전장부품 결함 및 오류에 대한 자율주행 자동차 DDT Fallback 평가 프레임워크에 관한 연구

하성민, 양현덕, 황영서, 이명수, 윤윤기, 윤경수
지능형자동차부품진흥원
ha4100@kiapi.or.kr, yhd0427@kiapi.or.kr, dudtj7476@kiapi.or.kr,
trust@kiapi.or.kr, ykyoon@kiapi.or.kr, kadbonow@kiapi.or.kr

A Study on an Evaluation Framework for DDT Fallback of Automated Driving Vehicle under E/E Components Faults and Errors

Seongmin Ha, Hyeondeok Yang, Youngseo Hwang, Myungsu Lee, Yunki Yoon, Kyungsu Yun
Korea Intelligent Automotive Parts Promotion Institute

요 약

본 논문은 자율주행 자동차의 전장부품 결함 및 오류 발생 시 자율주행 자동차의 DDT Fallback 기능을 체계적으로 평가하기 위한 프레임워크를 제안한다. Level 4 이상의 자율주행 시스템은 운전자 개입 없이 DDT 수행 및 Fallback 책임을 지며, 고장 상황에서의 안전 전이(Minimal Risk Condition 달성) 여부가 시스템 신뢰성 평가의 핵심이 된다. 제안한 프레임워크는 대상 차량의 명세 정의, 시스템 구성 요소 분류, DDT Fallback 기능 명세화, 결함·오류 유형 정의 및 주입 방법 설계, 기대 동작 정의, Test-Case 및 시나리오 도출, 정량적 평가 지표 설정, 결함 주입 시험 수행 및 합격 판정까지 총 11단계의 평가 프로세스를 제안하였다. 제안한 프로세스는 MIL, SIL, HIL, VIL 및 실차 시험 환경에 모두 적용 가능하며, 시나리오 기반 결함 주입 시험을 통해 DDT Fallback 전략의 적절성을 정량적으로 평가할 수 있다. 이를 통해 자율주행 시스템의 고장 대응 설계 검증과 안전성 향상에 기여할 수 있다.

Ⅰ. 서 론

SAE J3016에 따르면, Driving Dynamic Task (DDT)는 주행 중 차량을 제어하기 위해 수행해야 하는 모든 조작과 판단을 포함하며, 횡/종방향 차량 모션 제어와 Object and Event Detection and Response(OEDR)로 구분된다. DDT Fallback은 자율주행 시스템 고장 발생이나 Operation Design Domain(ODD) 이탈과 같이 시스템 또는 운전자가 DDT를 더 이상 수행할 수 없을 때, 차량을 안전한 상태로 이동하기 위한 조치 및 전략을 의미한다. SAE Level 3 이하에서는 인간 운전자가 fallback 책임을 지지만, Level 4 이상의 자동화 단계에서는 ADS(Automated Driving System)가 직접 fallback을 수행해야 한다. 따라서 DDT Fallback은 최소위험상태(MRC, Minimal Risk Condition) 달성을 위한 핵심 과정으로, ADS의 안전성 평가와 검증에서 필수적으로 고려된다[1].

ADS의 안전성을 확보하기 위한 국제 표준 역시 이러한 필요성을 반영한다. ISO 26262는 전기·전자(E/E) 시스템의 기능 안전을 다루며, 결함 발생 시 시스템이 안전 상태로 전이되도록 설계할 것을 요구한다[2]. 하지만 ISO 26262는 결함이 없는 상황에서 발생하는 위험을 다루지 못한다는 한계를 갖고 있으며, 이를 보완하기 위해 ISO 21448(SOTIF)이 제정되었다. SOTIF는 센서 한계, 인지 오인식, 의도된 기능의 불충분으로 발생할 수 있는 위험을 식별하고 완화하는 과정을 강조한다[3]. 최근 제정된 ISO 34501은 ADS 시험 시나리오에 대한 공통 용어 체계를 제공하여, 시나리오 기반 평가의 국제적 표준화를 지원하고 있다[4]. 또한 UL 4600은 ADS 안전성 평가를 위한 Safety Case 접근법을 제안하여, 기능안전·SOTIF·사이버보안·실시간 모니터링 등 모든 안전 근거를 통합적으로 제시할 것을 요구한다[5].

학계에서도 ADS 검증의 효율성을 높이기 위해 시뮬레이션 기반 critical scenario 생성과 적응형 시나리오 테스트 연구가 활발히 진행되고 있다[6]. 강화학습이나 게임이론 기반 기법을 활용해 ADS가 실패할 가능성이 높은 시나리오를 자동으로 탐색하는 연구들이 제안되고 있으며[6], 온라인 검증(runtime verification)을 통해 차량이 생성한 주행 궤적이 실시간으로 안전 규칙을 만족하는지 검사한 뒤 실행하는 방법도 제시되고 있다[7]. 이러한 연구들은 ADS의 안전성을 사전에 입증할 뿐만 아니라, 결함 주입(fault injection)을 통해 DDT Fallback 동작이 의도한 대로 수행되는지를 평가할 수 있는 기반을 제공한다.

그러나 현재까지의 연구와 표준은 DDT Fallback 자체의 체계적 평가 프로세스보다는 개별 시스템 기능 또는 시나리오 검증에 초점이 맞추어져 있다. 특히 E/E 부품 결함 및 오류가 실제 운행 중 발생했을 때 ADS가 수행하는 fallback 동작의 적절성, 안정성, 최소위험상태 도달 여부를 정량적으로 평가할 수 있는 통합 프레임워크는 아직 미비하다. 이에 본 연구는 전장부품(E/E Component) 결함 및 오류 상황에서의 자율주행 차량 DDT Fallback 동작을 체계적으로 평가할 수 있는 평가 프레임워크를 제안한다.

Ⅱ. 본론

본 논문에서는 자율주행 자동차의 전장부품에 결함 및 오류가 발생하였을 때 자율주행 시스템의 DDT Fallback 기능에 대한 평가를 위한 평가 프로세스를 제안한다. 그림 1은 제안하는 프레임워크의 전체 구조를 나타내며 총 11단계로 구성된다. 대상 자율주행 차량 식별 및 명세 단계에서는 검증 대상 차량의 SAE 자동화 수준, ODD, ADS 소프트웨어 버전, 센서·ECU 구성, 통신 네트워크, 차량 동역학 및 제원 정보를 식별하고 문서화한다. 자율주행 차량 구성 요소 파악 및 분류 단계에서는 인지·판단·제어 등 서브 시스템과 하위 모듈의 입출력 신호, 주기, 정상 범위를 명세화

하여 결함 주입 영향 지점을 명확히 한다. DDT Fallback 기능 확인 및 명세화 단계에서는 센서 대체 인지, 제어기 전환, 감속·안전정지 등 고장 대응 및 DDT Fallback 기능을 기능 ID, 수행 조건, 모니터링 신호 기준으로 정리한다. 전장부품별 결함 및 오류 유형 명세화 단계에서는 FMEA/FTA 자료를 기반으로 라이다 신호 단절·드리프트, CAN 지연·손실, ECU 리셋 등 주요 결함 유형을 선정하고 심각도(S), 발생도(O), 검출

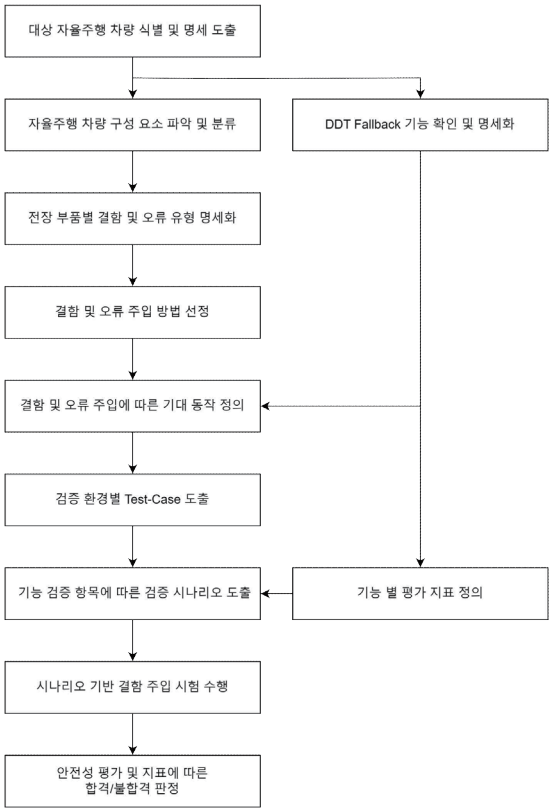

그림 1. 전장부품 결함 및 오류에 대한 자율주행 차량 DDT Fallback 기능 평가를 위한 평가 프로세스

도(D) 값과 탐지 방법을 기록한다. 결함 및 오류 주입 방법 선정 단계에서는 MIL/SIL 환경의 변수·모델 파라미터 변조, HIL/VIL/실차 환경의 CAN 인젝션·회로 차단·센서 시뮬레이터 등 환경별 주입 방법을 선택하고 주입 시점·지속·반복 횟수를 설정한다. 결함 및 오류 주입에 따른 기대 동작 정의 단계에서는 결함 발생 시 차량이 수행해야 하는 DDT Fallback 거동과 시스템·차량 단위의 기대 응답을 정의한다. 검증 환경별 Test-Case 도출 단계에서는 입력 조건, 주입 조건, 기대 출력을 포함한 테스트케이스를 설계하고 환경별로 구현 가능성을 검토한다. 기능별 평가 지표 정의 단계에서는 속도·가속도 RMS, 궤적 편차, 제동 응답 시간, 경고 발생 시간, 운전자 개입 시간 등 정량 지표와 합격 기준을 수학식으로 정의한다. 기능 검증 항목에 따른 검증 시나리오 도출 단계에서는 고장 대응 기능과 인지·판단·제어 안전성 항목을 고려해 시나리오를 구성한다. 시나리오 기반 결함 주입 시험 수행 단계에서는 설계된 시나리오를 기반으로 결함 주입 시험을 수행하고 차량 상태, 제어 명령, 경고 신호, 운전자 개입 여부를 로깅한다. 마지막으로 안전성 평가 및 합격/불합격 판정 단계에서는 수집된 데이터를 기반으로 평가 지표를 계산하여 Pass/Fail을 판정하고, 불합격 사례는 재시험 및 알고리즘 개선에 활용하며, 합격 사례도 거동 분석을 통해 추가 안전성 향상을 위한 개선 포인트를 도출한다.

Ⅲ. 결론

본 논문에서는 전장부품 결함 및 오류 상황에서 자율주행 자동차의 DDT Fallback 기능을 평가하기 위한 체계적 평가 프레임워크를 제안하였다. 제안한 프레임워크는 차량 명세 정의, 시스템 구성요소 분석, 결함 유형 및 주입 방법 설정, 기대 동작 정의, 시나리오 및 테스트케이스 도출, 정량적 평가 지표 정의, 시험 수행 및 합격 판정으로 이어지는 11단계 절차를 포함한다. 이를 통해 실제 주행 중 발생 가능한 결함과 오류를 시뮬레이션·HIL·실차 환경에서 재현하고, ADS의 Fallback 거동이 최소위험 상태 달성 요구사항을 만족하는지 정량적으로 검증할 수 있다. 본 프레임워크는 향후 ADS 개발 과정에서 결함 주입 기반의 안전성 검증을 표준화하고, ISO 26262, ISO 21448(SOTIF), ISO 34501, UL 4600 등 국제 표준에 부합하는 안전성 확보 프로세스를 구축하는 데 활용될 수 있다. 향후 연구에서는 실제 자율주행 차량을 대상으로 제안한 평가 프로세스를 활용하여 검증 시나리오를 도출하고 MIL, HIL 시뮬레이션과 실차 환경에서 시험을 진행할 예정이다.

ACKNOWLEDGMENT

이 연구는 2024년도 산업통상자원부 및 한국산업기술기획평가원(KEIT) 연구비 지원에 의한 연구임(RS-2024-00406153, 기능 재구성 및 자가복구된 전장부품을 활용한 안전 확보 제어 기술 개발)

참 고 문 헌

[1] SAE International. “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016),” SAE International Standard, April 2021.

[2] International Organization for Standardization. “ISO 26262 - Road Vehicles - Functional Safety,” ISO Standard, December 2018.

[3] International Organization for Standardization. “ISO 21448 - Road Vehicles - Safety of the Intended Functionality (SOTIF),” ISO Standard, June 2022.

[4] International Organization for Standardization. “ISO 34501 - Road Vehicles - Test Scenarios for Automated Driving Systems - Vocabulary,” ISO Standard, October 2022.

[5] Li, S., Zhang, Y., Phil, B., Simon, E., and Ji, Y. “Remote driving as the Failsafe: Qualitative investigation of Users’ perceptions and requirements towards the 5G-enabled Level 4 automated vehicles,” Transportation Research Part F, Vol. 100, 2024, pp. 211 - 230.

[6] Zheng, X., Liang, H., Wang, J., and Wang, H. “Game-Theoretic Adversarial Interaction-Based Critical Scenario Generation for Autonomous Vehicles,” Machines, Vol. 12, No. 8, Article 538, 2024.

[7] Pek, C., Koschi, M., and Althoff, M. “An Online Verification Framework for Motion Planning of Self-Driving Vehicles with Safety Guarantees,” AAET-Automatisiertes und vernetztes Fahren, 2019.