Journal of KIIT. Vol. 23, No. 6, pp. 159-168, Jun. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.6.159

기능 안전 강화를 위한 ISO 26262 활용에 관한 연구

김정식*, 추병균**, 곽윤식***

A Study on the Use of ISO 26262 to Enhance Functional Safety

Jungsik Kim*, Byounggyun Chu**, and Yoonsik Kwak***

2025년 국립한국교통대학교 지원을 받아 수행하였음

요 약

본 논문은 기능 안전 강화를 목적으로 다양한 국제 표준 간의 비교 분석을 통하여 효과적인 접근방법의 제안에 관한 것이다. 국제 표준 ISO 26262는 자동차 기능 안전에 초점을 두며, IEC 61508은 더 광범위한 범위를 포괄하는 여러 산업의 전기 및 전자 시스템에 대한 기능 안전을 규정하고 있다. 또한 ISO 21448은 결함이나 오작동과 관계없이 의도한 기능을 수행하지 못하는 것과 관련된 위험을 규정하고 있으며 개발 단계에서 고려사항을 강조하고 있다. 이 같은 다양한 표준의 특성 분석을 통하여 기능 안전 관행을 강화하기 위한 FMEA 목적과 유형의 조사 및 기존의 FTA 수행 방식과 개선된 FTA를 비교 분석하여 개선된 FTA에서는 효과적인 위험 요소 분석이 가능하도록 분석하였다. 또한, 기능 안전을 위한 시험 방법으로 신뢰성 시험 방법과 다양한 시험 방법의 절차를 제안하고, 시험자의 경험에 따른 각 시험 방법의 장단점을 분석하였다.

Abstract

This paper proposes an effective approach through comparative analysis of various international standards for the purpose of reinforcing functional safety. The international standard ISO 26262 focuses on automotive functional safety, while IEC 61508 specifies functional safety for electrical and electronic systems in various industries covering a wider range. In addition, ISO 21448 specifies risks related to failure to perform intended functions regardless of defects or malfunctions, and emphasizes considerations during the development phase. Through the analysis of the characteristics of these various standards, the purpose and types of FMEA were investigated to strengthen functional safety practices, and the existing FTA implementation method and the improved FTA were compared and analyzed to enable effective risk factor analysis in the improved FTA. In addition, reliability test methods and procedures of various test methods were proposed as test methods for functional safety, and the advantages and disadvantages of each test method according to the tester's experience were analyzed.

Keywords

ISO 26262, IEC 61508, FMEA, FTA, reliability test

* 한국교통대학교 산업경영공학과 교수
- ORCID: https://orcid.org/0000-0001-8031-6934
** 한국교통대학교 컴퓨터공학과 강사
- ORCID: https://orcid.org/0009-0000-7031-4855
*** 한국교통대학교 컴퓨터공학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0002-7407-207X

· Received: Dec. 26, 2024, Revised: Feb. 27, 2025, Accepted: Mar. 02, 2025
· Corresponding Author: Yoonsik Kwak
Korea National University of Transportation
Tel.: +82-43-841-5345, Email: yskwak@ut.ac.kr

Ⅰ. 서 론

최근 자동차, 철도, 항공, 의료, 원자력 등 모든 산업군에서 전기 전자 제어시스템의 사용이 증가하고 있다. 특히 자동차산업은 ADAS(Advanced Driver Assistance Systems)와 같은 고급 기능에 대한 요구사항 증가와 고객의 첨단 기능 요구에 따라 기존의 기계 중심에서 전기 전자 제어시스템 중심으로 급변하고 있으며, 이러한 비율은 지속적으로 확대되고 있다[1].

자동차산업은 자동차 패러다임의 변화, 환경 및 소음 등의 제약, 전기 전자 제품의 증가, 신뢰성 요구 강화 등의 요인으로 인해 급격히 변화하고 있다. 또한 완성차 간의 협력 도모(아이템 교환, 지속적인 부품 사용) 등으로 자동차산업의 패러다임이 바뀌고 있다.

자동차 내장형 시스템의 복잡도와 시스템의 기능성이 증가함에 따라 시스템적 결함 및 하드웨어 결함으로 인한 위험성이 높아지고 있다. 이는 기존 부품 수준의 신뢰성만으로는 자동차의 안전성을 보장할 수 없음을 의미한다. 안전성과 품질 확보를 위해서는 안전 임무를 수행하는 전자 장치를 중심으로 강화된 규정 및 지침이 요구된다.

2011년 BMW, Daimler, Volkswagen과 같은 자동차 OEM(Original Equipment Manufacturer) 업체들과 Robert Bosch GmbH, Continental 등의 대표적인 자동차 부품 협력사들이 참여하여 ISO 26262 자동차 기능 안전성 표준을 제정하고 채택하였다. ISO 26262 표준은 기능 안전(Functional safety) 표준으로, 관련 표준들은 다음과 같다.

ISO 26262와 직접적인 연관이 있는 변화로는 개발 기간 단축에 따른 신규 차량의 출시 증가, 전기·전자 제품의 사용 증가, 신뢰성 요구 강화로 인해 점점 복잡해지는 전기·전자 제품에 대한 검증 및 타당성 확인(V & V, Verification and Validation)의 필요성이 대두되었다. 현재의 시험·검사 기술로는 안전성을 확인하는 데 어려움이 있어 더욱 효과적인 V & V를 실시하여 안전한 제품이 자동차에 장착될 수 있도록 기준을 제정한 것이 ISO 26262 표준이다.

부품 간의 상호 작용으로 인해 전기·전자 시스템의 안전성이 중요해짐에 따라 기존의 검사 방법으로는 점점 복잡해지는 전기·전자 시스템의 안전성을 보장하기 어려워 전기·전자 시스템에 대한 기능 안전 표준인 ISO 26262가 요구되었다.

본 연구의 목적은 ISO(International Organization for Standardization) 26262와 기능 안전 관리를 위한 FMEA(Failure Mode and Effect Analysis), FTA(Fault Tree Analysis) 및 신뢰성 시험 방법에 대한 분석을 통하여 효과적인 기능 안전 확보 방안을 제안한다.

1.1 연구의 필요성 및 구성

본 논문은 기능 안전에 관한 표준화 배경을 바탕으로 ISO 26262의 주요 요구사항과 신뢰성 기법 활용을 조사, 분석하는 것으로 구성된다.

M.-S. Baek[2]은 ASIL(Automotive Safety Integrity Level)을 기반으로 FMEA의 RNP(Risk Priority Number)를 보완할 수 있는 평가 척도인 위험 우선순위를 강조하고 있다. 기업은 안전 무결성 기준(SIL, Safety Integrity Level)을 IEC 61508을 기본 규격으로 적용하고 있다. ISO 26262 기능 안전 표준은 개념부터 운용 및 폐기 단계까지의 요구사항 분석, 설계, 테스트 등의 공학 기법과 시스템의 오동작 등 안전 분석 기법을 제시하고 있다. 안전 분석 기법으로는 FMEA, FTA 등이 있다. 본 논문에서는 안전 분석 기법에서 사용되는 FMEA, FTA, B to B (Back-to-Back Test), 인터페이스 시험, 시스템 레벨 시험 등 다양한 시험 방법을 조사, 분석하였다.

기능 안전 관리의 조사, 분석은 사고가 발생하지 않도록 시스템의 실패를 발생시킨 구성 요소를 대체 및 예방 방안에 대해 조사, 분석하는 과정이다. 도성룡[3], [4]은 ISO 26262 기능 안전 표준의 공학 기법과 안전 분석 기법을 제시하고 있다. 양동현외 2[5]는 절차적 개념을 이용한 더 효과적인 FTA 안전 분석 방법을 강조하였다. 두 논문을 통해 FTA 기법의 목적과 유형에 대하여 조사, 분석하고, 효과적인 FTA 안전 분석 방법을 제안하였다.

J. Choi et al.[6]는 차량용 소프트웨어 FMEA에 적합한 기준을 제공하고 있다.

이 논문은 FMEA 적용 시 소프트웨어와 하드웨어의 차이점을 구조적으로 비교하였다. 또한 ISO 26262 기본 실무 가이드에서는 B to B, 시험 대상의 인터페이스 시험, 시스템 레벨 시험 등 다양한 시험 방법을 제시하고 있다[7].

그림 1은 기능 안전 규격 조사, 분석 체계를 나타낸다.

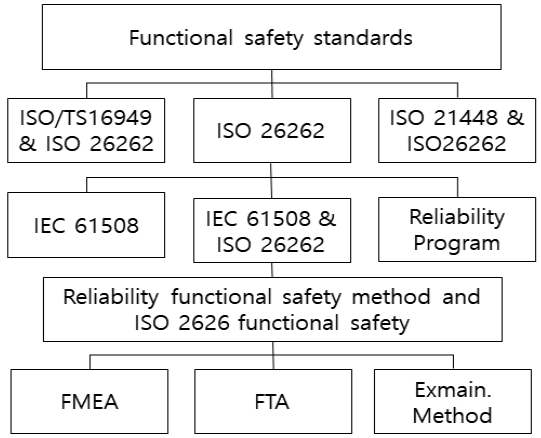


그림 1. 기능 안전 표준 체계
Fig. 1. Functional safety standards system

II. ISO 기능 안전에 관한 배경

2.1 ISO 26262 주요 요구사항

ISO 26262는 현재 국제적으로 사용되고 있는 자동차 기능 안전성 국제 표준이다. 국내·외의 자동차 기업들이 자동차의 기능 안전성을 증명할 때 ISO 26262 기준을 적용하고 있다.

기술적 안전 요구사항 명세서는 기능 개념과 초기 구조적 가정을 모두 고려하여 기능 안전 개념을 상세하게 표현하고 분석하여 기능 안전 요구사항에 부합하는지 검증하는 것을 목적으로 한다. 전제조건은 기능상의 안전 구상과 계획 확인이며, 이 요구사항의 작업 결과로 기술 안전 요구사항의 구체화, 시스템 검증 보고, 계획 확인 등이 있다.

시스템 설계는 기능의 요구사항과 기술적 안전에 적합한 시스템 설계와 기술적 안전 개념을 개발하며, 기술적 안전 요구사항에 시스템 설계와 기술적 안전 개념이 부합하는지를 검증하는 것을 목적으로 한다. 전제조건에는 '아이템 통합과 시험 계획', '기술 안전 요구사항의 구체화'가 있으며, 이 요구사항의 작업 결과로 기술적 안전 구상, 시스템 설계 구체화, 하드웨어-소프트웨어 인터페이스 구체화 등이 있다[8].

부품통합 및 시험은 각각의 안전 요구사항이 명세서와 ASIL 분류에 부합하는지 시험하고, 안전 요구사항을 만족하는 시스템 설계가 전체 부품에 의해 올바르게 구현되었는지를 검증하는 것을 목적으로 한다. 전제조건에는 안전 목표, 기능상의 안전 구상, 부품통합과 시험 등이 있으며, 작업 결과로 아이템 통합과 시험 계획, 통합 시험 설계 명세서, 통합 시험 보고 등이 있다.

안전 확인은 안전 목표에 부합하고 기능 안전 개념이 부품의 기능 안전에 적절한지에 대한 증거를 제공하며, 안전 목표가 차량 수준에서 정확하고 완전하며 충분히 달성되었는지를 증명하는 것을 목적으로 한다. 전제조건에는 위험 분석과 위험도 평가, 안전 목표, 확인 계획 등이 있으며, 작업 결과물로는 확인 계획과 확인 보고가 있다.

기능상의 안전 평가는 아이템에 의해 달성된 기능 안전을 평가하는 것을 목적으로 하며, 이에 대한 전제조건으로 안전 사례, 안전 계획, 검토 보고 확인과 가능할 경우의 회계 감사 확인 등이 있다. 작업 결과물로는 기능상의 안전 평가 보고가 있다.

제품을 위한 개봉은 아이템 개발 완료 시점에서 양산을 위한 배포 기준을 명세한 것으로, 양산을 위한 배포는 부품이 차량 수준에서 기능 안전을 위한 요구사항에 부합함을 확증하는 것을 목적으로 한다. 조건에는 기능상의 안전 평가 보고와 안전 사례가 있으며, 작업 결과물로는 제품을 위한 보고가 있다.

2.2 IEC 61508

IEC 61508은 전기, 전자, 프로그래밍할 수 있는 전자 장비의 기능적 안전성을 위한 국제 표준이다. 이 표준은 국제표준화 단체인 IEC(International Electrotechnical Commission)가 1980년대 중반에 개발을 시작했으며, 위험 기반의 안전성 관련 시스템 설계에 중점을 두고 있다. ISO 26262는 IEC 61508을 자동차의 전기·전자 시스템에 맞게 수정하여 개발된 표준이다.

IEC 61508 표준은 '안전 생명 주기(Safety Life Cycle)'와 '안전 무결성 기준(SIL)의 두 가지 기본 개념에 기반한다. 안전 무결성 기준은 시스템이 요구하는 이용 가능성을 충족시켜 공정에 대한 위험을 허용할 수 있는 수준으로 낮추기 위한 것이다. 안전 무결성 기준은 안전 관련 시스템이 모든 명시된 조건에서 주어진 일정한 시간 내에 요구되는 안전 기능을 수행할 확률과 가능성으로 정의되며, 안전을 위해 위험도를 줄일 수 있는 요소가 필요하다[9][10].

IEC 61508의 정량적 평가는 외부 요인의 위험 감소 장치와 안전 관련 시스템이 존재하지 않을 때 발생할 수 있는 위험 사건의 잠재적 결과를 결정하는 것이다. 발생 빈도와 결과가 확정된 위험한 경우에 대해서는 최종 사용자 컴퓨팅(EUC, End-User Computing) 위험 평가를 시행한다. 최종 사용자 컴퓨팅 위험 평가에서는 위험을 가정된 상황에서 산출된 정량적 잠재적 결과와 위험 사건의 발생 확률인 빈도의 곱으로 표현한다. IEC 61508에서 위험은 안전 무결성 기준을 도출하기 위해 사용되는 기본 개념으로, 정량적 값을 가지며 정성적인 위험 요소와 구별된다[9].

위험 매트릭스는 위험을 평가하는 도구로, 여기서 고려되는 요소는 위험 사건의 발생 빈도와 위험 사건의 심각도이다. 결과로 나온 심각성과 사건의 노출 시간을 매개변수로 사용하여 위험 사건의 발생 심각도를 평가한다. 정성적 기법은 사건의 영향과 빈도를 정확한 수치로 표현하지 못하는 단점이 있기 때문에, 각각의 매개변수를 몇 개의 일정한 수준으로 나누어 평가한다.

2.3 수명주기에 따른 신뢰성 프로그램

안전성을 보장하기 위해서는 신뢰성 강화를 위한 전반적인 이해가 요구된다. 신뢰성을 추진하는 전반적인 프로그램을 조사하면 제품 수명주기에 따른 프로그램과 신뢰성 척도, 신뢰성 수법, 신뢰성 시험 계획 및 시간에 흐름에 따른 고장원인과 대책을 조사하면 표 1과 같다. 신뢰성을 강화하기 위해서는 표 1을 연계하여 안정성에 관한 국제 규격과 ISO26262를 추진하는 것이 효과적일 수 있다.

ISO/TS 16949는 품질 관리 및 신뢰성에 중점을 두어 자동차 관련 제품의 필요한 요구사항을 결정하는 품질 관리시스템이다. 반면, ISO 26262는 RAMS(Reliability, Availability, Maintainability, and Safety)를 확보하여 자동차 제어 장치의 오작동으로 인한 사고를 예방하기 위한 기능 안전성 표준이다.

ISO/TS(Technical Specifications) 16949는 프로세스(Process)에 주 관심을 두어 제품 및 공정 품질을 개선함으로써 국제간 무역에서 신뢰성을 확보하고, 외주업체 간의 공급 체계에서 일관성을 유지하는 것을 강조한다. 반면, ISO 26262는 제품 안전에 중점을 두며, 제품 수명주기 전 단계의 기능 안전 표준과 위험 기반 안전 표준을 사용하고 ASIL 등급을 적용한다[2].

설계 시 다양한 검증 방법을 사용할 수 있으며, 정성적 방법을 사용하여 생산 부품 승인 프로세스(PPAP, Production Part Approval Process)로 승인하는 ISO/TS 16949와 달리, ISO 26262는 표준에서 요구하는 기법을 사용하며 정량적 등급을 활용한다[11].

ISO/PAS 21448(SOTIF, Safety Of The Intended Functionality)은 자율주행 시스템에서 환경과 상황에 따라 시스템의 고장이 없는 상태에서도 대처 또는 성능 한계로 인해 발생할 수 있는 위험을 방지하기 위한 안전 표준이다. ISO 21448은 자율주행 자동차의 안전성을 확보하기 위해 의도된 기능 및 구현과 관련된 모든 위험을 방지하기 위해 고안되었다[12].

ISO 26262는 전기/전자 시스템의 고장, 소프트웨어, 하드웨어 설계 및 도구의 결함에 의한 위험을 다루지만, 기술 발전으로 시스템의 자율성이 증가하면서 새로운 안전 문제가 제기되고 있다. ISO 21448은 결함이나 고장이 없더라도 의도된 기능을 제공하지 못하는 경우와 개발 단계에서 고려하지 못한 상황에서 발생하는 위험을 취급한다. 고장만을 고려하는 것이 아니라 의도되지 않은 상황을 방지하여 의도된 기능의 안정성(SOTIF, Safety Of The Intended Functionality)을 목표로 지속적인 개선을 수행해야 한다.

표 1. 생명 주기에 따른 신뢰성 프로그램
Table 1. Reliability programs according to the life cycle

Product planning / Research and development	Design	Manufacturing	Sale/Use	Etc
Top policy • Clarify reliability requirements • Set reliability goals • Collect reliability information design • Reliability program • Clarify design conditions (Usage conditions, environmental conditions, logistics conditions) • Reliability test plan • Maintainability plan • Reliability evaluation plan • Reliability prediction	• Reliability detail design • Reliability distribution • Maintainability design • Reliability prediction • Reliability design completion • Reliability test • Test analysis/evaluation • FMEA • FTA • DR	• Manufacturing reliability design • Process FMEA • Reliability Testing/Evaluation • Screening • Aging • Failure analysis • Production start • Shipping quality assessment	• Claim processing (PLD/PLP) • Reliability data collection(reliability & maintainability data) • Fault repair data • Before/After service • Market status reporting • Maintenance • Maintenance periodic /Maintenance method	• Components (product design, production technology & information management) • Designers of the product being reviewed, Reliability, Quality, Manufacturing, Service, Purchasing, Materials, Packaging/Shipping, Sales Stakeholder Negotiation

Reliability measures	Initial causes of failure	Accidental failure causes	Causes of wear failure
Reliability, MTBF, MTTFF, Failure rate, Internal life maintenance, MTBHE, System validity, MTBO, MTTF, Safety of characteristics, Defect rate Malfunction rate MTBM, Criticality of components	• Failure due to design errors • Use of substandard raw materials & components • Insufficient quality control • Insufficient debugging • Poor manufacturing & processing handling technology • Improper assembly during the process • Contamination • Improper installation & startup • Failure of components during storage & transportation • Improper packaging & transportation • Failure during transportation & storage • Failure during startup • User error	• Low safety factor • Stress (load) is higher than expected and strength is lower than expected • Assembly error • User malfunction/error • Failure not detected by the best inspection method • Failure not found during debugging • Failure due to failure that cannot be prevented by the best preventive maintenance • Failure due to natural disaster • Lack of overload and abnormal condition detection method • Failure due to abnormal usage conditions	• Corrosion or oxidation • Wear or fatigue • Aging & deterioration • Shrinkage & cracking • Use of short-life parts • Insufficient maintenance • Improper disassembly & assembly

Application of reliability methods	Early failure countermeasures	Contingency plans	Wear and tear countermeasures
FMEA, FMECA, FMPA, FAM, RFMA, FHA, EMEA, EMECA, FTA, ETA **Reliability test plan** Determination of warranty life, Determination of shape parameters, Determination of reliability scale, Determination of number of samples, Calculation of test time, Determination of confidence level, Acceptance criteria, Analysis of test effectiveness, Determination of accelerated life test method, Determination of test items, Determination of major failure modes & test items, Investigation of global quality certification standards(Reliability evaluation items)	• Redundant design • (Redundancy derating) • Load reduction • Product simplification • Use of high-reliability components • Reliability test automation • Process quality control, early flow control • Debugging • Aging/ Burn-In • Manufacturing technology education & training, improvement • Writing and distribution of user manuals	• Monitoring • Prevention of user errors, misuse & abuse • Design considering accurate stress information • Robust design • Preventive & predictive maintenance methods • Improvement of manufacturing technology • Automation of manufacturing processes	• Preventive maintenance through predictive maintenance • Use of parts made of strong materials • Management of reliability & maintainability information

III. ISO 26262에서의 신뢰성 수법

3.1 FMEA 평가 방법

FMEA는 시스템 개발 동안 발생할 수 있는 고장을 감지하고 이를 회피하거나 고장으로 인한 영향을 감소시키기 위해 수행하는 기법으로, 다음과 같은 목적으로 활용된다.

먼저 잠재 고장 모드를 확인하고 그 영향에 대한 중요도를 평가하며 원인을 분석하는 것이다. 다음으로, 고장을 회피하거나 제품 및 공정의 문제를 제거, 예방하고, 영향을 최소화하기 위한 대책을 마련하는 데 사용된다. 또한, 고장에 따른 위험 평가를 통해 개선 가능성을 식별하는 목적도 있다. 이 평가를 통해 중요 관리 특성을 확인하고 공정 및 설계의 잠재 결함에 대한 순위를 결정할 수 있다.

소프트웨어 FMEA의 분석 대상인 아키텍처 뷰(Architecture view)와 안전 분석 시 고려해야 할 영향성 범위의 제한, 컴포넌트(Components)의 안전 분석 순서 등의 내용이 포함되어 있다.

기존 기준을 사용한 결과와 이 논문에서 제안한 기준을 사용한 결과를 비교한 결과, 제안한 기준이 차량용 내장형 소프트웨어 FMEA에 더 효율적임을 확인하였다. 안전 목표를 위한 요구사항이 13%, 소프트웨어 FMEA의 횟수가 50% 이상 감소하였으며, 안전 메커니즘의 조정으로 소프트웨어 실행 시간도 개선되었다[11].

FMEA는 분석 대상에 따라 그림 2와 같이 제품 FMEA와 공정 FMEA로 구분된다. 제품 시스템 FMEA는 시스템과 외부 요소 간의 상호 작용 시 발생할 수 있는 잠재적 고장을 분석하며, 신규 시스템의 개념 개발 단계에서 위험 식별을 위해 수행된다. 제품 설계 FMEA는 시스템 내부의 하드웨어와 소프트웨어 구성 요소에서 발생할 수 있는 잠재적 고장을 분석하기 위해 수행된다. 공정 FMEA는 제품의 생산, 보관, 출하 등의 공정 과정에서 발생할 수 있는 위험을 분석하기 위해 수행된다.

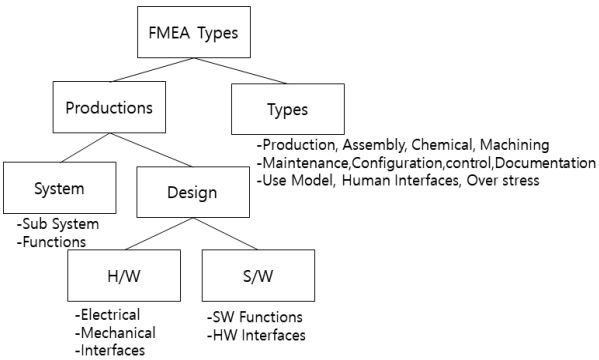


그림 2. FMEA 응용분류
Fig. 2. FMEA application classification

특히 FMEA를 효과적으로 적용하기 위해서는 기능 고장 해석(FFA, Funtion Failure Analysis)을 실시해야 한다. 기능 고장 해석은 기능에 대한 정의 및 규격, 기능과 부품 간의 연관 관계, 부품 내의 연관 관계, 기능 고장을 규명하는 과정이다. 이러한 기능 고장 분석을 통해 기능적 고장 해석뿐만 아니라 다른 기능에 미치는 영향도 분석할 수 있다.

3.2 FTA 적용 방법

기존 ISO 26262의 기능 고장 분석을 위해 수행된 FTA는 알려진 영향으로부터 가능한 원인을 찾아가는 연역적 추론 방식이었다. 참고문헌[12]에서는 기존 FTA 분석 방법을 개선한 새로운 FTA 분석 기법을 발표하였다[13][14]. 이 논문은 기존 연구에서의 문제점을 개선하기 위해 두 가지 연구 목표를 설정하였다. 첫 번째는 시스템의 개념 설계 단계에서 확보할 수 있는 설계 정보 중 기능 분석 결과에 기반하여 Top-Event 분간, 이벤트 분해 및 조합 등을 도출해 기능 기반 Fault Tree를 생성하는 것이다. 두 번째는 이렇게 도출된 기능 기반 Fault Tree를 활용하여 위험 요소 분석 방법을 제시하는 것이다.

그림 3은 언급된 논문에서 개선된 FTA를 수행하는 절차를 나타낸 것이다. 이 논문에서 제시한 방법에 따라 만들어진 기능 기반 Fault Tree는 식별된 모든 사건과 사건의 조합이 설계 초기 기능 분석 결과를 활용하여 도출된 것이다[13][14].

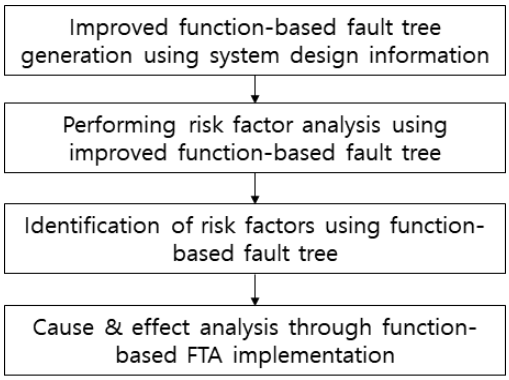


그림 3. 개선된 FTA
Fig. 3. Improved FTA

즉, 설계 과정에서 식별한 모든 기능에 대한 고장을 분석하여 Fault Tree에 반영하고, 기능 기반 FTA를 통해 기능 수준에서 위험 요소, 원인, 영향을 식별할 수 있음을 확인할 수 있었다. 이 결과를 활용하여 안전 생명 주기에서 기능 안전 개념 결정 단계에서 기능 안전을 도출할 수 있다.

기존 연구에서의 Fault Tree는 기존의 고장 정보에서 역으로 고장 모드와 관련된 기능을 식별하여 연결하게 하는 수준에서 도출되었다.

기존 방식에서는 구성품 수준에서 위험 요소의 기술, 영향, 원인 분석이 이루어지기 때문에, 안전 기능이 어떤 기능의 고장과 관련하여 필요한지, 다른 기능에 어떤 영향을 미치지 않도록 구현해야 하는지 등을 결정하는 데 어려움이 있었다.

표 2. 기존 및 개선된 FTA 차이점
Table 2. Differences from existing FTA application

Differences from the application of existing FTAs	
Existing FTA	·Identify which function is associated with the failure information ·Cause of risk factor -> Failure at component level ·Impossible to perform safety design according to safety life cycle ·High possibility of missing risk factors ·Quick and easy identification of risk factors
Improved FTA	·Deriving events by utilizing the functional analysis results derived during the design process ·Risk factors and causes -> identified at the functional level ·Design can proceed according to safety life cycle ·Low chance of missing risk factors ·Slower risk identification than before

앞서 제시한 기능 기반 FTA를 통해 위험 요소, 원인, 영향이 기능 수준에서 명확히 정의되어, 다음 절차인 기능 안전 개념 결정 단계에서 안전 기능이 어떤 기능의 고장에 대응하는 것인지, 원인이 되는 다른 기능의 고장을 어떻게 차단할 것인지, 다른 기능에 영향을 미치지 않도록 어떻게 할 것인지 등을 명확히 정의할 수 있다. 이렇게 하면 차후 상세한 설계 단계에서 안전 기능을 구현함으로써 설계 단계에서 이전보다 나은 수준의 안전을 확보할 수 있게 된다. 표 2에 기존 및 개선된 FTA 차이점을 요약하였다.

3.3 신뢰성 실험

3.3.1 수명주기에 따른 신뢰성 시험

제품 개발은 상품 기획, 개념 설계, 예비 설계 및 상세 설계를 거쳐 프로토타입과 시제품(Pilot)을 개발하고, 설계 검증 및 양산 검증을 거쳐 양산 단계에 이르게 된다.

표 3은 수명주기에 따른 신뢰성 시험 및 기술적 보고서입니다. 수명주기 동안 기능 및 성능 시험, 환경시험, 안전 시험 및 신뢰성을 실시하며, 시험 중에 발견된 설계 결함은 설계 변경을 통해 시정한다.

표 3. 수명주기에 대한 신뢰성 시험과 기술적 보고서
Table 3. Reliability tests and technical report over the life cycle

<table>
<tr><th>Product planning/research and development</th><th>Design</th><th>Manufacture (Mass production)</th><th>Sale/use</th></tr>
<tr><td>• Development growth test
• Burn-in (ESS)
• Warranty test
• Functional performance test
• Reliability acceptance test</td><td>• Environmental testing
• Safety testing
• Accelerated life testing
• HALT</td><td>• Conformance test
• ESS or PRAT
• Reliability assurance test (RQT)
• Reliability acceptance test (PRAT)
• Test analysis and corrective action</td><td>• Field experiment
• Orthopedic test</td></tr>
<tr><td colspan="4">• HALT(Highly Accerlerated Life Test)
• RGT(Reliability Growth)
• TAAT(Test Analyze And Fix)
• PRAT(Production Reliability Acception Test)
• ESS(Environment Stress Screening)
• ALT(Accerlerated Life Test)
• Burn-In
• RQT(Relibility Qualification Test)</td></tr>
<tr><td colspan="4">Technical report and reliability management</td></tr>
<tr><td>• ITR • SRR • ASR
• SFR • PDR • OTTR</td><td>• CDR
• TRR</td><td>• PRR
• FCR/SVR • PCA</td><td>• ISR
• DT & OT</td></tr>
<tr><td>• ITR(Initial Technological Review)
= Outline RAM target value, RAM program plan
• SRR(System Requirement Review)
= Set system RAM target value/ Assign target value considering requirements
• ASR(Alternative System Review)
= Check RAM requirement feasibility through comprehensive risk assessment, alternative study/technical proof
• SFR(System Functional Review)
= Check whether low-level RAM requirements are sufficiently defined and whether they meet RAM requirements
• PDR(Preliminary Design Review)
= Evaluate whether component RAM design satisfies user requirements
• OTTR(OT and Readiness Review)
= Evaluate operational test capability to verify RAM requirements</td><td>• CDR(Critical Design Review)
= Evaluate whether the final RAM design satisfies user requirements
• TRR (Test Readiness Review)
= Plan/prepare to evaluate whether RAM requirements are met</td><td>• PRR(Production Readiness)
= Verification of production readiness to meet design RAM level
• FCR/SVR(Functional Configuration/Audit/System Verification)
= Satisfying RAM requirements recorded in SFR, PDR, CDR
• PCA(Physical Configuration Audit)
= Verification that RAM is not degraded during the production process</td><td>• ISR (In-Service Review)
= Evaluation of RAM achievement during field use
• DT and OT (Development Test/Operation-al Test)
= Development test & operation test</td></tr>
</table>

신뢰성 시험은 표 3에서 설계 및 양산 검증 단계에서 실시되는 개발 성장 시험과 신뢰성 보증 시험, 양산 단계에서 수행되는 번인(Burn-in) 환경 스트레스 선별시험(ESS, Environmental Stress Screening) 또는 신뢰성 수락 시험(PRAT, Production Reliability Acceptance Test)으로 구분할 수 있다.

3.3.2 B to B

백투백 시험은 어떤 한 프로그램의 두 개 이상의 변형에 동일 입력값을 주어 시뮬레이션 모델의 반응과 실제 시험 대상의 반응을 비교하여 모델과 구현물 간의 차이점을 검출하는 시험이다. 이 시험 방법은 정확성과 타이밍을 포함하여 안전 메커니즘이 정확한 기능적 성능을 보장하는지 확인한다. 백투백 시험은 다음과 같은 목적으로 활용된다: 첫째, 소프트웨어의 구현과 신형 버전의 결과를 비교하거나 오류를 발견한다. 둘째, 고품질 소프트웨어의 신뢰성을 보장하기 위해 고수준의 품질 준수 테스트로 사용된다. 셋째, 소프트웨어 개발 후 병행 프로세스 테스트에 검증 도구로 사용된다.

백투백 시험 절차는 다음과 같다, 먼저, 테스트 사례를 생성하고 동일한 입력값을 사용하여 모델과 코드에 대한 테스트 케이스를 실행한다. 그리고 결과를 분석하여 차이점을 검출하고 보고서를 작성한다. 이 시험은 제어 모델과 소스 코드 간의 품질 검증 등 높은 신뢰성이 요구되는 분야에서 사용되는 중요한 시험기법이다.

3.3.3 성능 시험

성능 시험은 시스템이 지정된 용량 및 반응 시간 등의 성능 요구사항을 충족하는지를 검증하는 소프트웨어 시험기법이다. 이 시험 방법을 통해 외부와 내부 인터페이스가 정확하고 일관성 있게 구현되었는지를 보장해야 한다. 성능 시험의 주요 목표로는 애플리케이션 결과 평가, 액추에이터(Actuator)의 속도나 강도, 전체 시스템의 응답 시간 등이 포함된다. 검증 방법으로는 외부 인터페이스의 시험, 내부 인터페이스의 시험, 인터페이스 일관성 확인, 상호작용 및 통신의 시험이 있다.

3.3.4 결함 주입 시험

결함 주입 시험은 시스템이 정상적으로 동작하는 동안 인위적인 결함(시스템 내의 오류)을 강제로 발생시켜 예외 상황에 대한 시스템의 반응을 테스트하는 기법이다. 결함은 하드웨어와 소프트웨어 두 가지 측면을 가지며, 시스템의 Fail-Safe 기능을 검증하는 특징을 갖고 있다. 이 기법은 종종 안전 요구사항의 테스트 적용 범위를 개선하기 위해 사용한다. 그림 4는 결함 주입 시험의 종류를 나타낸 것이다.

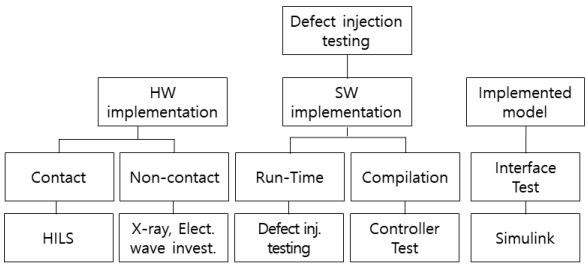


그림 4. 결함 주입 시험
Fig. 4. Defect injection test

3.3.5 에러 추정 시험

에러 추정 시험은 과거 장애에 대한 시험자의 지식이나 일반적인 장애 형태에 기반하여 결과를 도출하는 테스트 기법이다. 이 기법은 가능한 결함을 나열하고 결함이나 오류의 추정을 통해 검출하고 수정한다. 전문가 지식과 시험 대상의 에러를 추정하는 데 경험적 데이터를 이용하며, 이전에 비슷한 시험 대상에 대한 경험이 있는 시험자에게는 효과적인 방법이다. 에러 추정 테스트의 특징으로는 공식적인 기법으로 다루기 어려운 특별한 경우에 유용하며, 테스트 경험에 따라 효율성과 효과성의 수준이 달라질 수 있다. 에러 추정 시험의 장단점을 분석한 결과, 장점으로는 테스트 사례 작성 시간을 줄이고 시험자 역량을 충분히 발휘하여 시간 제약 시 효과적이다. 또한 단점으로는 테스트 경험에 따라 효과가 다르므로 일관성이 떨어지면 관리가 어려워진다는 결론을 얻을 수 있었다.

3.3.6 요구사항 분석 시험

요구사항 기법에는 요구사항 분류, 개념 모형화, 요구사항 할당, 요구사항 협상, 정형 분석 등이 포함된다.

요구사항 분류는 요구사항을 명확히 분류하여 확인하는 과정이다. 개념 모형화는 현실 세계의 상황을 단순화하여 개념적으로 표현한 모델을 만드는 과정으로 요구사항 할당은 요구사항을 만족시키기 위한 구성 요소를 식별하고 그들 간의 상호 작용을 분석하여 추가 요구사항을 발견하는 과정이다. 요구사항 협상은 요구사항이 충돌할 때 이를 해결하기 위한 과정이다. 정형 분석은 요구사항을 수학적 기호로 표현하고 이를 분석하는 과정으로 정형 분석은 요구사항 분석의 마지막 단계에서 수행된다.

3.3.7 SW 개발에서의 시험 방법

소프트웨어 개발 단계에서 사용할 수 있는 기법과 도구는 표 6에 제시하였다. 소프트웨어 개발 단계에서 사용되는 시험 방법으로는 소프트웨어 시험, 소프트웨어 통합 및 시험이 포함된다. 요구사항 분석 시험, 결함 주입 시험, 인터페이스 시험은 각 단계에서 공통으로 사용되며, 소프트웨어 시험에는 시험 케이스 관리와 구조적 범위, 소프트웨어 통합 및 시험에는 백투백 시험과 시험 범위가 포함된다.

표 6. 소프트웨어 개발 과정에서의 기술 및 도구
Table 6. Techniques and tools in the software development phase

phase	Sub-phase	Method	Tools
Software level development	SW Test	Requirements Analysis Test	HP Test-Director
		Defect injection testing	Tessy
		Interface Test	Simulink
		Test Case Management	Vector Open Test
		Structural Coverage	LDRA, SCADE Vector CAST
	Software Integration and Testing	Requirements Analysis Test	HP Test-Director
		Defect injection testing	Tessy
		Interface Test	Simulink
		Back to back comparison test	LIN emulators
		Test Coverage	Ncovereye, Bulls

Ⅳ. 결 론

자동차산업은 기계 중심이 아닌 전기 전자 제어 시스템 중심으로 급변하고 있으며, 안전성 강화를 위해 전자 장치 중심의 강화된 규정 및 지침이 필요하다.

IEC 61508과 ISO 26262는 서로 다른 등급표기를 가지고 있어 IEC 61508은 장치 산업을 주로 대상으로 하지만, ISO 26262는 대량 생산 이동식 차량을 위한 표준이다. IEC 61508은 예방과 예지보전을 중시하며 비교적 수동적인 반면에 ISO 26262는 사용 환경을 고려하여 사용자의 유동적인 판단을 중시한다.

ISO 16949는 제품 안전성과 RAMS 확보에 초점을 맞추고 있으며, ISO 21448은 산업 구조에 적용이 어렵지만, ISO 26262에서 고려하지 못하는 다양한 환경 요인과 넓은 범위의 위험을 취급한다.

FMEA의 목적과 유형을 조사하고, 기존의 FTA 수행 방식과 개선된 FTA를 비교 분석하여 개선된 FTA에서는 효과적인 위험 요소 분석이 가능하도록 분석했다. 또한, 기능 안전을 위한 시험 방법으로 신뢰성 시험 방법과 다양한 시험 방법의 절차를 제안하고, 시험자의 경험에 따른 각 시험 방법의 장단점을 조사했다.

ISO 26262를 적용한 제품은 지속적 요구될 것으로 예상되며, 효과적인 ISO 26262 기능 안전 강화를 위해 신뢰성과 연계하여 효과적인 기능 안전 관리가 가능할 것으로 기대된다.

References

[1] J.-I. Pyo, "A study of ISO 26262 functional safety in the automobile industry", Master's thesis in engineering, The Graduate School of Science and Technology, Dong-Eui University, Master's thesis, 2012.

[2] M.-S. Baek, "A Study on Evaluation of FMEA Based on Automotive Safety Integrity Level", Interdisciplinary Program of Management of Technology, The Graduate School, Pukyong National University, Doctoral; thesis, 2016.

[3] S.-R. Do, "Applying STPA to Establish a Safety Analysis System based on ISO 26262", The Graduate School, Sangmyung University, Doctoral

thesis, 2016.

[4] S.-R. Do, "A Study on the Performing of Safety Analysis of ISO26262 Development Phase Applying STPA Based on STAMP", Transactions of KSAE, Vol. 27, No. 12, pp. 965-975, Dec. 2019. http://doi.org/10.7467/KSAE.2019.27.12.965.

[5] D. Yang, S. Kim, and K. Kim, "A method of effective safety analysis through FTA for the ISO26262 functional safety", KSAE 2021 annual spring Conference, Online, pp. 541-546, Jun. 2021.

[6] J. Choi, Y. Kim, J. Cho, and Y. Choi, "The Software FMEA Guideline for Vehicle Safety", Journal of Korea Multimedia Society Vol. 21, No. 9, pp. 1099-1109, Sep. 2018. https://doi.org/10.9717/kmms.2018.21.9.1099.

[7] J. Kim and C. Lee, "Understanding SW Reliability for the Automotive Industry Based on ISO 26262", KIPE Magazine, Vol. 23, No. 1, pp. 44-47, 2018.

[8] S. Kwon, "IISO26262 Hardware Level Functional Safety Design and Evaluation", Master's thesis in engineering, The Graduate School of Science and Technology, University of Seoul, Master's thesis, 2021.

[9] S. K. Kim and Y. S. Kim, "A Study on a Safety Life Cycle of IEC 61508 for Functional Safety", Journal of Applied Reliability, Vol. 14. No. 1, pp. 81-91, Mar. 2014.

[10] B.-S. Cha, et al., "A study on improvement of ISO/IEC 29157 MAC protocol", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 13, No. 5, Oct. 2013. http://dx.doi.org/10.7236/jiibc.2013.5.17.

[11] G.-T. Lim and J.-C. Lee, "On a Method to Analyze and Verify the Functional Safety of ISO 26262 Based on Systems Engineering Framework", Journal of the Korea safety management & science, Vol. 15, No. 3, pp. 61-69, 2013. http://doi.org/10.12812/ksma.2013.15.3.61.

[12] S. Lee, "ISO 26262 and ISO/PAS 21448 as Exemption Clauses of Product Liability", Journal of IKEEE, Vol. 23, No. 1, pp. 346-349, Mar. 2019. http://doi.org/10.7471/ikeee.2019.23.1.346.

[13] H.-J. Jung and J.-C. Lee, "An Improved Method of FTA and Associated Risk Analysis Reflecting Automotive Functional Safety Standard", Journal of the Korea Academia-Industrial cooperation Society, Vol. 18, No. 9 pp. 9-17, Sep. 2017. https://doi.org/10.5762/KAIS.2017.18.9.9.

[14] S.-H. Kim and W.-J. Kim, "Designing and Implementing ISO 25000 Based Data ApplicationSystem Quality Control SW", Journal of KIIT, Vol. 12, No. 10, pp. 151-161, Oct. 2014. http://dx.doi.org/10.14801/kitr.2014.12.10.151.

저자소개

김 정 식 (Jungsik Kim)

1986년 8월 : 숭실대학교 산업공학과(공학석사)
1997년 8월 : 아주대학교 산업공학과(공학박사)
1991년 5월 ~ 현재 : 한국교통대학교 산업경영공학과 교수

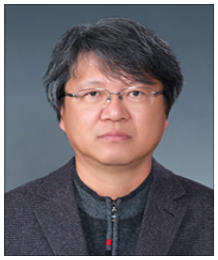
관심분야 : 신뢰성공학, 설비보전관리(TPM), 기술경영

추 병 균 (Byounggyun Chu)

2004년 8월 : 충북대학교 컴퓨터공학과(공학석사)
2010년 8월 : 충북대학교 컴퓨터공학과(공학박사)
2012년 3월 ~ 현재 : 한국교통대학교 컴퓨터공학과 강사

관심분야 : 네트워크 보안, 인터넷 통신

곽 윤 식 (Yoonsik Kwak)



1986년 9월 : 경희대학교 전자공학과(공학석사)
1994년 3월 : 경희대학교 전자공학과(공학박사)
1991년 5월 ~ 현재 : 한국교통대학교 컴퓨터공학과 교수

관심분야 : 센서네트워크, 인터넷 통신, 행정시스템