condition after signal stabilization
M	: current functional mode
$M_{tr}^{AEB\rightarrow AES}$	: AEB-to-AES transition request
F_{tr}	: transition-violation precursor flag
F_{mode}	: mode-persistence precursor flag
$F_{\mathrm{mon,tr}}$	: integrated transition monitoring flag
P_{δ}	: steering-feasibility guard flag
V_{tr}	: transition-timeliness validity flag
I_{col}	: collision occurrence flag
v_{imp}	: ego absolute longitudinal velocity at collision, m/s
Δt_{rec}	: recovery latency of the safety mechanism, s

1. 서 론

자동차 안전 기술은 사고 발생 후 상해를 완화하는 수동안전(Passive safety)을 넘어 충돌 이전에 위험을 판단하고

*Corresponding author, E-mail: hclee@hanyang.ac.kr

This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/licenses/by-nc/3.0) which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

차량 거동을 제어하는 능동 안전(Active safety) 기능으로 확장되고 있다.[1] 자율주행차 및 첨단 운전자 보조 시스템(Advanced Driver Assistance Systems, ADAS)에서 자동긴급제동(Autonomous Emergency Braking, AEB)과 자동긴급조향(Autonomous Emergency Steering, AES)은 충돌 임박 상황에서 직접 개입하는 대표적인 사고회피 기능이다.[2,3] AEB는 종방향 감속을 통해 충돌을 회피하거나 충돌 속도를 저감하며, AES는 자차 속도가 높거나 가용 제동 거리가 짧아 제동만으로 회피가 어려운 조건에서 횡방향 회피 경로를 제공한다.[4]

AEB와 AES를 연계 운용하기 위한 방식으로 순차형(Sequential) 또는 계층형(Hierarchical) 의사결정 구조가 사용될 수 있다.[5,6] 이러한 구조에서는 충돌까지의 시간(Time-To-Collision, TTC), 차두시간(Time Headway, THW), 상대 거리 및 상대 속도와 같은 지표를 바탕으로 충돌 위험을 판단한다.[7-9] 충돌 위험이 임계 수준에 도달하면 시스템은 우선 AEB 개입 여부를 판단하고 제동만으로 충돌 회피가 불충분하다고 판단되는 경우에 한하여 AES 개입 가능성을 고려한다. 이때 제동 회피 가능성은 제동 위협 지수(Braking Threat Number, BTN), 조향 회피 가능성은 조향 위협 지수(Steering Threat Number, STN)를 통해 평가될 수 있다.[10-12] 제동 우선(Braking-first) 구조는 제어 로직의 기능 경계를 명확히 하고 기능안전 분석에서 제어동작과 상태 천이 조건을 구분하기 용이하다.

그러나 순차형 AEB/AES 구조는 회피 가능 시간이 제한되는 Time-critical 상황에서 기능안전상 취약성을 가질 수 있다. 조향 회피는 제동 불충분 판단 이후에 고려되므로 AEB에서 AES로의 이산적 상태 천이(Discrete mode transition) 과정에서 제어 명령의 불연속성 또는 개입 지연이 발생할 수 있다.[13,14] 제동만으로는 회피가 불충분하지만 조향 회피는 가능한 임계 조건에서 AES 요청 또는 상태 천이 요청이 허용 시간 내에 제공되지 않으면 조향 회피 기회가 제한된다. 이 취약성은 단일 부품의 고장 모드만으로 설명되기 어렵다. 인지 지연, 위험 판단 지연, AES 요청 신호의 누락, AES 활성화 신호의 비활성 고착, AEB 활성 상태의 모드 고착 등 서로 다른 하위 인과 경로가 존재하지만 이들은 모두 해당 임계 조건에서의 상태 천이 지연 또는 실패라는 동일한 비안전 제어동작(Unsafe Control Action, UCA)으로 수렴한다. 따라서 순차형 구조의 한계는 사고회피 성능 저하가 아니라 제어 명령의 제공 여부, 제공 시점, 중재 판단 및 상태 천이 실패와 관련된 기능안전 문제로 다루어져야 한다.

UN Regulation No. 157에서 고려되는 Cut-in 유형의 시나리오는 이러한 천이 취약성을 분석하기에 적합한 대표적 운용 상황이다.[15] Cut-in 상황에서는 인접 차로의 대상 차량이 자차 주행 경로로 진입하면서 종방향 접근 위험과 횡방향 침범 위험이 동시에 증가하며, 이때 AES 요청이 누락되거나 AEB 활성 상태가 상태 천이를 차단하면 충돌, 충돌 속도 증가, 차로 이탈 또는 차량 안정성 상실로 이어질 수 있다. 기존 사고회피 연구는 위험 판단 지표를 이용한 개입 시점 결정 또는 모델예측제어(Model Predictive Control, MPC)를 이용한 제동·조향 통합 제어 성능 향상에 초점을 두어 왔다.[16-18] 그러나 기능안전 관점에서는 새로운 통합 제어기의 성능 제시와 독립적으로 기존 순차형 AEB/AES 기능이 어떠한 조건에서 UCA를 생성하는지, 서로 다른 원인이 어떻게 동일한 천이 고장 집합(Fault set)으로 수렴하는지, 그리고 이를 표준 기반 안전목표와 안전 메커니즘으로 어떻게 연결할 것인지에 대한 분석이 필요하다.

다수 구성요소의 상호작용에서 비롯되는 위험은 고장 모드 목록만으로는 충분히 분석하기 어렵다. 시스템 이론 기반 위험 분석 기법인 STPA(System-Theoretic Process Analysis)는 제어 명령의 미제공, 오제공, 지연 제공 및 중지 실패를 구조적으로 도출할 수 있으므로 판단, 중재 및 상태 천이가 결합된 순차형 AEB/AES의 기능안전 분석에 적합하다.[19] 본 연구에서는 STPA로 도출한 UCA와 인과 시나리오(Causal scenario)를 ISO 26262의 위험원 분석 및 위험성 평가(Hazard Analysis and Risk Assessment, HARA)의 오작동 거동, 위험 사건, ASIL 평가 및 안전목표 도출 과정과 연계하고, 안전목표 위반을 방지 또는 완화하기 위한 안전 메커니즘으로 변환한다.[20,21]

본 연구의 목적은 순차형 AEB/AES 기능에 내재된 상태 천이 취약성을 기능안전 관점에서 분석하고, 이를 완화하기 위한 안전 메커니즘(Safety mechanism)을 설계하여 R157 cut-in 시나리오의 고장 주입(Fault injection)으로 검증하는 데 있다.

본 논문의 주요 기여는 다음 네 가지이다. 첫째, 서로 다른 하위 인과 경로가 상태 천이 지연 또는 실패라는 동일한 UCA로 수렴함을 STPA로 분석하고 이를 순차 구조 고유의 구조적 고장 집합으로 정의한다. 둘째, 분석 결과를 기능안전 표준 절차와 연계하여 AES 요청 및 상태 천이 요청의 적시 제공을 핵심 안전목표로 도출하고, 조향 제어 개입 타당성이 확보되지 않는 경우 천이 보정을 억제해야 한다는 조건을 함께 제시한다. 셋째, 천이 위반 전조를 기본 중재 출력 이후에 관측 가능한 요청, 모드 및 시간 조건으로 재평가하고 조향 제어 개입 타당성이 확인되는 경우에 한하여 보정하는 안전 메커니즘을 설계한다. 넷째, R157 cut-in 고장 주입 검증을 통해 정상 조건, 고장 주입 조건 및 안전 메커니즘 적용 조건을 비교하여 요청 보정이 상태 천이 고장을 완화하는지를 평가한다.

본 논문은 2장에서 순차형 AEB/AES 기능의 항목 정의, 3장에서 STPA-HARA 기반 안전 분석, 4장에서 안전 메커니즘 설계, 5장에서 R157 cut-in 기반 고장 주입 검증을 다루고 6장에서 결론을 제시한다.

2. 순차형 AEB/AES 사고회피 시스템 정의

본 장에서는 STPA 기반 위험 분석과 ISO 26262 기반 HARA를 수행하기 위하여 분석 대상인 순차형 AEB/AES 사고회피 기능을 항목(Item)으로 정의한다. 본 항목은 안전 메커니즘이 적용되기 전의 기본 기능이며, 안전 메커니즘은 3장에서 도출되는 안전목표를 만족하기 위해 항목 분석 이후 추가되는 보정 계층으로서 4장에서 정의한다.

2.1 분석 대상 및 시스템 경계

본 연구의 분석 대상 항목은 자율주행차 또는 ADAS 차량에 탑재되는 순차형 AEB/AES 사고회피 기능이다. 해당 기능은 충돌 위험이 임계 수준에 도달한 상황에서 AEB 또는 AES 중 하나의 긴급 개입 요청을 생성하여 충돌을 회피하고, 회피가 물리적으로 불가능한 경우 충돌 속도를 저감한다. 이때 AES는 AEB와 독립적으로 활성화되지 않고 제동 가능성 평가 이후에 선택적으로 고려되므로, 본 항목은 AEB와 AES가 동시에 활성화되지 않는 배타적 모드 선택(Exclusive mode selection) 구조로 한정한다. 항목의 기능 요소는 인지/추적 인터페이스, 위험 판단, AEB 판단, 제동 가능성 평가, AES 판단, AEB/AES 중재 및 상태 천이, 명령 생성으로 구성되며 각 요소의 역할은 Table 1과 같다.

Table 1 Functional components of the sequential AEB/AES item

No.	Functional component	Primary role
1	Perception/ tracking interface	Receives object, lane, and ego-state information from external modules
2	Risk assessment	Evaluates collision risk and the need for emergency intervention
3	AEB decision logic	Determines whether an AEB request is required under critical risk
4	Braking feasibility assessment	Evaluates braking-only avoidance feasibility based on BTN
5	AES decision logic	Evaluates the feasibility of steering avoidance when braking is insufficient
6	AEB/AES arbitration and mode transition	Selects the final intervention mode and determines AEB-to-AES transition
7	Command generation	Outputs braking or steering commands to the actuator interface

본 항목의 시스템 경계는 안전 메커니즘 적용 전의 순차형 AEB/AES 의사결정 및 명령 생성 기능으로 한정하며, 항목 외부 기능에서 제공되는 상대 상태, 차선 경계 및 현재 모드 정보는 항목의 입력으로 사용한다. 포함 및 제외 범위는 Table 2와 같다.

Table 2 System boundary of the sequential AEB/AES item

Element	Scope	Definition in this study
Risk assessment / AEB / AES decision logic	Included	Determines collision risk and generates AEB or AES request
BTN-based braking feasibility assessment	Included	Determines braking-only avoidance feasibility
AEB/AES arbitration and mode transition logic	Included	Selects the final intervention mode and determines AEB-to-AES transition
Command generation	Included	Generates braking or steering requests for the actuator interface
Perception/tracking input interface	Included	Receives object, lane, and ego-state information from external modules
Sensor raw data processing	Excluded	Raw sensor data processing is treated as an external function
Object and lane recognition	Excluded	Object detection, tracking, and lane recognition are external functions
Brake/steering actuator dynamics	Excluded	Physical actuator dynamics and hardware faults are out of scope
Vehicle dynamics	Excluded	Treated as the controlled plant and feedback path
Safety mechanism	Excluded	Logical safety gate added after item analysis, defined in Chapter 4
Integrated AEB+ AES controller / fallback mode	Excluded	Joint optimization controller, fallback, and degraded mode are out of scope

이러한 경계 설정에 따라 본 연구는 센서 및 액추에이터의 하드웨어 고장을 직접 분석 범위에서 제외하고, 항목 내부의 판단 지연, 판단 누락, 부적절한 중재, 상태 천이 실패 및 명령 생성 오류를 분석 대상으로 한다. 인지 지연, 상대 거리 및 상대 속도 추정 오류, 차선 경계 오류, 현재 모드 피드백 불일치와 같은 입력 이상은 항목 외부에서 유입되는 원인으로 간주하되, 순차형 판단 오류와 결합하여 UCA를 유발할 수 있으므로 3장의 인과 시나리오에서 고려한다.

2.2 입력·출력 및 위험 판단 지표

순차형 AEB/AES 기능의 입력은 자차 상태, 대상 차량 상태, 차선 정보, 위험 판단 지표 및 현재 모드로 구성되며, 출력은 AEB 요청, AES 요청, 상태 천이 요청, 중재 모드, 제동 명령 및 조향 명령으로 구성된다.

$$\mathbf{x}_{in} = [v_e,\ a_e,\ d_x,\ v_x,\ d_y,\ v_y,\ y_L,\ y_R,\ R_{crit},\ BTN,\ STN,\ M]^{\mathrm{T}} \tag{1}$$

여기서 v_e와 a_e는 자차의 종방향 속도 및 가속도, d_x와 d_y는 대상 차량과의 상대 종방향 및 횡방향 거리, v_x와 v_y는 상대 종방향 및 횡방향 속도, y_L과 y_R은 좌우 차선 경계, M은 현재 기능 모드이다. 이때 상대 종방향 속도는 $v_x = v_t - v_e$로 정의하며 v_t는 대상 차량의 종방향 속도이다. R_{crit}, BTN, STN은 각각 충돌 위험, 제동 회피 가능성 및 조향 회피 가능성 판단에 사용되는 지표이다. M은 위험 판단 지표 계산에는 직접 사용되지 않지만, AEB 활성 상태에서 AES 활성 상태로의 천이 필요성을 판단하기 위한 모드 피드백 입력으로 사용된다.

$$\mathbf{y}_{out} = [AEB_{req},\ AES_{req},\ M_{tr}^{AEB\rightarrow AES},\ Arb_{mode},\ a_{cmd},\ \delta_{cmd}]^{\mathrm{T}} \tag{2}$$

식 (2)의 각 성분은 다음과 같이 정의한다. AEB_{req}와 AES_{req}는 각각 AEB 개입 및 AES 개입을 요구하는 이진 요청 플래그이고, $M_{tr}^{AEB\rightarrow AES}$는 AEB 활성 상태에서 AES 활성 상태로의 천이 요청 신호로서 그 생성 조건은 식 (8)에서 정의한다. Arb_{mode}는 AEB/AES 중재 로직이 선택한 현재 제어 주기에서 선택한 기능 모드로서 Table 3의 모드 집합 $\{M_0, M_1, M_2, M_3\}$ 중 하나의 값을 가진다. 이때 식 (1)의 입력 M은 직전 제어 주기에서 확정된 현재 모드 피드백이고 Arb_{mode}는 현재 주기의 중재 결과로 새로 선택된 모드 출력이므로, 두 신호는 동일한 모드 집합을 공유하되 관측 시점에서 구분된다. 마지막으로 a_{cmd}는 제동 액추에이터 인터페이스로 전달되는 종방향 감속도 명령이며 δ_{cmd}는 조향 액추에이터 인터페이스로 전달되는 조향각 명령이다.

Table 3 Operational modes of the sequential AEB/AES function

Mode	Mode name	Activation condition
M_0	No intervention	C_0
M_1	AEB active	C_1 or C_3
M_2	AES evaluation	$R_{crit} = 1$ and $B_{inf} = 1$
M_3	AES active	C_2

유효 종방향 거리 d_{eff}의 경우, L_e와 L_t는 각각 자차와 대상 차량의 길이이며 d_s는 종방향 안전 여유 거리이다. v_{cl}은 상대 종방향 속도 중 두 차량 간 종방향 거리가 감소하는 경우의 속도 크기를 나타낸다. v_x의 음수값은 두 차량 간 종방향 거리가 감소함을 의미하고 식 (3)과 같이 정의한다.

$$d_{eff} = d_x - \frac{L_e + L_t}{2} - d_s, \qquad v_{cl} = \max(-v_x,\ 0) \tag{3}$$

등속 상대 운동을 가정한 충돌까지의 시간과 충돌 위험 임계 상태는 식 (4)와 같이 정의한다. Cut-in 상황에서는 종방향 TTC만으로 위험을 충분히 표현하기 어렵기 때문에 대상 차량이 자차 주행 영역에 존재하거나 해당 영역으로 진입 중임을 나타내는 Lateral gating 조건 G_{lat}을 함께 사용한다.

$$TTC = \begin{cases} \dfrac{d_{eff}}{v_{cl}}, & d_{eff} > 0,\ v_{cl} > 0 \\ 0, & d_{eff} \le 0 \\ \infty, & d_{eff} > 0,\ v_{cl} = 0 \end{cases}, \qquad R_{crit} = \begin{cases} 1, & TTC \le TTC_{th} \wedge G_{lat} = 1 \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

제동 회피 가능성은 요구 감속도와 가용 감속도의 비율인 BTN으로 평가한다. BTN이 임계값 이상이면 제동만으로 회피가 불충분한 상태로 판단한다.

$$a_{brake,req} = \frac{v_{cl}^2}{2\,d_{eff}}, \quad a_{brake,avail} = \min(\mu g,\ a_{brake,max}), \quad BTN = \frac{a_{brake,req}}{a_{brake,avail}}, \quad B_{inf} = \begin{cases} 1, & BTN \ge BTN_{th} \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

여기서 $a_{brake,req}$는 유효 종방향 거리 내에서 충돌을 회피하는 데 요구되는 감속도이고 $a_{brake,avail}$은 노면 마찰 한계와 제동 시스템 성능 한계를 함께 고려한 가용 감속도이다. μ는 노면 마찰계수, g는 중력가속도, $a_{brake,max}$는 제동 시스템이 제공 가능한 최대 감속도이며, BTN_{th}는 제동 불충분 판정을 위한 BTN 임계값이다.

조향 회피 가능성은 요구 횡방향 이동량, 조향 가능 시간 및 가용 횡가속도를 이용하여 평가한다.

$\hat{y}_e$는 AES 개입을 가정하여 조향 가능 시간 T_{steer} 이후에 예측되는 자차 중심의 횡방향 위치이며, 차선 경계 y_R 및 y_L과 동일한 차선 기준 좌표계에서 정의한다. $[y_R + y_s,\ y_L - y_s]$는 횡방향 안전 여유 y_s를 제외한 허용 회피 영역이다.

$$\Delta y_{req} = \max\left(0, \frac{W_e + W_t}{2} + y_s - |d_y|\right),$$
$$a_{lat,req} = \frac{2\,\Delta y_{req}}{T_{steer}^2},$$
$$a_{lat,avail} = \min(\mu g,\ a_{lat,max}), \tag{6}$$
$$STN = \frac{a_{lat,req}}{a_{lat,avail}},$$
$$S_{feas} = \begin{cases} 1, STN \le STN_{th} \wedge \hat{y}_e \in [y_R + y_s,\ y_L - y_s] \\ 0, \text{otherwise} \end{cases}$$

여기서 Δy_{req}는 충돌 회피에 요구되는 최소 횡방향 이동량이고 W_e와 W_t는 각각 자차와 대상 차량의 폭, y_s는 횡방향 안전 여유 거리이다. $a_{lat,req}$는 조향 가능 시간 T_{steer} 이내에 Δy_{req}를 확보하는 데 요구되는 횡가속도이고 $a_{lat,avail}$은 노면 마찰 한계와 차량 안정성 한계를 함께 고려한 가용 횡가속도이며 $a_{lat,max}$는 차량 안정성 관점의 최대 허용 횡가속도이다. STN_{th}는 조향 회피 가능 판정을 위한 STN 임계값이다.

식 (4)~(6)의 $R_{crit}, B_{inf}, S_{feas}$는 이후 순차형 판단 로직, STPA의 UCA 도출 및 안전 메커니즘의 모니터링 조건을 정의하기 위한 기본 변수로 사용된다.

2.3 순차형 판단 로직 및 모드 정의

충돌 위험이 임계 수준에 도달하면 AEB를 우선 판단하고, 제동만으로 회피가 가능한 경우 AEB를 최종 개입 모드로 선택한다. 제동만으로 회피가 불충분하며 조향 회피가 가능한 경우에는 AES 요청 및 상태 천이 요청을 허용 시간 내 제공해야 한다. 기능안전 분석을 위한 핵심 상황 조건은 식 (7)과 같이 정리한다.

$$C_0: R_{crit} = 0,$$
$$C_1: R_{crit} = 1 \wedge B_{inf} = 0,$$
$$C_2: R_{crit} = 1 \wedge B_{inf} = 1 \wedge S_{feas} = 1, \tag{7}$$
$$C_3: R_{crit} = 1 \wedge B_{inf} = 1 \wedge S_{feas} = 0$$

식 (7)은 충돌 위험과 제동 및 조향 회피 가능성에 따라 구분한 판단 조건이다. C_0는 충돌 위험이 임계 수준에 도달하지 않은 조건이고, C_1은 충돌 위험이 임계 수준이지만 제동으로 회피 가능한 조건이다. C_2는 제동만으로 회피가 불충분하나 조향 회피가 가능한 조건이며, C_3는 제동만으로 회피가 불충분하고 조향 회피도 가능하지 않은 조건이다. 이 중 C_2는 본 연구의 핵심 임계 조건이다. C_2 조건에서 AES 요청 또는 상태 천이 요청이 적시에 제공되지 않으면 조향 회피가 가능한 시간이 제한될 수 있다. 이 조건은 3장 STPA의 UCA 도출과 4장 안전 메커니즘 설계의 기준이 된다.

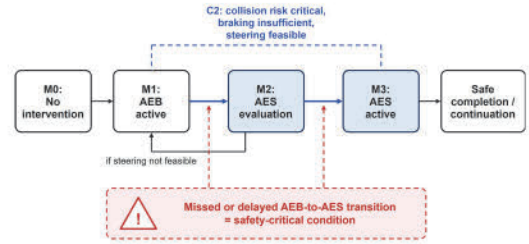


Fig. 1 State transition diagram of the sequential AEB/AES function

M_2는 최종 개입 모드가 아니라 제동 불충분 조건에서 조향 가능성을 평가하는 일시 상태로 정의한다. $S_{feas} = 1$이 확인되어 C_2가 성립하는 경우에는 M_3로 천이하고 $S_{feas} = 0$인 경우에는 C_3로 분류되어 M_1을 유지한다.

AEB 상태에서 AES 상태로의 천이 요청 신호는 식 (8)과 같이 정의한다.

$$M_{tr}^{AEB \to AES}(k) = \begin{cases} 1, & M(k-1) = M_1 \ \wedge\ C_2 = 1 \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

식 (8)은 순차형 구조의 천이 조건을 나타낸다. 이전 모드가 AEB 활성이고 현재 조건이 C_2이면 AES 요청 또는 상태 천이 요청이 제공되어야 하며, 이 요청이 누락되거나 지연되면 조향 회피가 필요한 상황에서도 AEB 단독 개입이 유지될 수 있다.

2.4 운용 조건 및 분석 가정

본 연구의 주요 운용 상황은 R157에서 고려되는 Cut-in 시나리오이며, 해당 조건에서 순차형 AEB/AES 기능의 위험 판단, 제동 및 조향 회피 가능성 평가, 상태 천이 특성을 분석한다. 기능안전 분석을 위한 운용 조건과 가정은 Table 4와 같다.

본 연구의 분석 가정은 다음과 같다. 첫째, 자차는 차선 경계가 인식 가능한 도로에서 주행하며, Cut-in 대상 차량의 상대 위치, 상대 속도 및 횡방향 이동 정보는 인지/추적 인터페이스를 통해 제공된다. 둘째, 제동 및 조향 액추에이터는 상위 요청을 수행 가능한 정상 상태로 가정하고, 액추에이터 하드웨어 고장은 분석 범위에서 제외한다. 셋째, 본 연구는 제동·조향 동시 최적화 제어기 또는 MRM(Minimal Risk Maneuver)/MRC(Minimal Risk Condition) 전체 설계를 제안하지 않는다.

Table 4 Operating conditions and analysis assumptions

Item	Definition or assumption
Road condition	Straight or low-curvature road with recognizable lane boundaries
Main scenario	R157 cut-in scenario under medium- and high-speed conditions
Base function	Braking-first sequential AEB/AES logic without simultaneous AEB+AES activation
Fault scope	Decision delay, request omission, request delay, arbitration delay, and mode-transition failure
Verification use	Fault injection is evaluated in Chapter 5 using scenarios where the normal sequential function is collision-free
HARA basis	ASIL evaluation is performed in Chapter 3 based on the item definition, operational situation, and STPA results

본 연구의 분석 가정은 다음과 같다. 첫째, 자차는 차선 경계가 인식 가능한 도로에서 주행하며, Cut-in 대상 차량의 상대 위치, 상대 속도 및 횡방향 이동 정보는 인지/추적 인터페이스를 통해 제공된다. 둘째, 제동 및 조향 액추에이터는 상위 요청을 수행 가능한 정상 상태로 가정하고, 액추에이터 하드웨어 고장은 분석 범위에서 제외한다. 셋째, 본 연구는 제동·조향 동시 최적화 제어기 또는 MRM(Minimal Risk Maneuver)/MRC(Minimal Risk Condition) 전체 설계를 제안하지 않는다.

3. STPA-HARA 기반 안전 분석

본 장에서는 2장에서 정의한 순차형 AEB/AES 사고회피 기능을 대상으로 STPA 기반 위험 분석을 수행하고 그 결과를 ISO 26262의 HARA 절차와 연결한다. 본 장의 목적은 모든 잠재 위험을 동일 수준으로 상세화하는 것이 아니라, C_2 조건에서 AES 요청 또는 상태 천이 요청이 적시에 제공되지 않는 공통 오작동으로 수렴하는 주요 UCA와 고장 집합을 도출하는 데 있다.

3.1 STPA 제어 구조, 손실 및 위험원 정의

순차형 AEB/AES 기능의 제어 구조는 Fig. 2와 같이 환경 및 대상 차량, 인지/추적 인터페이스, 위험 판단, AEB 판단 로직, BTN 기반 제동 가능성 평가, AES 판단 로직, AEB/AES 중재 및 상태 천이 로직, 제동·조향 액추에이터 인터페이스, 자차 동역학 및 피드백 경로로 구성된다.

본 연구에서 고려하는 시스템 수준 손실은 인명 상해, 차량 충돌, 차로 이탈 또는 차량 안정성 상실, 불필요한 긴급 개입으로 인한 2차 위험이다. 위험원은 이러한 손실로 이어질 수 있는 차량 수준의 비안전 상태로 정의하며, 본 연구에서 고려하는 위험원은 다음과 같다. H1은 AEB

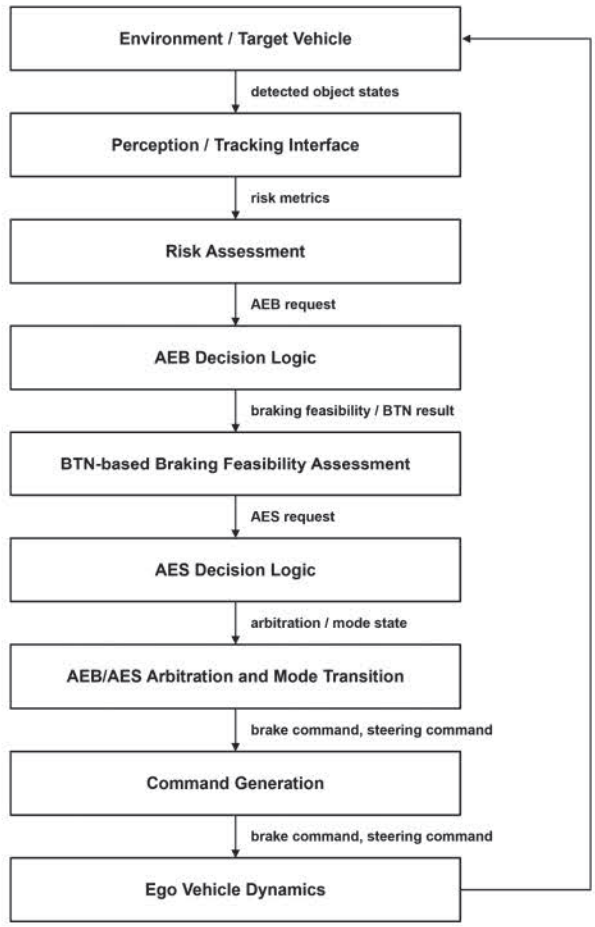


Fig. 2 STPA control structure of the sequential AEB/AES function

개입 지연으로 충분한 감속이 확보되지 못한 상태, H2는 C2C_2 C2 조건에서 조향 회피 가능 시간이 감소한 상태, H3는 AEB 단독 개입이 유지되어 충돌 회피가 불가능한 상태, H4는 고속 Cut-in 조건에서 충돌 속도가 증가한 상태, H5는 AES 조향 명령으로 차로 이탈 또는 차량 안정성 저하가 초래된 상태, H6는 불필요한 긴급 개입으로 2차 위험에 노출된 상태이다. 이 중 H2와 H3는 본 연구의 핵심 위험원이며, 이를 유발하는 부적절한 제어동작은 3.2절에서 UCA로 도출한다.

Table 5의 제어동작 중 본 연구의 중심은 C2C_2 C2 조건에서 허용 시간 내 제공되어야 하는 AES_{req}와 $M_{tr}^{AEB\rightarrow AES}$이다.

3.2 Unsafe Control Action 및 인과 시나리오 도출

본 절에서는 Table 5의 제어동작을 대상으로 미제공, 부적절한 제공, 제공 시점 오류 및 지속시간 오류의 관점에서 UCA를 도출하고 각 UCA를 유발할 수 있는 제어 구조상의 원인 경로를 인과 시나리오로 정리한다.

Table 5 Control actions of the sequential AEB/AES function

ID	Control action	Symbol	Unsafe relevance
CA-1	Provide AEB request	AEB_{req}	Omission or delay reduces initial deceleration margin.
CA-2	Provide AES request	AES_{req}	Omission or delay reduces steering avoidance time under C2.
CA-3	Provide AEB-to-AES transition request	$M_{tr}^{AEB\rightarrow AES}$	Omission or delay keeps the function in AEB active state.
CA-4	Provide braking command	a_{cmd}	Insufficient or excessive braking affects collision speed and stability.
CA-5	Provide steering command	δ_{cmd}	Incorrect or excessive steering may violate lane or stability constraints.

$$UCA_{AEB,omit}: R_{crit} = 1 \wedge AEB_{req} = 0 \quad (9)$$

$$UCA_{AES,omit}: C_2 = 1 \wedge AES_{req} = 0 \quad (10)$$

$$UCA_{AES,delay}: C_2 = 1 \wedge \left(t_{AES} - t_{C_2} > T_{AES,allow}\right) \quad (11)$$

$$UCA_{tr}: C_2 = 1 \wedge \left(M_{tr} = 0 \vee t_{tr} - t_{C_2} > T_{tr,allow}\right) \quad (12)$$

식 (9)는 충돌 위험이 임계 수준임에도 AEB 요청이 제공되지 않는 경우를 나타낸다. 식 (10)과 식 (11)은 C_2 조건에서 AES 요청이 제공되지 않거나 허용 시간보다 늦게 제공되는 경우이다. 식 (12)는 AEB 활성 상태에서 AES 상태로의 천이 요청이 누락되거나 지연되는 경우를 나타낸다. 여기서 t_{C_2}는 C_2 조건이 천이 판단 조건으로 유효하게 확정된 시점이고 t_{AES}와 t_{tr}은 각각 AES 요청과 상태 천이 요청이 최초로 제공된 시점이다. $T_{AES,allow}$와 $T_{tr,allow}$는 C_2 성립 이후 각 요청의 제공에 허용되는 최대 지연 시간이며 $T_{tr,allow}$의 산출식은 4장 식 (20)에서 정의한다. UCA-2~UCA-4는 서로 다른 제어 구조 위치에서 발생하지만 차량 수준에서는 조향 회피 가능 시간의 감소라는 공통 결과로 수렴한다.

Table 6에서 UCA-2, UCA-3 및 UCA-4가 본 연구의 중심 UCA이다. UCA-1은 후속 조향 회피 시간 여유를 감소시키는 선행 위험으로 고려하며, UCA-5는 천이가 수행된 후 조향 명령이 차량 안정성, 차선 경계 또는 회피 공간 제약을 위반할 수 있는 위험으로서 4장의 조향 제어 개입 타당성 조건과 연결된다.

Table 6 Unsafe control actions and representative causal scenarios

UCA ID	Unsafe control action	Unsafe context	Representative causal scenario	Related hazard
UCA-1	AEB request is not provided or is delayed.	$R_{crit} = 1$	Risk assessment delay; AEB request output delay; incorrect suppression of AEB request.	H1, H2
UCA-2	AES request is not provided.	$C_2 = 1$	AES enable stuck-off; steering-feasibility false-negative; arbitration suppresses AES.	H2, H3
UCA-3	AES request is provided later than the allowable time.	$C_2 = 1$	C2 recognition delay; AES output delay; arbitration transition delay.	H2, H3
UCA-4	AEB-to-AES transition request is not provided or is delayed.	$M(k-1) = M_1$ (AEB Active) and $C_2 = 1$	AEB mode stuck; transition latch failure; transition condition not updated.	H3, H4
UCA-5	Steering command is incorrect or excessive.	AES active	Lane-boundary margin not reflected; yaw-rate or lateral-acceleration limit ignored.	H5
UCA-6	AEB/AES intervention is provided under a non-critical condition.	$R_{crit} = 0$	False target; TTC false positive; lateral gating false positive.	H6

3.3 STPA-HARA 연계 및 안전목표 도출

STPA에서 도출한 UCA와 인과 시나리오는 HARA의 오작동 거동 및 위험 사건으로 변환한다. 본 연구에서는 UCA가 발생하는 운용 상황을 R157 cut-in 기반 중속 및 고속 조건으로 두고 각 위험 사건에 대해 심각도(S), 노출도(E) 및 제어가능성(C)을 정성적으로 평가한다. HARA 매핑은 식 (13)과 같이 표현할 수 있다.

$$HE_i = MB_i \wedge OS_i \wedge H_i \quad (13)$$

여기서 HE_i는 위험 사건, MB_i는 오작동 거동, OS_i는 운용 상황, H_i는 STPA에서 정의한 위험원이다. 오작동 거동은 MB-1(AEB 요청의 미제공 또는 지연), MB-2(AES 요청의 미제공 또는 지연), MB-3(AEB 활성 상태 지속으

로 인한 상태 천이 차단), MB-4(과도하거나 부적절한 조향 명령), MB-5(비임계 조건에서의 불필요 개입)로 정의하고, 운용 상황은 OS-1(중속 조건의 전방 차량 접근), OS-2(중속 및 고속 조건의 Cut-in 진입), OS-3(비임계 주행 조건)으로 정의한다.

HE-2부터 HE-5까지의 S/E/C는 다음 근거로 평가하였다. 심각도는 중·고속 Cut-in 조건에서 상태 천이 실패가 대상 차량과의 충돌로 이어져 생명을 위협하거나 치명적 상해를 유발할 수 있으므로 S3로 평가하였다. 노출도는 기능 고장의 발생 빈도가 아니라 해당 운용 상황에 대한 노출을 기준으로 하며 차로 추종 주행 중 인접 차량의 Cut-in은 대상 운용 영역에서 반복적으로 발생하므로 E4를 적용하였다. 제어가능성은 C_2가 성립한 시점에 이미 제동만으로 회피가 불충분하고 잔여 조향 회피 시간이 제한되어 운전자 또는 기본 기능이 추가로 충돌을 회피할 가능성이 낮으므로 C3로 평가하였다. 이에 따라 HE-2부터 HE-5까지를 S3/E4/C3 조합의 ASIL D로 분류하였다. HE-1은 AEB 개입 지연에 해당하는 위험 상황으로 천이 실패 이전 단계에서 조향 회피 가능성이 있어 후속 AES로 충돌을 완화할 여지가 있으므로 제어가능성을 C2로 평가하여 ASIL C로 분류하였다. HE-6과 HE-7은 각각 부적절한 조향 명령과 비임계 조건의 불필요 개입에 해당하며, 충돌 임박 상황이 아니어서 심각도와 노출도가 상대적으로 낮으므로 각각 S2/E3/C3의 ASIL B, S2/E3/C2의 ASIL A로 분류하였다.

Table 7 STPA-HARA mapping and preliminary safety goals

HE ID	MB / OS	Hazardous event	S/E/C → ASIL	Safety goal	Safety constraint
HE-1	MB-1 /OS-1	AEB request is not provided or is delayed during a critical approach.	S3/E4/C2 → C	SG-1: AEB request shall be provided within the allowable time under a critical collision risk.	SC-1
HE-2	MB-2 /OS-2	AES request is not provided under C2 in a cut-in situation.	S3/E4/C3 → D	SG-2: AES request or AEB-to-AES transition request shall be provided within the allowable time under C2.	SC-2
HE-3	MB-2 /OS-2	AES request is delayed beyond the allowable time under C2.	S3/E4/C3 → D	SG-2: AES request or AEB-to-AES transition request shall be provided within the allowable time under C2.	SC-2
HE-4	MB-3 /OS-2	AEB active state blocks AES evaluation or intervention under C2.	S3/E4/C3 → D	SG-3: AEB active state shall not block required AES evaluation or AEB-to-AES transition under C2.	SC-3
HE-5	MB-3 /OS-2	AEB-to-AES transition is blocked or delayed in a high-speed cut-in.	S3/E4/C3 → D	SG-3: AEB active state shall not block required AES evaluation or AEB-to-AES transition under C2.	SC-3
HE-6	MB-4 /OS-1, OS-2	Excessive or incorrect AES steering command causes lane-boundary violation or stability degradation.	S2/E3/C3 → B	SG-4: AES steering command shall not violate vehicle-stability, lane-boundary, or avoidance-space constraints.	SC-4
HE-7	MB-5 /OS-3	Unnecessary emergency intervention under a low-risk condition induces secondary risk.	S2/E3/C2 → A	SG-5: AEB or AES intervention shall not be provided under a non-critical condition.	SC-5

HE-2부터 HE-5까지가 ASIL D로 평가됨에 따라 이들에 대응하는 SG-2와 SG-3이 본 연구의 최상위 안전목표이며, 순차형 AEB/AES 구조의 천이 타이밍 취약성을 직접 다룬다. SG-4는 천이가 수행되더라도 조향 명령이 차량 안정성, 차선 경계 및 회피 공간 제약을 만족해야 함을 규정하며, 4장에서 안전 메커니즘의 요청 보정 허용 여부를 판단하는 조향 제어 개입 타당성 조건의 근거로 사용된다.

3.4 극한 조건 천이 고장 집합 선정

본 절에서는 3.2절의 UCA와 인과 시나리오, 3.3절의 예비 ASIL 및 안전목표를 종합하여 순차형 AEB/AES 구조의 극한 조건 천이 고장 집합을 선정한다. 여기서 극한 조건 천이 고장 집합은 단일 최고 위험 사건이 아니라, C_2 조건에서 SG-2와 SG-3을 동시에 위협하고 공통 상태 천이 오작동을 유발하는 원인 경로의 집합을 의미한다.

위험 판단, 제동 및 조향 회피 가능성 평가, AES 활성화 경로, AEB/AES 중재에서 발생하는 서로 다른 인과 경로는 C_2 조건에서 AES 요청 또는 상태 천이 요청이 허용 시간 내 제공되지 않는 공통 상태 천이 오작동으로 수렴한다.

본 연구에서는 UCA-2, UCA-3 및 UCA-4를 통합한 극한 조건 UCA를 UCA_{WC}로 표기하고 식 (14)와 같이 정의한다.

$$UCA_{WC}:\ C_2 = 1 \wedge \left(AES_{req} = 0 \vee t_{AES} - t_{C_2} > T_{AES,allow} \vee M_{tr} = 0 \vee t_{tr} - t_{C_2} > T_{tr,allow}\right) \tag{14}$$

식 (14)는 C_2가 성립하여 AES 천이가 요구되는 상황임에도 AES 요청이 생성되지 않거나, AES 요청이 허용 시간을 초과하여 지연되거나, 상태 천이 요청이 생성되지 않거나, 상태 천이가 허용 시간을 초과하여 수행되는 경우를 통합적으로 나타낸다. 식 (14)의 변수 및 파라미터는 식 (9)~(12)에서 정의한 바와 같다. 본 장의 C_2는 STPA-HARA 분석을 위한 상황 조건이며 4장에서 사용하는 $C_{2,mon}$은 동일한 관측 신호를 이용하여 C_2 성립을 실행 중 모니터링하기 위한 구현 조건으로 구분된다. 따라서 3장의 고장 집합은 분석상 원인 경로를 정리한 것이고 4장의 모니터링은 각 고장 원인을 직접 진단하기보다 안전목표 위반 전조를 관측한다.

Table 8 Worst-case AEB-to-AES transition fault set

ID	Representative cause path	Related UCA	Common effect	SG
FS-1	Risk assessment delay	UCA-1, UCA-2, UCA-3	Delayed AEB/AES intervention and reduced AES time margin	SG-1, SG-2
FS-2	Braking-insufficiency false-negative	UCA-2, UCA-3	AES evaluation is not initiated or is delayed	SG-2
FS-3	Steering-feasibility false-negative	UCA-2, UCA-4	AES is incorrectly suppressed under C_2	SG-2, SG-3
FS-4	AES enable stuck-off	UCA-2, UCA-3	AES request is not generated or is delayed	SG-2
FS-5	AEB mode stuck	UCA-4	AEB-to-AES transition is blocked	SG-3
FS-6	Mode transition delay	UCA-3, UCA-4	AEB-to-AES transition is delayed beyond the allowable time	SG-2, SG-3

Table 8의 고장 항목은 서로 다른 제어 구조 위치에서 발생하지만 모두 AES 요청 또는 상태 천이 요청의 누락 및 지연으로 수렴하므로, 본 연구는 이를 순차형 AEB/AES 구조의 극한 조건 천이 고장 집합으로 선정한다. 부적절한 조향 명령은 천이 고장 집합에 포함하지 않고 SG-4와 연결되는 조향 제어 개입 타당성 조건으로 분리하여 4장에서 다룬다.

본 절의 선정은 STPA-HARA 분석에 근거한 정성적 결과이며, 5장에서는 이 고장 집합의 모든 항목을 동일 수준으로 재현하기보다 4장에서 정의하는 모니터링 전조 F_{tr}와 F_{mode}에 대응하는 대표 고장을 선정하여 검증한다. 대표 고장은 AES 활성화 경로와 AEB 모드 유지 상태를 각각 대표하는 AES enable stuck-off 및 AEB mode stuck으로 설정한다. 따라서 5장의 고장 주입은 FS-1~FS-6 전체에 대한 완전 커버리지 검증이 아니라 공통 천이 위반 전조를 발생시키는 대표 고장 사례 검증으로 해석하며 $R_{crit}, B_{inf}, S_{feas}$ 자체의 미검출 또는 지연은 본 안전 메커니즘의 완전 보완 대상이 아니므로 핵심 고장 주입에서 제외한다.

4. 오작동 모니터링 및 안전 메커니즘 설계

본 장에서는 3장의 STPA-HARA 결과를 기반으로 순차형 AEB/AES 기능의 상태 천이 위반 전조를 실행 중 모니터링하고, 필요한 경우 최종 요청을 제한적으로 보정하는 안전 메커니즘을 설계한다.

4.1 설계 개념 및 적용 범위

본 메커니즘은 고장 원인을 세부 유형으로 분류하지 않고 서로 다른 천이 관련 고장이 공통으로 유발하는 기능 수준의 비정상 출력 거동을 모니터링한다. 따라서 모니터링 대상은 고장 근본 원인이 아니라 요청 누락, 요청 지연, 천이 누락 및 모드 지속 여부이다. 여기서 보정은 누락되거나 지연된 요청을 최종 출력단에서 생성하는 동작을 의미한다.

입력 신호는 기본 순차형 AEB/AES 기능이 사용하거나 출력하는 관측 가능한 신호로 한정된다. 따라서 본 연구는 별도 센서, 별도 ECU 또는 독립 인지 처리 경로를 전제하지 않으며, 공통원인고장에 대한 완전한 독립성도 가정하지 않는다. 또한 본 메커니즘은 액추에이터 하드웨어 진단과 Fail-operational 구조를 포함하지 않는다.

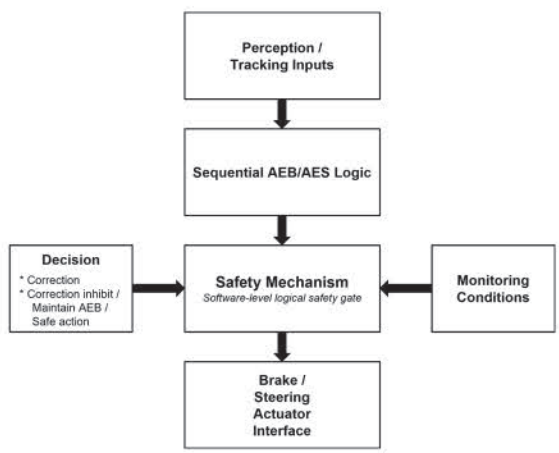


Fig. 3 Conceptual architecture of the proposed safety mechanism

Fig. 3은 기본 순차형 AEB/AES 로직의 출력이 논리적 안전 게이트를 통과하여 최종 출력으로 변환되는 구조를 나타낸다. 안전 게이트는 상태 천이 위반 모니터링과

조향 제어 개입 타당성 가드 및 요청 보정으로 구성된다.

4.2 천이 위반 전조 정의 및 실행 중 모니터링

천이 위반 모니터링은 2장 식 (7)의 C_2 조건을 실행 중 관측 가능한 신호로 재구성한 $C_{2,\mathrm{mon}}$을 이용하여 활성화하며 식 (15)와 같이 정의한다.

$$C_{2,\mathrm{mon}}(t) = R_{\mathrm{crit}}(t) \wedge B_{\mathrm{inf}}(t) \wedge S_{\mathrm{feas}}(t) \tag{15}$$

여기서 $C_{2,\mathrm{mon}}$은 C_2와 동일한 판정 논리를 안전 메커니즘이 실행 중 관측 가능한 신호로 재구성한 모니터링 조건이며, 지속성 확인 이전의 판단값이다. 단일 샘플의 판단 변동이 보정으로 이어지는 것을 방지하기 위해 $C_{2,\mathrm{mon}}$이 $N_{C_2,\mathrm{th}}$ 샘플 이상 연속 유지된 경우에 한하여 $C_{2,\mathrm{valid}}$로 확정한다. 이산 시간 k에서 $N_{C2}(k)$는 $C_{2,\mathrm{mon}} = 1$이 연속적으로 유지된 샘플 수이며, $C_{2,\mathrm{mon}} = 0$이면 0으로 초기화된다.

$$C_{2,\mathrm{valid}}(k) = \begin{cases} 1, & N_{C_2}(k) \geq N_{C_2,\mathrm{th}} \\ 0, & N_{C_2}(k) < N_{C_2,\mathrm{th}} \end{cases} \tag{16}$$

$$t_{C_2} = \min\{t \mid C_{2,\mathrm{valid}}(t) = 1\} \tag{17}$$

$$\tau_{C_2}(t) = t - t_{C_2} \tag{18}$$

여기서 $N_{C_2,\mathrm{th}}$는 C_2 조건의 지속성을 확인하기 위한 최소 연속 샘플 수이고 $C_{2,\mathrm{valid}}$는 $N_{C_2}(k) \geq N_{C_2,\mathrm{th}}$를 만족하여 유효성이 확인된 모니터링 조건이다. t_{C_2}는 $C_{2,\mathrm{valid}}$가 최초로 성립한 시점이며 τ_{C_2}는 해당 시점 이후의 경과 시간이다.

천이 허용 시간은 고정 경험값이 아니라 $C_{2,\mathrm{valid}}$ 성립 시점의 잔여 회피 시간에서 유도한다. T_{rem}은 t_{C_2}에서 산출한 보수적 잔여 회피 시간이고 T_{corr}는 모니터링·계산·전달·액추에이터 응답 지연을 포함하며 T_{margin}은 모델 오차와 판단 불확실성에 대한 여유 시간이다.

$$T_{\mathrm{lat,req}} = \sqrt{\frac{2\Delta y_{\mathrm{req}}}{a_{\mathrm{lat,avail}}}} \tag{19}$$

여기서 $T_{\mathrm{lat,req}}$는 충돌 회피에 필요한 횡방향 이동량을 확보하는 데 요구되는 시간이고, Δy_{req}는 충돌 회피에 필요한 최소 횡방향 이동량이며, $a_{\mathrm{lat,avail}}$은 조향 및 차량 안정성 한계를 고려한 가용 횡가속도이다. 이를 이용하여 허용 천이 시간은 식 (20)과 같이 정의한다.

$$T_{\mathrm{tr,allow}} = \max\big(0,\, T_{\mathrm{rem}}(t_{C_2}) - T_{\mathrm{lat,req}} - T_{\mathrm{corr}} - T_{\mathrm{margin}}\big) \tag{20}$$

여기서 $T_{\mathrm{tr,allow}}$는 t_{C_2} 이후 AES 요청 또는 상태 천이 요청에 허용되는 최대 지연 시간이다. 식 (20)은 요청이 단순히 지연되었는지가 아니라, 그 지연이 조향 회피 가능 시간을 소진하는지를 판단하는 시간 한계이다.

상태 천이 위반 전조는 $C_{2,\mathrm{valid}}$가 성립한 상황에서 AES 요청이 제공되지 않고 AES 활성 상태로의 천이도 완료되지 않은 채 허용 시간을 초과한 경우로 정의한다.

$$F_{\mathrm{tr}}(t) = 1 \quad \text{if} \quad C_{2,\mathrm{valid}}(t) = 1 \wedge AES_{\mathrm{req}}(t) = 0 \wedge M(t) \neq M_1 \wedge \tau_{C_2}(t) > T_{\mathrm{tr,allow}}(t) \tag{21}$$

여기서 M 는 Table 3에서 정의한 AES 활성 모드이다. $M(t) \neq M_{\mathrm{AES}}$ 조건은 상태 천이 요청이 순간 펄스로 제공된 후 현재값이 0으로 복귀하더라도 이미 AES 활성 상태로 천이가 완료된 경우에는 요청 누락으로 판정하지 않기 위한 것이다. AEB 활성 모드 M_1이 허용 시간보다 오래 유지되어 상태 천이를 차단하는 현상은 식 (22)의 모드 지속 전조로 모니터링한다.

$$\begin{aligned} &F_{\mathrm{mode}}(t) = 1, \\ &if\ C_{2,\mathrm{valid}}(t) = 1 \wedge M(t) \\ &= M_1 \wedge \tau_{C_2}(t) > T_{\mathrm{tr,allow}}(t) \\ &F_{\mathrm{mon,tr}} = F_{\mathrm{tr}} \vee F_{\mathrm{mode}} \end{aligned} \tag{22}$$

$F_{\mathrm{mon,tr}} = 1$이면 상태 천이 보정 후보 상태로 진입한다. 다만 보정 수행 여부는 4.3절의 조향 제어 개입 타당성 가드에서 결정된다. Table 9는 3장의 고장 집합이 본 절의 모니터링 조건으로 수렴하는 관계를 요약한다.

Table 9 Mapping between fault groups and runtime monitoring conditions

Fault group	Observed precursor	Monitoring condition
Delayed C_2 observation	Late monitor arming	Delayed $C_{2,\mathrm{valid}}$ activation
AES request omission or delay	Missing or late AES request	$F_{\mathrm{tr}} = 1$
AEB mode persistence	AEB mode remains active under C_2	$F_{\mathrm{mode}} = 1$
Arbitration transition delay	Late AEB-to-AES transition	$F_{mon,tr} = F_{tr}$ or F_{mode}

4.3 조향 제어 개입 타당성 가드 및 요청 보정

상태 천이 위반 전조가 검출되더라도 AES 요청 보정

이 항상 허용되는 것은 아니다. 조향 개입이 차량 안정성, 차선 경계 또는 회피 공간 조건을 만족하지 못하면 보정 자체가 SG-4의 위반으로 이어질 수 있다. 따라서 요청 보정은 $F_{\mathrm{mon,tr}} = 1$ 및 조향 제어 개입 타당성 $P_\delta = 1$이 동시에 만족되는 경우에만 허용한다.

$$\begin{aligned} &P_\delta(t) = 1 \text{ if } |\delta_{\mathrm{cmd}}(t)| \le \delta_{\max} \wedge |\hat{r}(t + T_{\mathrm{steer}})| \\ &\le r_{\max} \wedge \left|\hat{a}_y(t + T_{\mathrm{steer}})\right| \le a_{y,\max} \\ &\wedge\ \hat{y}_e(t + T_{\mathrm{steer}}) \in [y_R + y_s,\ y_L - y_s] \\ &\wedge O_{\mathrm{avoid}}(t + T_{\mathrm{steer}}) = 0 \end{aligned} \tag{23}$$

여기서 $\delta_{\max}$, $r_{\max}$ 및 $a_{y,\max}$는 각각 조향각, 요레이트 및 횡가속도의 안정 한계이고, $\hat{r}$과 $\hat{a}_y$는 예측 구간 T_{steer} 이후의 요레이트 및 횡가속도 예측값이며, O_{avoid}는 인접 차로 또는 의도된 회피 공간의 점유 여부를 나타낸다. 식 (23)의 조건 중 하나라도 만족되지 않으면 $P_\delta = 0$으로 판정한다.

P_δ는 기본 기능의 조향 회피 가능성 S_{feas}와 구분되는 보정 허용 조건이다. S_{feas}는 조향 회피가 물리적으로 가능한지를 판단하는 반면, P_δ는 안전 메커니즘이 요청을 보정하여도 조향 개입이 차량 안정성, 차선 경계 및 회피 공간 조건을 위반하지 않는지를 판단한다. 다만 회피 공간 점유 정보가 제공되지 않는 S1부터 S4까지의 조건에서는 $O_{\mathrm{avoid}} = 0$으로 가정하므로, $P_\delta = 1$ 판정은 회피 공간 점유를 독립적으로 검증한 결과가 아니라 제한된 검증 환경에서의 조향 제어 개입 타당성 판정으로 해석한다. S5에서는 인접 차량을 배치하여 $O_{\mathrm{avoid}} = 1$ 조건을 구성한다.

$$\mathbf{y}_{\mathrm{final}}(t) = \begin{cases} \mathbf{y}_{\mathrm{seq}}(t), & R_{\mathrm{crit}}(t) = 0 \text{ or } F_{\mathrm{mon,tr}}(t) = 0 \\ \mathbf{y}_{\mathrm{AES,corr}}(t), & R_{\mathrm{crit}}(t) = 1 \wedge F_{\mathrm{mon,tr}}(t) = 1 \\ & \wedge P_\delta(t) = 1 \\ \mathbf{y}_{\mathrm{AEB,maintain}}(t), & R_{\mathrm{crit}}(t) = 1 \wedge F_{\mathrm{mon,tr}}(t) = 1 \\ & \wedge P_\delta(t) = 0 \end{cases} \tag{24}$$

여기서 $\mathbf{y}_{\mathrm{seq}}$는 기본 순차형 AEB/AES 기능이 생성한 식 (2)의 출력으로 저위험 조건이거나 상태 천이 위반 전조가 검출되지 않으면 보정 없이 통과시킨다. $F_{\mathrm{mon,tr}}(t) = 1$이고 $P_\delta(t) = 1$이면 $P_\delta(t) = 1$ 및 $M_{\mathrm{tr,final}}^{\mathrm{AEB}\to\mathrm{AES}} = 1$을 포함하는 보정 출력 $\mathbf{y}_{\mathrm{AES,corr}}$를 적용하고, $P_\delta(t) = 0$이면 AES 요청과 상태 천이 요청의 보정을 억제하고 기본 AEB 요청을 유지하는 $\mathbf{y}_{\mathrm{AEB,maintain}}$을 적용한다. 이 분기는 조향 제어 개입 타당성이 확인되지 않은 상태 천이를 수행하지 않기 위한 설계 원칙이다.

4.4 상태 기계, 안전 상태 및 추적성

4.2절의 모니터링과 4.3절의 가드 및 출력 보정 동작은 Fig. 4의 상태 기계로 통합한다. 상태 간 천이는 $C_{2,\mathrm{valid}}$, $F_{\mathrm{mon,tr}}$, P_δ 및 R_{crit}에 의해 결정되며, 상태 천이 위반이 검출되면 P_δ에 따라 요청 보정 경로 또는 보정 억제 경로로 분기한다.

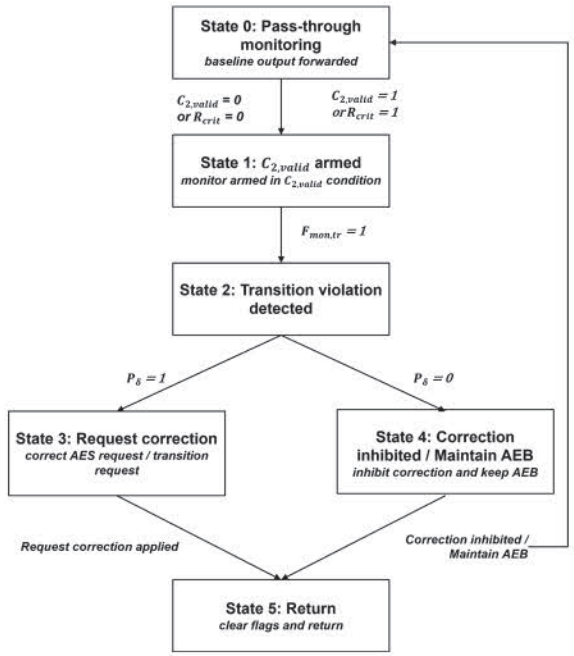


Fig. 4 State machine of the proposed safety mechanism

본 연구에서 안전 상태는 AES 활성 여부만으로 정의하지 않고 조향 제어 개입 타당성이 확인되어 천이 보정이 수행된 경우에 대해 천이 적시성, 차량 안정성, 차선 경계 및 회피 공간 조건이 동시에 만족되는 상태로 정의한다.

$$\begin{aligned} &SS_{design}(t) = V_{\mathrm{tr}}(t) \wedge V_{\mathrm{stab}}(t) \wedge V_{\mathrm{lane}}(t) \wedge V_{\mathrm{occ}}(t) \\ &V_{\mathrm{tr}}(t) = 1 \text{ if } C_{2,\mathrm{valid}}(t) = 1 \wedge P_\delta(t) = 1 \\ &\Rightarrow \left(AES_{\mathrm{req,final}}(t) = 1 \vee M_{\mathrm{tr,final}}^{\mathrm{AEB}\to\mathrm{AES}}(t) = 1\right) \end{aligned} \tag{25}$$

여기서 SS_{design}은 안전 메커니즘 설계에서 요구되는 설계상 안전 상태이며, 5장의 고장 주입 검증에서 사용하는 제한적 평가 지표 SS_{eval}과 구분한다. V_{stab}은 조향각, 요레이트 및 횡가속도가 안정 한계 이내임을, V_{lane}은 예측 횡방향 위치가 허용 회피 영역 이내임을, V_{occ}는 회피 공간이 점유되지 않았음을 의미한다. V_{tr}을 V_{tr}인 경우로 한정하는 이유는 $P_\delta = 0$에서 요청 보정이 억제되어 조향 회피에 의한 충돌 회피가 보장되지 않기 때문이며, 이때

안전 메커니즘은 안전 상태가 아니라 보정 억제 안전 동작 SA_{inh}를 수행한다.

Table 10 Traceability from STPA-HARA results to the safety mechanism

Safety goal	Violation precursor	Monitor or guard	Action	Safe state or safe action
SG-2	$F_{tr} = 1$	Transition timing monitor	Correct AES request and transition request	$V_{tr} = 1$
SG-3	$F_{mode} = 1$	Mode persistence monitor	Correct transition request	$V_{tr} = 1$
SG-4	$P_\delta = 0$	Steering plausibility guard	Inhibit AES correction and maintain AEB request	SA_{inh}
SG-5	$R_{crit} = 0$ with correction demand	Pass-through guard	No correction	$y_{final} = y_{seq}$

Table 10은 3장에서 도출한 안전목표가 본 장의 모니터링 조건, 보정 동작 및 판정 기준으로 연결되는 추적 관계를 정리한다. SG-2와 SG-3은 상태 천이 위반 전조의 검출과 요청 보정으로, SG-4는 조향 제어 개입 타당성 미확보 시의 보정 억제로, SG-5는 비임계 조건의 무보정 통과로 각각 반영된다.

5. R157 Cut-In 기반 고장 주입 검증

본 장에서는 R157 cut-in 조건에서 대표 상태 천이 고장을 주입하고, 정상 조건(G1), 고장 주입 조건(G2) 및 안전 메커니즘 적용 조건(G3)을 비교하여 상태 천이 고장에 따른 위험 확대와 안전 메커니즘의 완화 효과를 평가한다.

5.1 검증 시나리오 및 비교군

검증 조건은 2장에서 정의한 R157 cut-in 상황을 기반으로 구성한다. 자차 속도는 60 km/h의 중속 조건과 120 km/h의 고속 조건으로 설정하고, 대상 차량의 종방향 속도, 횡방향 속도 및 Cut-in 시작 시 종방향 거리를 변화시키며 매개변수 분석을 수행한다. 도로 및 액추에이터 조건에는 2.4절의 분석 가정을 적용하며, 매개변수 범위는 Table 11과 같다.

비교군은 Table 12와 같이 G1, G2 및 G3로 정의한다. 고장 주입 대상은 G1에서 충돌이 발생하지 않고 $C_{2,valid}$가 성립하는 경계 인접 조건에서 선정하며, 안전 메커니즘의 효과는 동일 고장 조건의 G2와 G3를 비교하여 평가한다.

Table 11 Parameter sweep conditions for the R157 cut-in scenario

Parameter	Case 1	Case 2
Ego longitudinal speed	60 km/h	120 km/h
Target longitudinal speed	10-50 km/h (10 km/h step)	10-110 km/h (10 km/h step)
Target lateral velocity	0.5-3.0 m/s (0.5 m/s step)	0.5-3.0 m/s (0.5 m/s step)
Cut-in longitudinal distance	10-120 m (10 m step)	10-120 m (10 m step)

Table 12 Comparison groups for fault injection verification

Group	Configuration	Purpose
G1	Normal sequential AEB/AES	Confirm collision-free baseline and select reference conditions
G2	Fault-injected sequential AEB/AES	Confirm transition violation or risk increase
G3	Fault-injected sequential AEB/AES with the safety mechanism	Confirm monitor-based correction or inhibition

5.2 정상 성능 경계 및 대표 시나리오 선정

G1의 매개변수 분석은 고장 주입 기준 조건을 선정하기 위해 수행한다. Table 11의 조건에서 얻은 정상 순차형 AEB/AES 기능의 충돌 여부 분포는 Fig. 5와 같다.

Fig. 5에서 충돌은 주로 Cut-in 시작 거리가 짧고 대상 차량의 종방향 및 횡방향 속도가 낮은 영역에 집중된다. 짧은 시작 거리는 잔여 회피 시간을 감소시키고, 낮은 횡방향 속도는 대상 차량이 자차 주행 경로에 머무는 시간을 증가시킨다. 120 km/h 조건에서는 동일한 Cut-in 시작 거리에서도 잔여 회피 시간이 짧아져 충돌 영역이 확대되며, 이는 고속 조건에서 상태 천이에 허용되는 시간 여유가 감소함을 의미한다.

대표 시나리오는 검증 목적에 따라 두 그룹으로 구분하여 선정한다. S1부터 S4까지는 요청 보정 분기를 평가하기 위한 시나리오로, 정상 조건 G1에서 충돌이 발생하지 않고, $C_{2,valid}$가 성립하며, 요청 보정 효과를 평가할 수 있도록 $P_\delta = 1$ 구간이 관측되고, Fig. 5의 충돌 경계에 인접한 조건을 사용한다. S5는 보정 억제 분기를 평가하기 위한 R157 cut-in 시나리오의 확장으로 동일한 조건에 인접 차량의 회피 공간 점유 조건을 추가하여 $P_\delta = 0$이 판정되는 상황을 구성한다. S5는 회피 공간이 점유되어 조향 보정 타당성이 확보되지 않는 조건을 평가하므로 S1부터 S4까지의 G1 무충돌 및 $P_\delta = 1$ 선정 기준을 적용하지 않는다.

Table 13의 대표 시나리오는 Fig. 5의 충돌 경계 근처에서 선정하였으며, G1의 $C_{2,valid}$, P_δ 및 I_{col}의 시뮬레이션

Table 13 Selected representative scenarios for fault injection verification

Scenario	Ego speed	Target long. speed	Target lat. velocity	Cut-in distance	Injected fault	Target flag
S1	60 km/h	10 km/h	2 m/s	25 m	AES enable stuck-off	F_{tr}
S2	60 km/h	10 km/h	2 m/s	25 m	AEB mode stuck	F_{mode}
S3	120 km/h	40 km/h	2.5 m/s	40 m	AES enable stuck-off	F_{tr}
S4	120 km/h	40 km/h	2.5 m/s	40 m	AEB mode stuck	F_{mode}
S5	60 km/h	10 km/h	2 m/s	25 m	AES enable stuck-off	F_{tr}

결과로 조건 성립을 확인하였다.

5.3 고장 주입 정의 및 평가지표

고장 주입은 천이 고장 집합의 모든 원인을 개별적으로 재현하지 않고, 4장에서 정의한 F_{tr}와 F_{mode}를 유발하는 대표 고장을 주입하는 방식으로 수행한다. 대표 고장은 AES 활성화 신호가 비활성으로 고착되는 AES enable stuck-off와 AEB 활성 상태가 유지되는 AEB mode stuck으로, 각각 F_{tr} 및 SG-2와 F_{mode} 및 SG-3에 대응한다. 두 고장과 4장 모니터링 및 안전목표의 대응 관계는 Table 14와 같다.

Table 14 Representative injected faults and corresponding monitoring paths

Representative fault	Target flag	Related safety goal	Meaning
AES enable stuck-off	F_{tr}	SG-2	AES request is not provided under C_2
AEB mode stuck	F_{mode}	SG-3	AEB active state blocks the AEB-to-AES transition

AES enable stuck-off는 $C_{2,\mathrm{valid}}$ 성립 이후 AES 활성 허가 신호와 AES 요청이 제공되지 않는 고장으로 식 (26)과 같이 구현한다.

$$AES_{\mathrm{enable}}^{\mathrm{fault}}(t) = 0, \quad AES_{\mathrm{req}}^{\mathrm{fault}}(t) = 0, \quad t \geq t_{C2} \tag{26}$$

AEB mode stuck은 $C_{2,\mathrm{valid}}$ 성립 이후에도 모드가 AEB 활성 상태로 유지되고 상태 천이 요청이 제공되지 않는 고장으로 식 (27)과 같이 구현한다.

$$M^{\mathrm{fault}}(t) = M_{\mathrm{AEB}}, \quad M_{\mathrm{tr}}^{\mathrm{fault},AEB\to AES}(t) = 0, \quad t \geq t_{C2} \tag{27}$$

여기서 t_{C2}는 $C_{2,\mathrm{valid}}$가 성립한 시점이다. 두 고장은 $C_{2,\mathrm{valid}}$ 성립 이후 회피 종료 시점까지 유지되는 고착 형태로 정의한다. 따라서 G2와 G3에는 동일한 고장이 주입되며 G3에서의 성능 차이는 고장 제거가 아니라 안전 메커니즘에 의한 감지 및 요청 보정 동작의 결과로 해석한다. $R_{\mathrm{crit}}, B_{\mathrm{inf}}, S_{\mathrm{feas}}$ 자체의 미검출 또는 지연은 본 메커니즘의 완전 보완 대상이 아니므로 핵심 고장 주입에서 제외한다.

천이 응답 시간은 $C_{2,\mathrm{valid}}$ 성립 시점 이후 AES 요청 또는 상태 천이가 최초로 제공되기까지의 시간으로 식 (28)과 같이 정의한다.

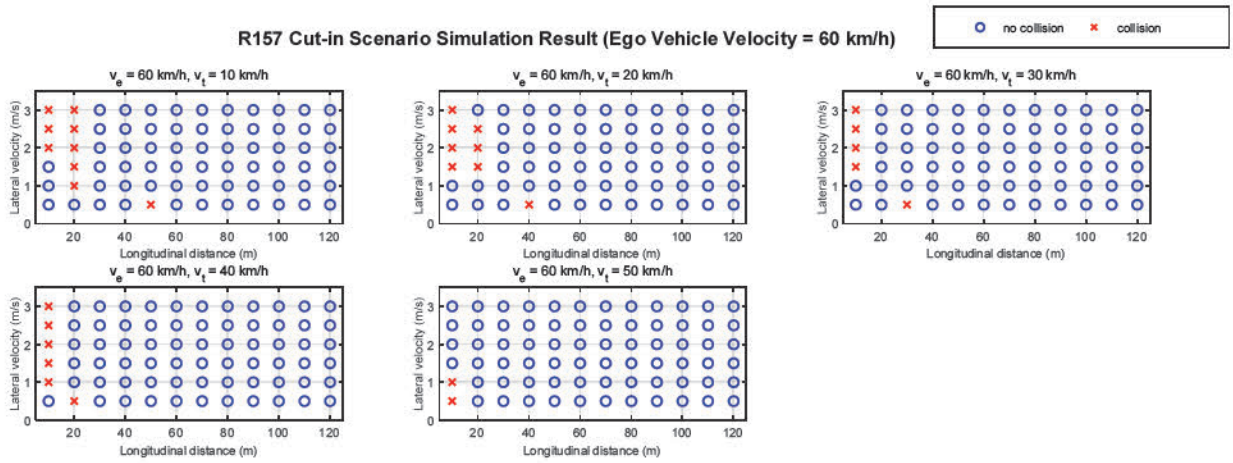
$$\Delta t_{\mathrm{tr}} = \min(t_{AES}, t_{tr}) - t_{C2} \tag{28}$$

t_{AES}는 AES 요청 최초 제공 시점, t_{tr}은 상태 천이 요청 또는 AES 모드 진입 최초 관측 시점이다. 두 시점 중 하나가 회피 종료 시점까지 관측되지 않으면 해당 시점은 $+\infty$로 처리한다. $C_{2,\mathrm{valid}} = 1$이고 $P_{\delta} = 1$인 조건에서 $\Delta t_{\mathrm{tr}} \leq T_{\mathrm{tr,allow}}$이면 $V_{\mathrm{tr}} = 1$로 판정하며 $P_{\delta} = 0$이면 보정 억제 안전 동작을 별도로 판정한다.

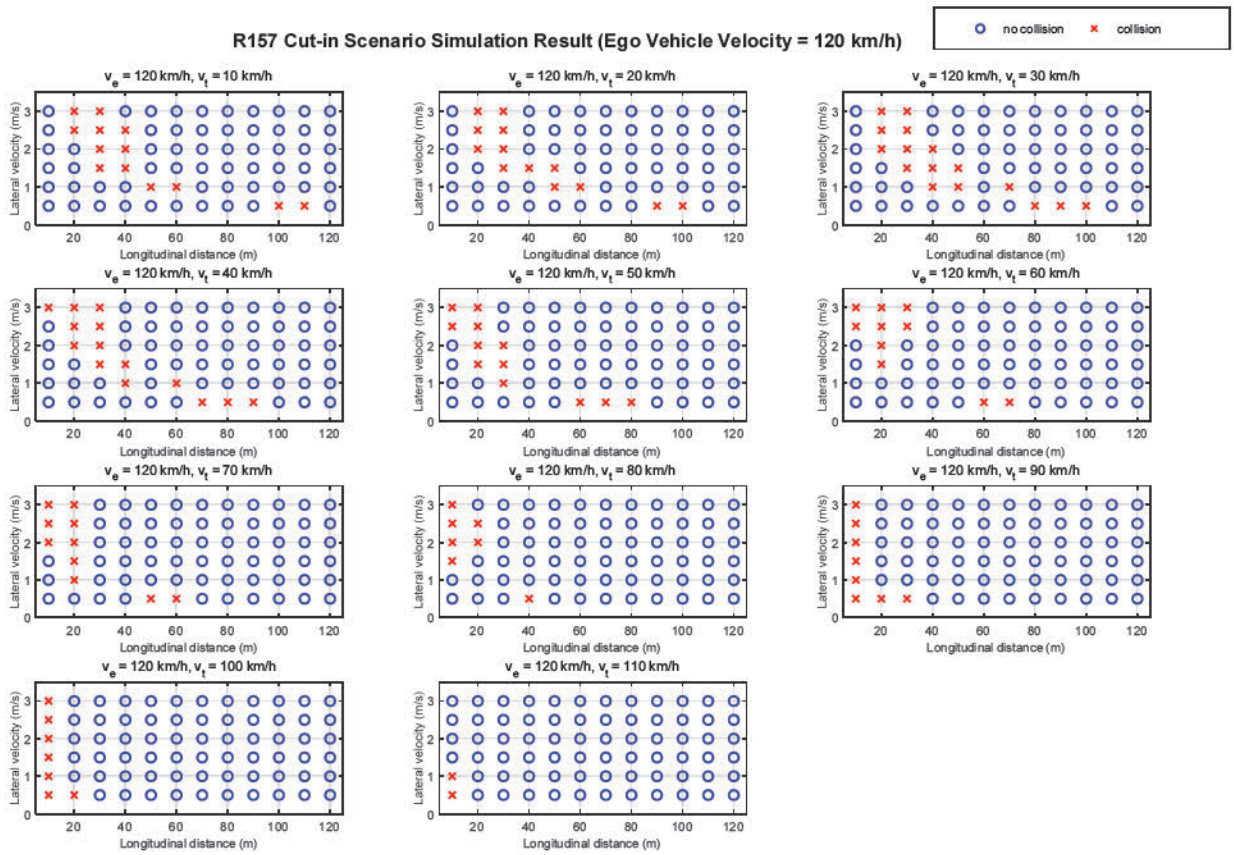
한편 안전 메커니즘의 회복 지연 시간 Δt_{rec}는 모니터링 전조가 활성화되어 천이 위반을 인식한 시점부터 안전 메커니즘이 최종 보정 출력을 제공하기까지의 시간으로 정의하며 식 (29)와 같이 계산한다. 여기서 t_{mon}은 $F_{mon,tr}$이 최초로 성립한 시점이고, t_{corr}은 안전 메커니즘을 거친 최종 AES 요청 또는 상태 천이 요청이 제공된 시점이다. Δt_{rec}는 모니터링, 계산 및 전달 지연을 포함하며, 천이 응답 시간 Δt_{tr}과 구분되는 별도 지표이다.

$$\Delta t_{rec} = t_{\mathrm{corr}} - t_{mon} \tag{29}$$

사고회피 성능 지표는 충돌 발생 여부 I_{col}과 충돌 속도 v_{imp}로 구성하며 식 (30)과 같이 정의한다. 본 검증의 대표 시나리오는 고장 조건에서 AES 천이 실패로 AEB 상태에 머문 채 충돌하거나 안전 메커니즘 적용 후 AES 천이를 통해 조향 회피하는 경우로 구성되므로 종방향 최소 거리는 횡방향 조향 회피가 포함된 조건에서 회피 성능을 일관되게 판정하기 어려우므로 지표에서 제외한다. 여기서 v_{imp}는 충돌이 발생한 경우 충돌 시점 t_{col}에서의 자차 종방향 절대 속도이며 충돌이 발생하지 않은 경우 N/A로 표기한다.



(a)



(b)

Fig. 5 Baseline collision map of the normal sequential AEB/AES under the R157 cut-in parameter sweep: (a) ego speed 60 km/h, (b) ego speed 120 km/h

$$I_{col} = \begin{cases} 1, & \text{collision occurs} \\ 0, & \text{otherwise} \end{cases}, \quad v_{imp} = v_e(t_{col}) \tag{30}$$

최종 안전 상태와 보정 억제 안전 동작은 4.4절의 정의를 적용한다. 다만 본 검증 환경에서는 차로 경계 조건 V_{lane}과 회피 공간 점유 조건 V_{occ}를 산출하지 않으므로 안전 상태 판정은 4장에서 정의한 안전 상태 SS_{design} 전체를 검증하지 않고 제한적 평가 지표 SS_{eval}로 한정한다. 검증에서는 $P_\delta = 1$ 조건에서 충돌이 발생하지 않고 천이 적시성 V_{tr}이 만족되면 SS_{eval}로 판정한다. $P_\delta = 0$ 조건에서 AES 보정을 억제하고 AEB 요청을 유지하는 보정 억제 안전 동작 SA_{inh}은 대표 시나리오 S1-S4의 정량 판정 범위에 포함하지 않고 S5에서 판정한다. 평가지표와 판정 기준은 Table 15와 같다.

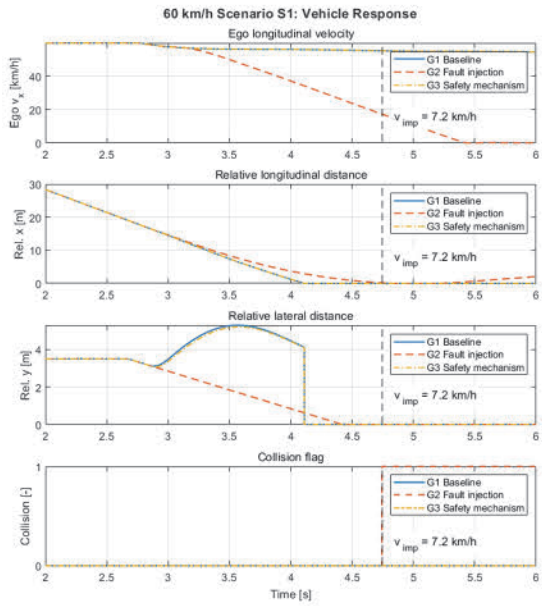
Table 15 Evaluation metrics and judgement criteria

Category	Metric	Judgement criterion
Collision risk	I_{col}, v_{imp}	$I_{col} = 0$ for G3 (SS); v_{imp} quantifies G2 collision severity
Transition timing	Δt_{tr}, V_{tr}	$\Delta t_{tr} \le T_{tr,allow}$ under $C_{2,valid} = 1$ and $P_{delta} = 1$
Recovery response	Δt_{rec}	Final corrected output is generated after monitor activation
Monitor response	F_{tr}, F_{mode}, $F_{mon,tr}$	Target precursor or monitor flag is activated
Safe action	SA_{inh}	Judgement criterion for $P_\delta = 0$; evaluated in S5

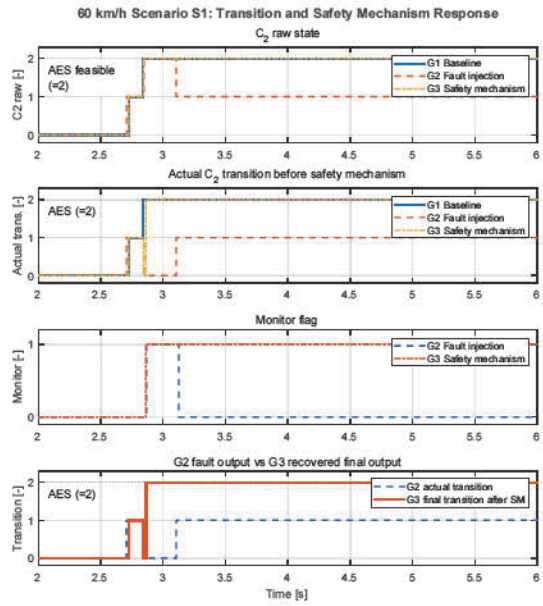
5.4 고장 주입 및 안전 메커니즘 적용 결과

본 절에서는 Table 13의 대표 시나리오에 대해 동일한 천이 고장을 G2와 G3에 주입하고, 안전 메커니즘 적용 전후의 차량 응답과 요청 보정 결과를 비교한다. G2의 F_{tr} 및 F_{mode}는 주입 고장이 4장의 천이 위반 전조 조건을 사후적으로 만족하는지를 확인한 결과이고, G3의 $F_{mon,tr}$는 안전 메커니즘의 요청 보정 또는 보정 억제를 개시하는 모니터링 플래그이다. 정량 평가는 5.3절에서 정의한 지표와 Table 15의 판정 기준을 따른다. S1부터 S4까지 모두 G2에서는 천이 적시성 위반으로 충돌($I_{col} = 1$)에 이르렀으나 G3에서는 $F_{mon,tr}$ 검출 후 최종 요청이 보정되어 충돌이 발생하지 않았다($I_{col} = 0$). 회복 지연 시간 Δt_{rec}은 모두 10 ms로 계측되었으며, 이는 제어 주기 한 스텝 내에 최종 보정 출력이 제공되었음을 의미한다. 네 경우 모두 $P_\delta = 1$이 관측되어 SS_{eval}로 판정되었다. 반면 S5에서는 $O_{\text{avoid}} = 1$로 $P_\delta = 0$이 판정되어 G3에서 AES 요청 보정이 억제되고 AEB 요청이 유지되었다. 이때 G3에서도 충돌은 발생하였으나 충돌 속도가 저감되었으며, 보정 억제 안전 동작 SA_{inh}로 판정되었다.

시나리오의 결과는 Figs. 6~10에 제시하며, 각 그림은 (a) 차량 상태와 (b) 안전 메커니즘 응답으로 구성된다. (a)는 자차 속도, 종방향 상대 거리, 횡방향 상대 거리 및 충돌 플래그를, (b)는 $C_{2,\text{valid}}$, 천이 신호, 감시 플래그 및 최종 보정 출력을 같은 시간축에서 비교하여 고장 주입 시 천이 신호 결손과 안전 메커니즘 적용 시 요청 복구 시점을 보인다. 각 그림에서 G2의 충돌 시점에 표시되는 속도는 충돌 시점의 자차 종방향 절대 속도 v_{imp}이다.

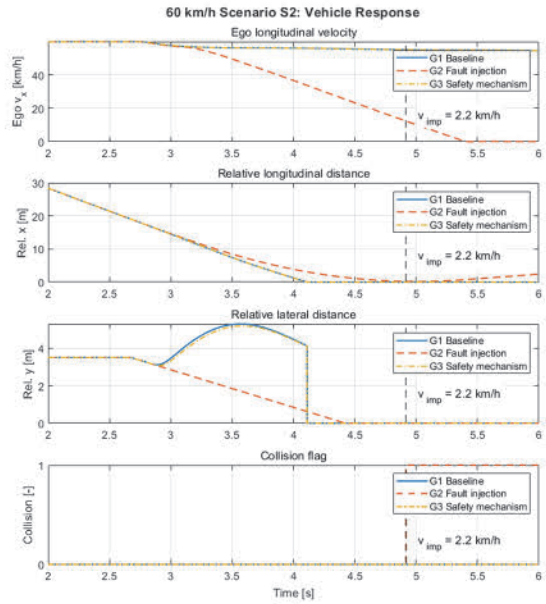


(a)

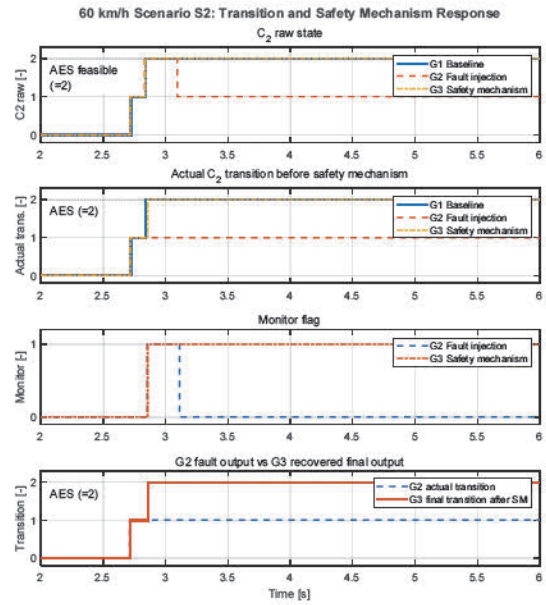


(b)

Fig. 6 Results for S1 (60 km/h, Case 1): (a) vehicle response, (b) transition and safety mechanism response

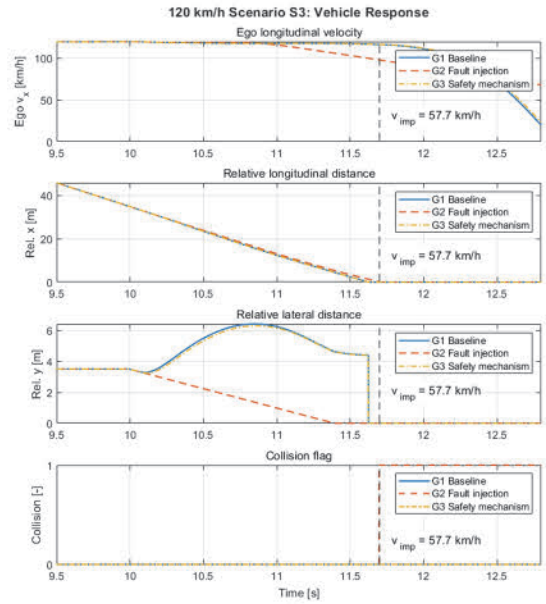


(a)

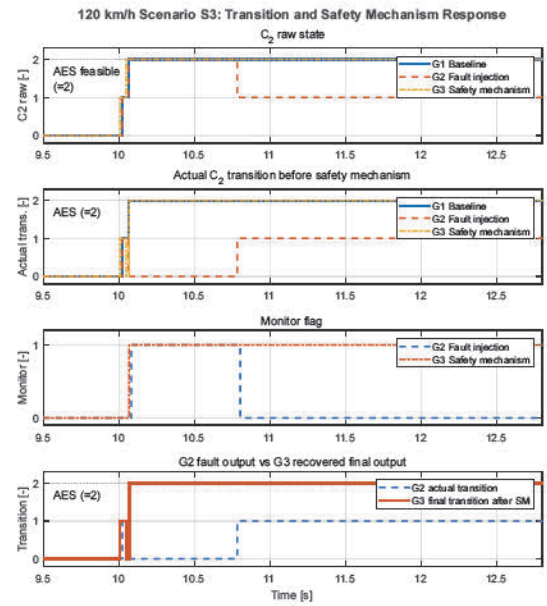


(b)

Fig. 7 Results for S2 (60 km/h, Case 2): (a) vehicle response, (b) transition and safety mechanism response



(a)

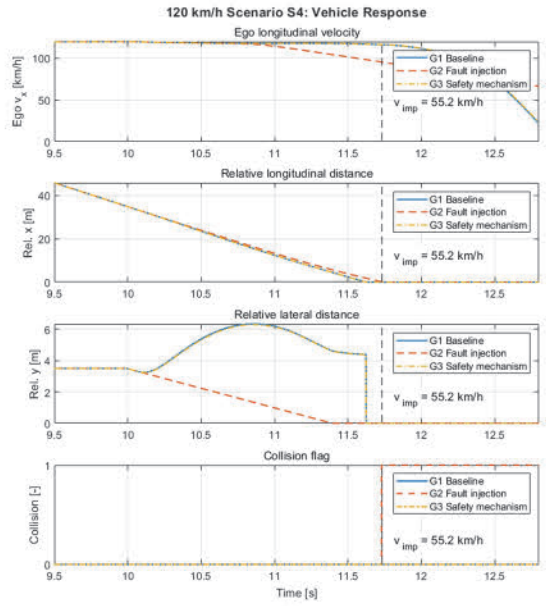


(b)

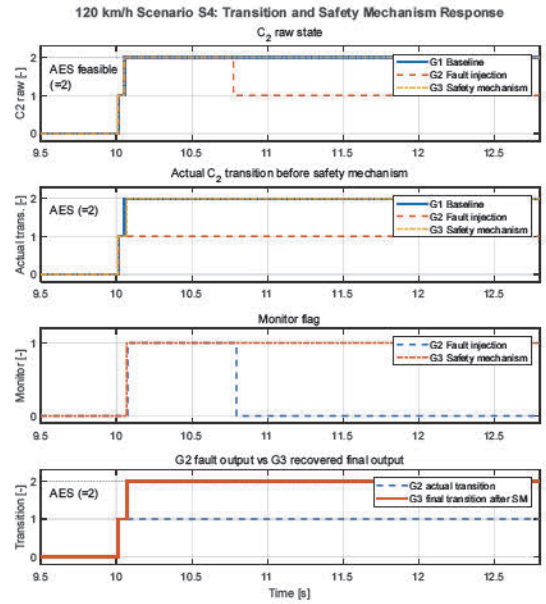
Fig. 8 Results for S3 (120 km/h, Case 1): (a) vehicle response, (b) transition and safety mechanism response

AES enable stuck-off가 주입된 S1과 S3에서 G2는 $C_{2,\mathrm{valid}}$ 성립 이후 AES 요청이 회피 종료 시점까지 제공되지 않아 $F_{tr} = 1$로 판정되었고 천이 응답 시간이 허용 시간을 초과하여 천이 적시성을 위반하였다. AEB mode stuck이 주입된 S2와 S4에서 G2는 $C_{2,\mathrm{valid}}$성립 이후에도 AEB 활성 상태가 유지되어 $F_{mode} = 1$로 판정되었고, AEB-to-AES 천이가 생성되지 않았다. 두 고장 모두 충돌에 이르렀으며 시나리오별 충돌 속도는 Table 16과 같다. 반면 G3에서는 $F_{mon,tr}$ 검출 후 최종 요청이 보정되어 S1부터 S4까지 모두 충돌이 회피되었다.

동일한 천이 고장이라도 자차 속도에 따라 충돌 심각도가 크게 달라졌다. 60 km/h 조건의 S1과 S2는 2.207 km/h 및 7.198 km/h로 제한된 반면, 120 km/h 조건의 S3와 S4는 55.240 km/h 및 57.746 km/h로 증가하였다. 이는 고속 조건에서 잔여 회피 시간이 짧아 천이 적시성 위반이 충돌 심각도를 크게 확대함을 보여준다.

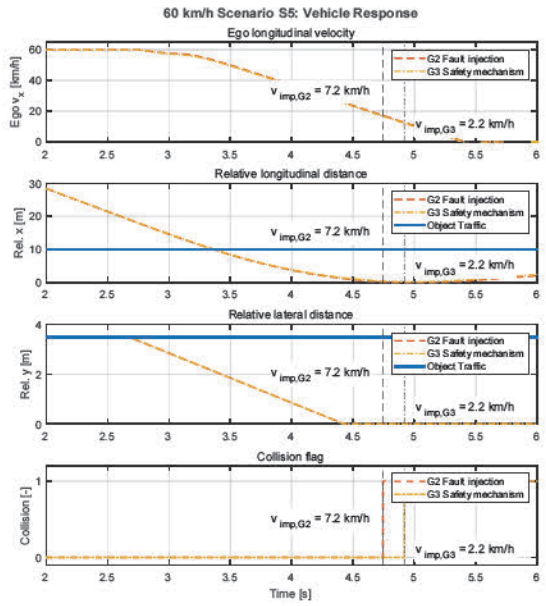


(a)

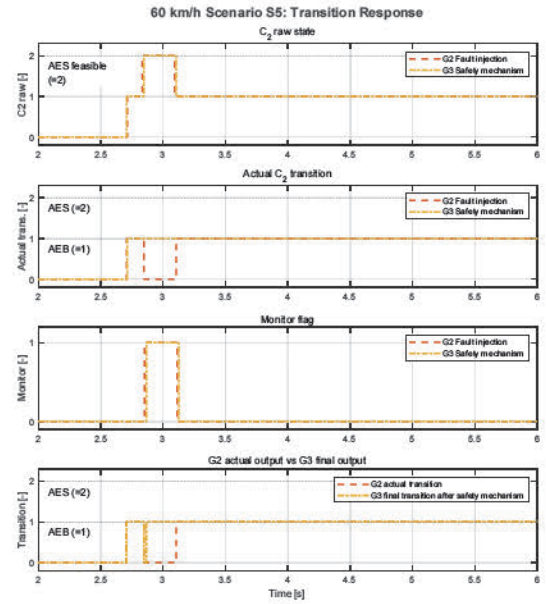


(b)

Fig. 9 Results for S4 (120 km/h, Case 2): (a) vehicle response, (b) transition and safety mechanism response



(a)



(b)

Fig. 10 Results for S5 with an occupied avoidance space at 60 km/h: (a) vehicle response, (b) transition and safety mechanism response

S1부터 S4까지 차량 수준 응답에서 G2는 AES 개입이 적시에 제공되지 않아 충돌에 이른 반면, G3에서는 안전 메커니즘의 요청 보정으로 AES 천이가 회복되어 횡방향 회피가 수행되었다. 안전 메커니즘 응답에서 G2는 기본 천이 출력이 지연 또는 결손되어 F_{tr} 또는 F_{mode}가 활성화된 반면, G3에서는 천이 위반 전조가 검출된 뒤 최종 출력단에서 천이 요청이 보정되었다. 이는 고장이 기본 출력을 차단하더라도 안전 메커니즘이 최종 출력을 보정함을 나타내며, Table 16의 $\Delta t_{rec} = 10$ ms와 대응된다.

S1부터 S4까지는 $P_\delta = 1$이 관측되어 안전 메커니즘의 보정 동작이 허용되었다. 따라서 본 검증의 제한적 평가 지표 SS_{eval}는 천이 적시성 V_{tr}, 보정 허용 조건 $P_\delta = 1$ 및 충돌 미발생 $I_{col} = 0$을 근거로 판정하였으며 식 (31)과 같이 정리된다.

Table 16 Comparison of fault-injected and safety-mechanism results

Scenario	S1	S2	S3	S4	S5
Speed [km/h]	60	60	120	120	60
G2 I_{col}	1	1	1	1	1
G2 t_{col} [s]	4.743	4.917	11.697	11.729	4.743
G2 v_{imp} [km/h]	7.198	2.207	57.746	55.24	7.198
G3 dt_{rec} [ms]	10	10	10	10	10
G3 I_{col}	0	0	0	0	1
G3 v_{imp} [km/h]	0	0	0	0	2.207
G3 recovered	1	1	1	1	1
Judgement	SS_{eval}	SS_{eval}	SS_{eval}	SS_{eval}	SA_{inh}

$$SS_{eval} = V_{tr} \wedge (P_\delta = 1) \wedge (I_{col} = 0) \tag{31}$$

Fig. 10은 S1과 동일한 Cut-in 조건에 인접 차량을 추가한 S5의 결과를 나타낸다. 인접 차량이 위치하여 의도된 회피 공간을 점유함에 따라 $O_{avoid} = 1$ 및 $P_\delta = 0$이 성립하였다. G2에서는 AES enable stuck-off에 의해 AES 요청이 제공되지 않아 7.198 km/h의 충돌 속도로 충돌하였다. G3에서는 $C_{2,valid}$ 성립 이후 천이 위반 전조가 검출되어 $F_{mon,tr}$이 활성화되었으나, 조향 제어 개입 타당성 가드가 $P_\delta = 0$으로 판정됨에 따라 안전 메커니즘은 AES 요청 및 AEB-to-AES 천이 요청의 보정을 억제하고 AEB 요청을 유지하였다. 따라서 S5의 판정 기준은 충돌 미발생이 아니라, 회피 공간이 점유된 조건에서 부적절한 AES 천이를 강제하지 않고 AES 보정을 억제하며 AEB 요청을 유지하는지 여부이며, 이를 근거로 보정 억제 안전 동작 SA_{inh}이 성립하는 것으로 판정하였다. 차량 수준 결과에서 G3는 AEB 제동을 유지한 상태로 충돌하였으나 충돌 속도는 2.207 km/h로 G2 대비 저감되었으며, 이는 SA_{inh} 동작에 수반되는 부가적 결과이다.

6. 결 론

본 연구는 순차형 AEB/AES 사고회피 기능을 대상으로 STPA-HARA 기반 기능안전 분석을 수행하고 상태 천이 고장을 핵심 안전 문제로 정의하였다. STPA 분석 결과, 서로 다른 인과 경로가 $C_{2,valid}$ 조건에서 AES 요청 또는 상태 천이 요청의 누락 및 지연이라는 동일한 비안전 제어동작으로 수렴함을 확인하였다. 이 고장 집합을 극한 조건 고장 집합으로 정의하고 HARA의 위험 사건, ASIL 평가 및 안전목표와 연계하여 안전 분석과 설계 사이의 추적성을 확보하였다.

제안한 안전 메커니즘은 기본 순차형 AEB/AES 판단 로직을 대체하는 통합 제어기가 아니라 기본 출력 이후에 배치되어 천이 위반 전조를 감시하고 조건부로 최종 요청을 보정하는 후단 안전 게이트로 정의하였다. 안전 메커니즘은 $C_{2,valid}$ 성립 이후 천이 적시성 위반 전조와 보정 허용 조건 P_δ를 감시하며 $P_\delta = 1$인 경우 AES 요청 또는 상태 천이 요청을 최종 출력단에서 보정하고 $P_\delta = 0$인 경우 AES 보정을 억제하고 AEB 요청을 유지하도록 설계하였다. 따라서 제안한 구조는 고장 원인을 직접 제거하는 방식이 아니라 안전목표 위반으로 이어질 수 있는 천이 결손을 감시하여 최종 출력단에서 제한적으로 보정하는 안전 계층으로 해석된다.

UN R157 cut-in 기반 고장 주입 검증에서는 AES 활성화 신호 비활성 고착과 AEB 활성 모드 고착을 대표 고장으로 적용하고, 정상 조건(G1), 고장 주입 조건(G2) 및 안전 메커니즘 적용 조건(G3)을 비교하였다. 안전 메커니즘이 없는 G2에서는 대표 시나리오 모두 충돌하였으며, 고속 조건일수록 충돌 심각도가 확대되었다. 동일한 고장이 유지된 G3에서는 $P_\delta = 1$인 시나리오의 경우 상태 천이 위반 전조가 검출된 후 최종 요청이 보정되어 충돌이 발생하지 않았고, $P_\delta = 0$인 시나리오에서는 AES 보정이 억제되고 AEB 요청이 유지되는 보정 억제 안전 동작이 수행되었다. 이는 제안한 안전 메커니즘이 기본 사고회피 로직을 재설계하지 않고도 상태 천이 고장에 따른 안전목표 위반을 완화하거나 부적절한 조향 개입을 방지함을 보여준다.

본 연구의 검증은 직선 도로의 Cut-in 조건, 두 대표 천이 고장 및 단일 회피 공간 점유 조건에 한정된다. S5를 통해 AES 보정이 억제되고 AEB 요청이 유지되는 기능 동작을 확인하였으나, 인접 차량의 위치와 속도 변화에 따른 보정 억제 경계 및 회피 공간 점유 판단 알고리즘의 검출 성능은 독립적으로 평가하지 않았다. 또한 안전 메커니즘이 기본 기능과 판단 신호를 공유하므로 공통 원인 고장에 대한 독립적 대응을 보장하지 않는다. 향후에는 독립 채널 구조로 확장하여 공통 원인 고장에 대한 견고성을 검증하고, 다양한 인접 차량 위치와 다중 객체 조건으로 시나리오를 확장하며, 곡선 도로, HILS 및 실차 환경에서 보정 억제 동작과 실시간성 및 SOTIF 관점의 성능 한계를 함께 평가할 필요가 있다.

후 기

본 연구는 산업통상자원부 SDV용AI가속기반도체 기술개발사업의 연구비 지원(과제번호: RS-2025-25456979, AI가속기 및 AP 구동을 위한 SW 개발)의 지원으로 수행된 연구임.

References

1) World Health Organization, Global Status Report on Road Safety 2023, World Health Organization, Geneva, 2023.
2) W. Yang, J. Liu, K. Zhou, Z. Zhang and X. Qu, "An Automatic Emergency Braking Model Considering Driver's Intention Recognition of the Front Vehicle," Journal of Advanced Transportation, Vol.2020, Paper No.5172305, 2020.
3) A. Eidehall, J. Pohl, F. Gustafsson and J. Ekmark, "Toward Autonomous Collision Avoidance by Steering," IEEE Transactions on Intelligent Transportation Systems, Vol.8, No.1, pp.84-94, 2007.
4) J. Park, D. Kim and K. Huh, "Emergency Collision Avoidance by Steering in Critical Situations," International Journal of Automotive Technology, Vol.22, No.1, pp.173-184, 2021.
5) C. Ackermann, R. Isermann, S. Min and C. Kim, "Collision Avoidance with Automatic Braking and Swerving," Proceedings of the 19th IFAC World Congress, Vol.47, No.3, pp.10694-10699, 2014.
6) X. Tan, G. Wu, Z. Li, K. Liu and C. Zhang, "Autonomous Emergency Collision Avoidance and Collaborative Stability Control Technologies for Intelligent Vehicles: A Survey," IEEE Transactions on Intelligent Vehicles, Vol.10, No.12, pp.5229-5248, 2025.
7) M. M. Minderhoud and P. H. Bovy, "Extended Time-to-Collision Measures for Road Traffic Safety Assessment," Accident Analysis & Prevention, Vol.33, No.1, pp.89-97, 2001.
8) K. Vogel, "A Comparison of Headway and Time to Collision as Safety Indicators," Accident Analysis & Prevention, Vol.35, No.3, pp.427-433, 2003.
9) S. G. Shin, H. K. Lee and S. H. You, "Decision Making for Collision Avoidance Systems Considering a Following Vehicle," International Journal of Automotive Technology, Vol.24, No.2, pp.421-434, 2023.
10) M. Brannstrom, E. Coelingh and J. Sjoberg, "Decision-Making on When to Brake and When to Steer to Avoid a Collision," International Journal of Vehicle Safety, Vol.7, No.1, pp.87-106, 2014.
11) R. Hayashi, P. Chatporntanadul and M. Nagai, "Improvement of Trajectory Tracking Performance in Autonomous Collision Avoidance by Steering," Proceedings of the 7th IFAC Symposium on Advances in Automotive Control, Vol.46, No.21, pp.410-415, 2013.
12) Q. Cui, R. Ding, X. Wu and B. Zhou, "A New Strategy for Rear-End Collision Avoidance via Autonomous Steering and Differential Braking in Highway Driving," Vehicle System Dynamics, Vol.58, No.6, pp.955-986, 2020.
13) H. Li, T. Zheng, F. Xia, L. Gao, Q. Ye and Z. Guo, "Emergency Collision Avoidance Strategy for Autonomous Vehicles Based on Steering and Differential Braking," Scientific Reports, Vol.12, Paper No.22647, 2022.
14) D. Kim, S. Kim, S. Lee and C. Ahn, "Performance Analysis and Controller Design of Evasive Steering System," Transactions of KSAE, Vol.28, No.3, pp.219-225, 2020.
15) United Nations Economic Commission for Europe, UN Regulation No.157 - Uniform Provisions Concerning the Approval of Vehicles with Regard to Automated Lane Keeping Systems, UNECE, Geneva, 2021.
16) P. Falcone, F. Borrelli, J. Asgari, H. E. Tseng and D. Hrovat, "A Model Predictive Control Approach for Combined Braking and Steering in Autonomous Vehicles," Proceedings of the 15th Mediterranean Conference on Control and Automation, pp.1-6, 2007.
17) J. Ji, A. Khajepour, W. W. Melek and Y. Huang, "Path Planning and Tracking for Vehicle Collision Avoidance Based on Model Predictive Control with Multi-Constraints," IEEE Transactions on Vehicular Technology, Vol.66, No.2, pp.952-964, 2017.
18) Y. Baek and H. Lee, "Integrated Collision Avoidance Framework for Autonomous Vehicles Using Sparse Gaussian Process Regression and Stochastic Model Predictive Control," International Journal of Automotive Technology, pp.1-14, 2026.
19) N. G. Leveson and J. P. Thomas, STPA Handbook, Massachusetts Institute of Technology, Cambridge, 2018.
20) International Organization for Standardization, ISO 26262-3: Road Vehicles - Functional Safety - Part 3: Concept Phase, ISO, Geneva, 2018.
21) S. Han, J. Byeon, S. Ahn and J. Yoo, "Derivation of STPA Safety Analysis and V&V Methodology for Ensuring SOTIF in Autonomous Driving System," Transactions of KSAE, Vol.33, No.1, pp.61-80, 2025.