Transactions of KSAE, Vol. 29, No. 10, pp.967-980 (October, 2021)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2021.29.10.967

ISO26262 표준을 준수하는 차량용 전장 품 개발을 위한 의존 고장 분석의 적용

박 병 규*·주 백 수·이 승 환

에스피아이디 엔지니어링 사업본부

Application of Dependent Failure Analysis for Development of Automotive Electronics Complying with ISO26262 Standards

Byoungkyu Park* · Baegsu Joo · Seunghwan Lee

Engineering Division, SPID Co., Ltd., 145 Gasan Digital 1-ro, Geumcheon-gu, Seoul 08506, Korea
(Received 9 April 2021 / Revised 30 June 2021 / Accepted 2 July 2021)

Abstract : During the development of the E/E system for vehicles complying with the Functional Safety ISO 26262 standard, if interference between the elements that make up the E/E system is likely to violate the safety goals or possibly violate the mutual coexistence between the components of different quality levels, measures are required to exclude or mitigate them. The first order for these measures is to perform a dependent failure analysis. Dependent failure analysis verifies that freedom and independence are ensured from interference required by the elements by analyzing the dependency relationship between the elements constituting the E/E system. In addition, it is used to secure safety measures in order to mitigate the possible dependent failures. In this paper, we present cases of dependent failure analysis in the automotive industry and propose a document format for dependent failure analysis that can be applied in practice.

Key words : Functional safety(기능안전) ISO 26262(자동차 기능 안전성 국제 표준), Safety analysis(안전 분석), Dependent failure analysis(의존 고장 분석), Cascading failure(연계 고장), Common cause failure(공통 원인 고장), Freedom from interference(간섭으로 부터의 자유), Independence(독립성)

Nomenclature

ASIL	: automotive safety integrity level
BLDC	: brushless direct current
CAN	: controller area network
CCF	: common cause failure
CF	: cascading failure
CMF	: common mode failure
CMU	: clock monitoring unit
DFI	: dependent failure initiators
ECU	: electric control unit
ECC	: error correcting code
E/E system	: electric/electronic system
EPS	: electric Power Steering
EMC	: electromagnetic compatibility
EMI	: electromagnetic interference
FFI	: freedom from interference
FSR	: functional safety requirement
MCU	: Microcontroller unit
PCB	: printed circuit board
QM	: quality management
SPI	: serial peripheral interface

1. 서 론

국방, 항공 우주, 의료, 가전, 산업, 자동차 분야 등에서 작동되는 모든 E/E system은 필연적으로 구성 요소인 엘리먼트들의 집합으로 이루어져 있다. 이러한 엘리먼트

*Corresponding author, E-mail: pbk@espid.com

들은 설계 및 제조 상황에 따라 여러 품질 수준으로 존재하기도 하는데, 이때 서로 다른 품질 수준을 가진 엘리먼트들 간의 조합은 결함, 에러, 고장을 야기시킬 수 있는 근본 원인이 되기도 한다. 이러한 이유로 기능안전 ISO 26262:2018 표준을 준수하는 차량용 E/E system 설계에서는 서로 다른 품질 수준을 가진 구성 요소들 간에 간섭이 있어 상호 공존을 위배할 개연성이 있다면, 목표한 품질 수준을 확보하기 위하여 이에 상응하는 조치를 요구한다. 이 요구는 차량용 E/E system 내 기초 부품으로 사용되는 반도체 설계[1,2] 역시 동일하게 적용된다. 이러한 요구를 적절히 이행하기 위해서 기능안전 ISO 26262:2018 표준에서는 ISO 26262-9:2018, 7절 의존 고장 분석을[3] 참조하여 수행할 것을 권고한다. 의존 고장 분석은 정성적 안전 분석 기법 중 하나로서, 두 개 이상의 엘리먼트들을 대상으로 서로 간의 간섭 여부를 분석하고, 엘리먼트에 요구된 독립성을 확인하며, 분석을 통해 식별된 결함에 따른 영향 및 문제점에 대한 대책을 수립하는데 효과적인 분석 기법이다.[1,3]

이러한 의존 고장 분석을 자동차 산업에 적용함에 있어 참조할 만한 자료는[1-11] 손쉽게 접근이 가능하다. 하지만 아쉽게도 실무에 바로 적용할 수 있는 차량 E/E system 관련 의존 고장 분석 사례는 찾아보기 어렵다. 사실, 참조 문헌[4]에서 전동식 파워 스티어링(EPS)에 대한 의존 고장 분석 방안을 소개하였으나, 기술된 아키텍처에 대한 어떠한 설명이 없고, 정형화된 양식 없이 의존 고장 분석을 다루었기 때문에 전동식 파워 스티어링(EPS)의 의존 고장 분석을 이해하는데 어려움이 있었다.

이에 본문에서는 실무에 적용할 수 있는 의존 고장 분석 문서 양식을 제안하고, 제안된 문서 양식을 사용하여 실증 사례인 전동식 파워 스티어링(EPS)에 대한 의존 고장 분석을 시스템 개발, 하드웨어 개발, 소프트웨어 개발 수준으로 보여줌으로써, 차량 E/E system 관련 의존 고장 분석의 이해와 더불어 제안된 양식의 효용성을 설명한다.

2. 의존 고장 분석의 이해

2.1 의존 고장 분석의 목적과 정의

의존 고장 분석은 E/E system을 구성하는 엘리먼트들 간에 의존 관계를 분석하여 엘리먼트에 요구되는 간섭으로부터 자유 및 독립성이 확보되었음을 확인하고, 발생 가능한 의존 고장에 대해, 필요 시 이를 완화시키기 위한 안전 조치수단을 확보하는 것이다.[3]

2.2 연계 고장과 공통 원인 고장

의존 고장에는 연계 고장(CF) 과 공통 원인 고장(CCF)이 있다.[1-6]

2.2.1 연계 고장

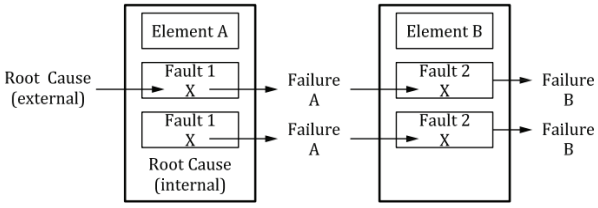

Fig. 1 Cascading failure[1,3-6]

위 Fig. 1은 연계 고장에 대한 참조 그림으로서 연계 고장의 메커니즘을 보여준다. Fig. 1에서 보는 바와 같이 연계고장은 엘리먼트 A의 내부 또는 외부의 근본 원인(Root cause)으로 인해 초래된 엘리먼트 A의 고장이 엘리먼트 B로 연계되어 엘리먼트 B가 고장이 발생하는 현상이다.[1,3-6] (엘리먼트 B는 엘리먼트 A와 동일한 아이템이거나 다른 아이템이 될 수 있다. 여기서의 아이템은 기능안전 ISO 26262-1:2018에서 정의된 것을 의미한다.)[5]

2.2.2 공통 원인 고장

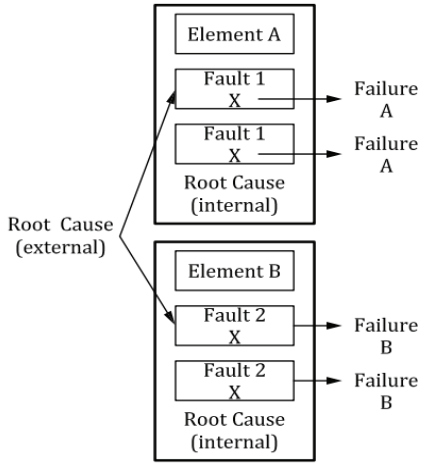

Fig. 2 Common cause failure[1,3-6]

위 Fig. 2는 공통 원인 고장에 대한 참조 그림으로서, 공통 원인 고장의 메커니즘을 보여준다. Fig. 2에서 보는 바와 같이 공통 원인 고장은 아이템의 엘리먼트 내부 또

는 외부로부터 야기 되는 근본 원인(Root cause)의 결과로 두 개 이상의 엘리먼트가 고장 나는 현상이다.[1,3-6] 이러한 공통 원인 고장에는 하나의 공통된 근본 원인으로 인하여 여러 엘리먼트가 같거나 유사한 고장 모드가 동시에 발생하는 공통 모드 고장(CMF)을 포함한다.[5,7]

2.3 독립성과 간섭으로 부터의 자유

독립성과 간섭으로 부터의 자유는 의존 고장 분석에 있어서 매우 중요한 분석 대상이다.[1-3,6]

다음은 독립성과 간섭으로 부터의 자유에 대한 설명이다.

2.3.1 독립성(Independence)

독립성이란 “안전 요구사항을 위반할 수 있는 두 개 이상의 엘리먼트 간에 의존 고장이 없는 상태”를 말한다.[3,5] 즉, 독립성 요구를 충족한 엘리먼트는 연계 고장(CF)과 공통 원인 고장(CCF)이 없다. 이러한 독립성 요구의 실현은 안전 설계 구현에 있어 매우 중요한 요소 중 하나이다.

하지만, 차량 전장 품 설계에 있어, 요구된 엘리먼트에 대한 독립성 실현은 쉽지 않는 것이 현실이다. 차량 아이템을 구성하는 엘리먼트인 센서 모듈이나 제어 모듈 등과 같은 서로 다른 제조사로부터 제조되고 완제품으로 존재하는 차량 전장품들에 대한 독립성 요구의 실현은 상대적으로 수월한 편이나 이와 달리, 하나의 PCB 기판에 실장 되어 동일한 공간에 존재하는 개별 전자 부품(엘리먼트)들에 대해서는 독립성 요구를 충족시키기 위한 설계는 매우 까다롭다. 특히, 공통 원인 고장을 완전히 배제시키기가 어렵다. 이는 단가를 중요하게 여기는 자동차 산업의 특수성에 따른 한정된 PCB 공간 및 한정된 하드웨어 자원으로 기인한다. 일반적으로 E/E system의 엘리먼트에 요구된 독립성 확보 하기 위한 수단으로써 이중화 된 설계를 하게 되는데 이중화 된 설계는 분리된 전원 소스와 (논리적 또는 물리적으로) 분리된 메모리, 분리된 처리 장치, 분리된 입출력 장치 등과 같은 이중화 된 리소스 등이 요구 될 수 있으며, 뿐만 아니라 더러는 EMC/EMI로부터 보호하기 위한 개별 차폐 등이 요구 될 수도 있다. 이러한 요구들로 인하여 더 넓은 PCB Size 및 더 많은 하드웨어 리소스가 필요하게 된다. 이는 결국, 단가 상승으로 이어질 수 있음으로 차량 전장 품 제조사들이 기피하는 이유가 된다. 그렇기 때문에 차량 E/E system에서의 독립성은 모든 엘리먼트에 적용하는 것 보다는 필요한 부분을 적절히 식별하여 적용하는 것이 합리적이다.

2.3.2 간섭으로 부터의 자유(FFI)

간섭으로 부터의 자유(Freedom from interference)란 “안전 요구사항을 위반할 수 있는 둘 이상의 엘리먼트 간에 연계 고장(CF)이 없는 상태”를 의미한다.[3,5] 이것은 분석 대상 엘리먼트에 대한 고장이 다른 엘리먼트의 고장으로부터 초래 된 것이라면, 분석 대상 엘리먼트는 ‘간섭으로부터 자유롭지 않다’라는 의미이다.

2.4 의존 고장 이니시에이터(DFI)

Dependent Failures Initiator(DFI) 란 의존 고장이 발생하는 근본 원인(Root cause)을 말한다.[2,3,5]

의존 고장 분석에 있어서 근본 원인을 식별하는 이유는 의존 고장에 대한 적절하고 합당한 조치를 마련하기 위함이다. 이러한 조치를 완화 조치(Mitigation measures)[2]라 부르며, 본문의 ‘2.6 의존 고장 완화 조치’에서 자세히 설명한다.

DFI를 식별하는 제안된 방법으로써, ISO 26262-9:2018, Annex C[3]를 참조한다. 아래와 같이 차량 E/E System에 존재 가능한 7가지로 분류된 결합 요소(Coupling factor) 별 DFI 예를 System, HW, SW, Semiconductor 개발 수준으로 제공한다.[3]

-. Shared resource
-. Shared information input
-. Insufficient environmental immunity
-. Systematic coupling
-. Components of identical type
-. Communication
-. Unintended interface

그리고 ISO 26262-11:2018, 4.7.5[2]에서는 반도체 엘리먼트에 대한 참고할 만한 각 사례 별 DFI 목록 및 대책을 제공해 준다.

2.5 의존 고장 분석의 필요성

독립성은 ASIL 분해에 대한 정당성을 부여해 주고,[2-3,5] 간섭으로 부터의 자유는 서로 다른 품질 수준을 갖는 엘리먼트들 간의 공존 기준을 충족시켜준다.[1-3] 뿐만 아니라, 독립성과 간섭으로 부터의 자유는 안전 메커니즘의 유효성 측면에서 중요하게 적용된다.[1,2]

다음 Fig. 3은 이러한 의존 고장 분석의 이점을 보여준다.

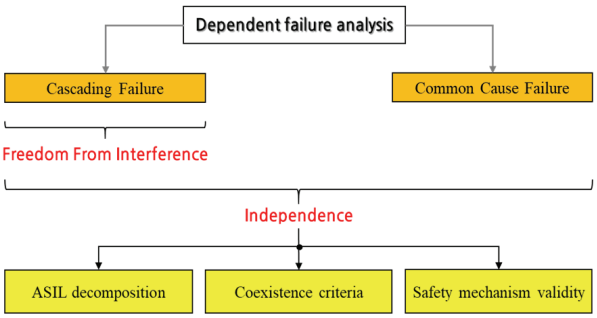

Fig. 3 Benefits of dependent failure analysis[1-3)]

2.5.1 ASIL 분해(Decomposition)

ISO 26262-9:2018에서 설명된 ASIL 분해[3)]는 하나의 안전 요구사항을 중복된(Redundant) 형태로 나누기 위해 안전 요구사항을 분해하게 되는데, 이 때 분해된 안전 요구사항을 구현하는 엘리먼트에 대한 독립성(Independence)을 요구한다.[2,3,5)] 독립성이 요구된 개별 엘리먼트는 의존 고장 분석을 통해 연계 고장과 공통 원인 고장이 없다는 것을 증명해야 한다. 설사 의존 고장이 있더라도 이를 완화할 수 있는 안전 조치를 제시하고, 안전 조치가 효과적으로 의존 고장을 완화한다는 증명을 해야 한다. 만약 이를 증명하지 못한다면, ASIL 분해는 이루어지지 않는다.[3)]

2.5.2 공존 기준(Coexistence Criteria)

예컨대, QM과 ASIL A 조합, ASIL B와 ASIL C 조합 등과 같은 ASIL 할당 및 ASIL 분해의 결과로 초래된 서로 다른 품질 수준을 갖게 되는 엘리먼트들 간의 조합은 기능안전 측면의 문제를 야기 하는 원인이 되기도 한다. 왜냐하면, 품질 수준이 낮은 엘리먼트는 품질 수준이 높은 엘리먼트보다 고장 날 확률이 높고, 이로 인해 안전 목표 위배 확률 역시 커질 수 있기 때문이다. 이러한 이유로, 품질 수준이 낮은 엘리먼트의 고장이 품질 수준이 높은 엘리먼트의 고장으로 이어지면 안 된다. 그렇기 때문에, 기능안전 ISO 26262-9:2018 표준에서는 아키텍처 설계 시 서로 다른 품질 수준을 갖은 엘리먼트들에 대한 조합의 조건으로 공존 기준(Coexistence criteria)을 제시한다.[3)]

Fig. 4는 서로 다른 품질 수준을 갖은 엘리먼트 조합에 있어서 공존 가능과 불가에 대한 비교 그림이다. 상위 품질 수준을 갖는 안전 관련 엘리먼트인 1과 하위 품질 수준을 갖는 비 안전 관련 엘리먼트 2와의 조합에 있어서 엘리먼트 1의 고장의 원인이 엘리먼트 2에 있다면, 이것은 연계 고장에 해당한다. 즉, 엘리먼트 1은 엘리먼트 2의 간섭으로부터 자유롭지 못하다. 이 경우, 비 안전 관련 엘리먼트 2는 엘리먼트 1의 품질 수준을 부여받아 안전 관련으로 취급된다. 하지만, 이와는 달리, 안전 관련 엘리먼트 5와 비 안전 관련 엘리먼트 6과의 조합에 있어서 상위 품질 수준을 갖는 엘리먼트 5의 고장의 원인이 하위 품질 수준을 갖는 엘리먼트 6에 있지 않는다면, 이것은 연계 고장이 없다는 것을 의미한다. 즉, 엘리먼트 5는 엘리먼트 6의 간섭으로부터 자유롭다. 이 경우, 엘리먼트 5와 엘리먼트 6은 서로 다른 품질 수준을 갖더라도 공존이 가능하다. 이러한 공존 기준 메커니즘은 서로 다른 ASIL 등급을 갖는 안전 관련 엘리먼트들 간의 조합에 있어서도 동일하게 적용된다.

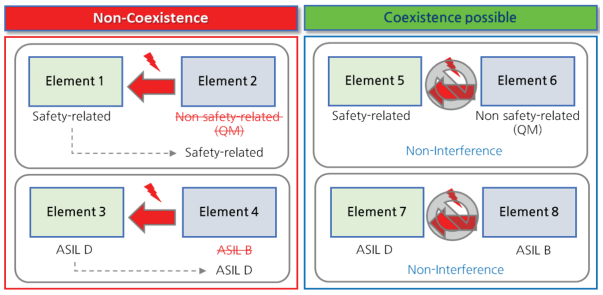

Fig. 4 Coexistence criteria mechanism

2.5.3 안전 메커니즘 유효성(Safety Mechanism Validity)

기능 안전에서의 안전 메커니즘은 안전 목표를 위배할 개연성이 있는 엘리먼트의 고장을 회피하거나 억제하기 위한 설계적 관점의 실질적 수단으로서 사용된다. 이러한 안전 메커니즘이 얼마나 신뢰할 만한지 평가하기 위하여 안전 메커니즘에 대한 효과성(Effectiveness)과 더불어 안전 메커니즘의 유효성(Validity)을 확인해야 한다. 안전 메커니즘의 효과성은 안전 메커니즘의 동작이 의도한 대로 수행하는지를 확인하는 것이다. 이를 위해 안전 메커니즘에 대한 기능 및 성능 테스트를 수행한다. 그리고, 안전 메커니즘의 유효성은 안전 메커니즘이 간섭으로부터 자유로운지를 확인하는 것이다. 이를 위해 안전 메커니즘에 대한 의존 고장 분석을 수행한다.

의존 고장 분석을 통해 안전 메커니즘과 안전 메커니즘이 모니터링하는 엘리먼트 사이에 연계 고장이 없음을 확인하고, 만약 있다면, 연계 고장에 대한 완화 조치를 마련해야 한다. 왜냐하면, 최악의 경우, 안전 메커니즘이 모니터링하는 대상 엘리먼트의 고장이 안전 메커니즘의 고장으로 이어진다면, 그 안전 메커니즘은 신뢰하기 어렵기 때문이다. 이는 결국 해당 안전 메커니즘을 개선해야 할 이유가 된다. 그리고 안전 메커니즘의 유효성 측면에서 한 가지 더 고려되어야 하는 것은 안전 메커니즘에 대한 독립성이다. 사실 안전 메커니즘은 간섭으로부터 자유로운 것 보다는 독립성을 충족하는 것이 더 좋다. 그 이유는, 안전 메커니즘이 독립성을 충족할 경

우, 연계 고장과 공통 원인 고장으로부터 자유롭기 때문에 간섭으로부터 자유로운 것 보다 훨씬 신뢰할 수 있기 때문이다.

하지만, 앞서 밝힌 바와 같이 차량 산업의 특수성으로 인해 동일 PCB 기판에 여러 엘리먼트들과 상호 공존하는 안전 메커니즘의 엘리먼트는 공통 원인 고장으로부터 자유롭지 못할 때가 종종 있다. 이러한 상황에서 안전 메커니즘의 유효성에 대한 최상 조건은 연계 고장과 공통 원인 고장이 없는 독립성을 충족한 것이며, 최소 조건은 연계 고장이 없는 간섭으로부터 자유를 충족한 것이다.

2.6 의존 고장 완화 조치

ISO26262-11:2018, 4.7.5에서 기술된 의존 고장 완화 조치(Mitigation measures)는 Avoidance와 Control 두 가지가 있다.[2)]

2.6.1 방지(Avoidance)

출시 전 의존 고장 발생의 근본 원인을 배제하여 출시 후 운용 중 의존 고장의 발생을 회피하는 조치이다.[2)] 예) Isolation, Partitioning, Redundancy/Diversity design, Robust design, 전용 생산 시험 등.

2.6.2 제어(Control)

의존 고장의 발생을 방지하지 못하지만, 안전 목표를 위반하지 못하도록 하는 조치로서, 의존고장이 발생했을 때 제어하거나 완화할 수 있는 조치이다.[2)]

예) On-line Monitoring(ECC, CMU, Watch-dog Timer,..), Self Test(Built-In Self-Test 포함) 등

2.6.3 완화 조치가 필요한 경우

식별된 모든 의존 고장에 대한 완화 조치가 필요한 것은 아니나 다음과 같은 상황에 대해서는 완화 조치가 필요하다.

① 서로 다른 엘리먼트들 간의 ASIL coexistence(공존)이 필요할 때

② 안전 관련 엘리먼트가 안전 목표를 위반할 개연성이 있을 때(이 경우, CF는 단일점 결함임)

③ 안전 메커니즘에 대한 유효성을 확보해야 할 때

2.7 의존 고장 분석의 수행 시점

다음 Fig. 5는 기능안전 ISO 26262 안전 생명 주기 내 각 개발 단계에서의 안전 분석 적용 시점을 나타낸 그림이다. 대표적 안전 분석인 FMEA, FTA와 의존 고장 분석은 안전 생명 주기의 여러 개발 단계에서 수행되며, 분석의 내용은 서로 관련이 있거나, 보완된다.

1) Concept 단계에서는 아키텍처 상에서의 ASIL 할당에 따른 공존 기준 수립 및 ASIL 분해에 대한 독립성 확보를 위해 의존 고장 분석을 수행한다.
2) System 설계 단계에서는 하드웨어 및 소프트웨어 그리고, 하우징 및 링크 장치 등과 같은 기구류들이 같이 통합될 때의 의존 관계를 살펴보고 이에 대한 간섭에 대한 자유성 및 독립성에 대한 요구를 충족하는지를 확인하기 위해 의존 고장 분석을 수행한다. 이때 운용(Operation) 및 환경 조건을 고려한다.
3) 하드웨어, 소프트웨어, 반도체 설계 단계 역시, 이들 개별 설계 수준에 대한 간섭에 대한 자유성, 독립성 관계를 분석하고 이에 대한 대책을 수립하기 위해 의존 고장 분석을 수행한다.

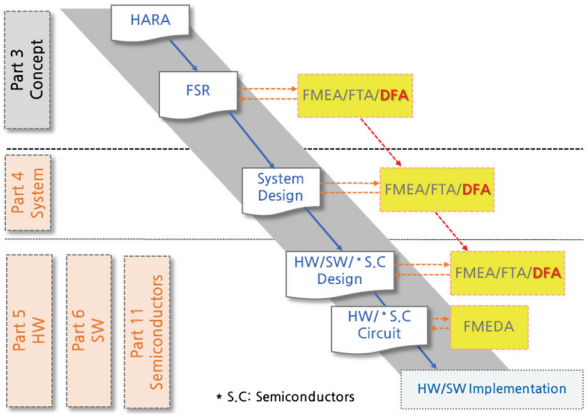

Fig. 5 Application timing of safety analysis for each development phase within the safety life cycle

2.8 의존 고장 분석 수행 가이드

ISO 26262-11:2018 부속서 B[2)]에서는 마이크로 컨트롤러에 대한 의존 고장 분석을 사례를 일부 보여주기 때문에 의존 고장 분석 수행에 있어 훌륭한 지침을 제공해 준다. 그런데, 여기에서는 분석 대상 엘리먼트를 '1:1' 또는 '1:다'로 묶어 DFI를 식별하고, 이에 따른 완화 조치를 기술하였을 뿐, 분석 대상 엘리먼트들 간의 연계고장(CF) 또는 공통 원인 고장(CCF)를 구분하지 않았다. 이는 마이크로 프로세스 설계 단계에서 의존 고장 분석이 이루어졌기 때문에, 아키텍처 설계 개선에만 중점을 둔 탓으로 생각된다.

특히 '1:다'Grouping은 의존 고장을 초래하는 근본 원인인 DFI를 식별하는데 도움이 될 수 있겠으나, 분석 대상 엘리먼트의 의존 고장 식별에 있어, 연계 고장(CF)인지, 공통 원인 고장(CCF)인지를 식별하기가 어렵다. 이는 앞서 설명한 의존 고장 분석의 이점인 독립성 및 엘리

먼트들 간의 공존 기준, 안전 메커니즘의 유효성을 증명하는 측면에 있어서, 다소 불편하다. 그럼으로 되도록 분석 대상 엘리먼트에 대한 Grouping은 '1:1' 즉, 분석 대상 엘리먼트와 그 분석 대상 엘리먼트가 연결된 다른 엘리먼트 하나만을 쌍으로 묶어 분석할 것을 제안한다.

3. 의존 고장 분석의 실무 적용

3.1 의존 고장 분석 문서 양식의 제안

아래의 Table 1은 제안된 의존 고장 분석 양식으로써, ISO 26262-11:2018 Annex B[Examples of dependent failure analysis][2]를 참조하여 만들었다. 왼쪽 부분에는 분석대상 엘리먼트들에 대한 식별된 의존 고장 현황을 기술하고, 오른쪽 부분에는 이에 대한 조치 사항들을 기술한다. 조치 사항들을 기술함으로써, 조치 사항들에 대한 추적 및 해결 현황에 대한 파악이 용이하다. 본 양식을 사용한다면 시스템/하드웨어/소프트웨어 개발 수준의 아키텍처만으로도 의존 고장을 수행하는데 충분할 것이다.

다음은 각 항목 별 기입해야 할 내용에 관한 설명이다.

1) Project name: 프로젝트 이름을 기술한다.
2) Project ID: 프로젝트 ID를 기술한다.
3) Subject: 의존 고장 분석을 수행할 제품 개발 수준을 기술한다. 제품 개발 수준에는 Concept, System, Hardware, Software, Semiconductor가 있다.
4) Start date: 의존 고장 분석 시작일을 기술한다.
5) Revision date: 의존 고장 분석 개정 날짜를 기술한다.
6) Responsibility: 의존 고장 분석에 대한 책임자 또는 책임 부서를 기입한다.
7) ID: 개별 의존 고장 분석에 대한 식별 번호.
8) Element 1: 분석 대상 엘리먼트를 기술한다.
9) Element 2: 분석 대상 엘리먼트와 연결된 다른 엘리먼트를 기술한다.
10) DFI(Dependent Failures Initiators): 의존 고장을 초래하는 DFI를 식별하여 기술한다. 참고할 만한 문서는 참조 문헌 2), 3), 8), 9), 10)이다.
11) Effects from dependent failure: 분석 대상 엘리먼트들 간의 의존 고장으로 인한 영향을 기술한다.
12) Is there a probability of violating safety goals ?: 분석 대상 엘리먼트들 간의 의존 고장이 어떠한 안전 목표를 위배할 가능성이 있는지를 기술한다. 안전 목표 위배 가능성이 있는 의존 고장일 경우, 반드시 완화 조치가 마련되어야 한다.
13) CCF/CF: 의존 고장 타입을 구분한다. 공통 원인 고장이면 CCF를 표기하고, 연계 고장이면, CF를 표기한다.
14) Measure for fault (A)Voidance or (C)Ontorl: 의존 고장에 대한 완화 조치를 기술한다. (A)Voidance 일 경우, 조치에 (A)를 표기하고, (C)Ontorl 일 경우, 조치에 (C)를 표기한다.
15) Verification method: 완화 조치를 검증할 수 있는 방안을 기술한다. 이는 마련된 완화 조치가 해당 의존 고장을 의도대로 완화시켰음을 증명하기 위함이다.
16) Does the described measure to apply ?: 기술된 완화 조치가 적용 되었는지를 표기한다.
17) If the described measures are not applied, why ?: 기술된 완화 조치를 적용 하지 않았다면, 그 이유가 무엇인지를 기술한다. 다음의 이유로 완화 조치가 적용되지 않을 수 있다.
    ① 예를 들어, 소프트웨어 안전 메커니즘을 통해 하드웨어의 의존 고장을 대처할 수 있는 대안 수단이 있는 경우라면, 하드웨어 수준의 의존 고장 분석에서는 완화 조치가 필요하지 않을 수 있다.
    ② 비록, 담당자에 의해 완화조치가 마련된다 해도, 일정/비용/기술적 난이도 등에 따라서 거절될 수 있다. 이러한 경우 거절된 완화 조치는 다시 실행 가능한 완화 조치로 변경되어야 한다.
18) The(person or department) in charge: 완화 조치 담당자 또는 담당 부서를 기술한다.
19) Identification date: 완화 조치 식별일을 기술한다.
20) Target completion date: 완화 조치 목표 완료일을 기술한다.

Table 1 Dependent failure analysis form

Project Name		Start Date	
Project ID		Revision Date	
Subject		Responsibility	

ID	Target Element		DFI (Dependent failures initiators)	Effects from dependent failure	Is there a probability of violating safety goals?	Type	Measures for dependent failures						
	Element 1	Element 2				CCF /CF	Measure for fault (A)voidance or (C)ontrol	Verification method	Does the described measure to apply?	If the described measures are not applied, why?	The (person or department) in charge	Identification date	Target completion date

3.2 의존 고장 분석 사례

다음은 전동식 파워 스티어링(EPS)에 대한 의존 고장 분석 결과를 'Table 2 시스템 개발 수준', 'Table 3 하드웨어 개발 수준', 'Table 3 소프트웨어 개발 수준' 별로 각각 보여준다. 분석 대상 엘리먼트들 간의 의존 고장에 대한 판단은 전문가의 판단에 따라 이루어지며, 안전 목표를 위배할 개연성이 있거나, 안전 메커니즘의 유효성을 보장하기 어려운 의존 고장에 대해서는 이에 대한 완화 조치를 각 개발 수준에서 마련한다. 참고로, 본 예제에 사용된 전동식 파워 스티어링(EPS)에 대한 아키텍처는 어느 특정 상용 제품이 아니며, 제안된 양식 사용에 관한 이해를 돕기 위해 작성된 것임을 밝힌다.

3.2.1 제품의 이해

전동식 파워 스티어링(EPS)은 전기모터의 힘으로 조향 핸들을 돌려주는 장치를 말하며, 운전자가 핸들을 틀어 방향을 정해 주면, 동력 조향 장치가 운전자가 원하는 방향만큼 동력을 가하는 장치이다. 전동식파워 스티어링은 회전각 센서, 토크 센서, 모터로 구성된다. 회전각 센서 및 토크 센서에서 입력되는 핸들의 동작에 따라 ECU에서 모터를 제어한다. ECU에서는 속도 등의 운전 상태에 따라 제어 모드를 변화시킨다. 아래 Fig. 6은 EPS에 대한 아키텍처이다.

1) Power supply(H1)
   배터리로부터 전원을 입력 받아 EPS 장치의 전원을 공급한다.
   PWR_Motor: BLCD 모터 전원
   +5 V: 제어기 메인 전원
2) Power monitor circuit(H9)
   배터리 전압 상태를 모니터링하여 과전압과 저전압 상태를 알아낸다.
3) Steering angle sensor(H4)
   조향 각 센서로서, 핸들의 조향 속도, 조향 방향 및 조향 각을 검출하는 역할을 한다.
4) Torque sensor(H5)
   핸들 축의 비틀림(Torsion) 힘을 측정하는 센서이다. 운전자가 핸들에 가하는 힘(Torque)를 감지한다.
5) Motor position sensor(H6)
   홀 센서로 이루어져 있으며, BLDC 모터의 위치를 알아낸다.
6) Current Sensor(H7)
   BLDC 모터의 상태를 모니터링 하기 위한 전류 센서이다.
7) Vehicle Speed Input(H8)
   CAN 통신을 통해 입력되는 차량의 속도 정보.
8) Motor Power Relay Driver(H21) &
   Motor Power Relay(H24)
   BLDC 모터의 전원을 공급하는 HW Component.
   비상시 BLDC 모터의 전원을 차단해 줌으로써 핸들을 수동으로 조작 가능 하도록 한다.
9) Flash ROM(H29)
   Boot Code와 Calibration Code가 들어 있다.

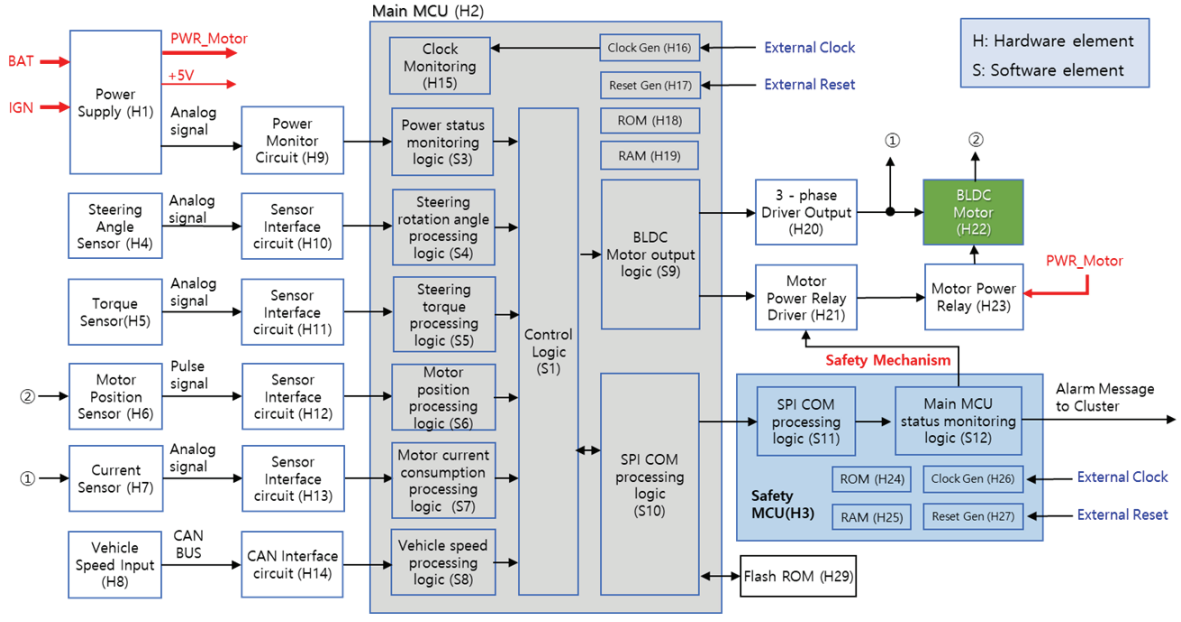

Fig. 6 EPS Architecture

10) Main MCU (H2)
전원 상태 모니터링 로직(S3), 스티어링 회전각 처리 로직(S4), 스티어링 회전력 처리 로직(S5), 모터 위치 처리 로직(S6), 모터 소비 전류 처리 로직(S7), 차속 처리 로직(S8), 제어 로직(S1), BLDC 모터 출력 로직(S9), SPI 통신 처리 로직(S10)이 실행된다.
제어 로직은(S4) 메인 로직으로서, 모든 처리 로직을 콜 한다. 또한 입력 처리 로직으로 부터 받은 데이터를 프로그램 된 알고리즘에 따라 계산하여 계산 결과를 BLDC 모터 출력 로직(S9)으로 전달한다.
Main MCU (H2)는
- Steering Angle Sensor(H4),
- Torque Sensor(H5),
- Vehicle Speed Input(H8)
으로 부터 전달받은 값(Data)를 계산하여 운전자의 조향 의지를 판단한다. 판단 결과를 SPI 통신을 통해 Sub MCU(H3)로 전달하며, 판단 결과를 BLDC 모터 출력 로직(S9)으로 전달한다.
- Vehicle Speed Input(H8)
으로 부터 입력 받은 차량 속도에 따라 조향력을 조절한다. 저속 주행시에는 조향력을 증가시켜 운전자가 핸들 조작이 용이하게 하고, 고속 주행시에는 조향력을 감소시켜 핸들을 무겁게 만든다.
- Motor Position Sensor(H6)
를 통해 BLDC 모터의 위치를 제어한다. 만약, BLDC 모터가 Stuck 되어 움직이지 않는다면,
- Motor Power Relay(H24)
를 off 시켜, BLDC 모터의 전원을 차단해 줌으로써 핸들을 수동으로 조작 가능 하도록 한다.
- Current Sensor(H7)
을 통해 BLDC 모터에 대한 open/short/over current 상태를 감시한다. 만약, BLDC 모터 상태가 이상이 있을 경우
- Motor Power Relay(H24)
를 off 시켜, BLDC 모터의 전원을 차단해 줌으로써 핸들을 수동으로 조작 가능 하도록 한다.

11) Sub MCU(H3)
SPI 통신 처리 로직 (S11)과 Main MCU 상태 감시 로직(S12)이 실행된다.
Sub MCU는 안전 메커니즘으로서,
- Main MCU(H2)
와의 SPI 통신을 통하여, Main MCU (H2)의 상태를 Main MCU로 부터의 계산 이벤트가 발생할 때 마다 모니터링한다.
- Main MCU(H2)
의 이상 동작을 감지하였을 경우,
- Motor Power Relay(H24)
를 off 시켜, BLDC 모터의 전원을 차단해 줌으로써 핸들을 수동으로 조작 가능 하도록 한다.

3.2.2 할당된 안전 목표 및 안전 요구사항

안전 요구사항을 통해 제품에 할당된 기능을 이해한다. 그리고 식별된 의존 고장이 다음의 안전 목표를 위배할 개연성이 있는 경우라면, 이에 대한 완화 조치가 마련된다.

1) Safety Goal 1
주행 중 의도하지 않는 스티어링 휠의 움직임을 방지하여야 한다. (ASIL D)
[안전 요구사항]
- EPS_REQ-1:
BLDC 모터의 상태를 매 20 ms 주기로 모니터링 하여야 한다.
- EPS_REQ-2:
주행 중 의도하지 않는 BLDC 모터의 움직임을 감지할 경우, BLDC 모터의 전원을 500 ms 이내에 차단해야 한다. (Manual 상태로 전환)

2) Safety Goal 2
주행 중 스티어링 휠의 잠김을 방지하여야 한다. (ASIL D)
[안전 요구사항]
- EPS_REQ-1:
BLDC 모터의 상태를 매 20 ms 주기로 모니터링 하여야 한다.
- EPS_REQ-3:
주행 중 운전자의 조향 의지를 BLDC 모터에 전달하였음에도 불구하고, BLDC 모터가 움직이지 않을 경우, BLDC 모터의 상태가 Stuck 일 것으로 판단하여 BLDC 모터의 전원을 500 ms 이내에 차단해야 한다. (Manual 상태로 전환)

3.2.3 시스템 수준의 의존 고장 분석

시스템 아키텍처에서 식별된 하드웨어 및 소프트웨어 엘리먼트들이 분석 대상이며, 분석 대상 엘리먼트들에 대한 사용자 시나리오 기반 분석을 수행한다. 이때 운용 조건 및 환경 조건을 고려한다.

시스템 수준에 대한 의존 고장 분석의 깊이는 시스템 아키텍처 수준까지이며, 하드웨어와 소프트웨어 엘리먼트를 고려 하나, 회로도 수준(하드웨어 소자 수준) 또는 소프트웨어 소스 코드 수준까지 할 필요는 없다. 시스템 수준의 의존 고장 분석 결과로 시스템 아키텍처 설계가 개선될 수 있다(단, 본문에서는 지면상의 이유로 개선된 시스템 아키텍처에 대한 언급은 생략한다.).

Table 2 Example of system development level dependent failure analysis for EPS

ID	Target Element		DFI (Dependent Failures Initiators)	Effects from dependent failure	Is there a probability of violating safety goals?	Type	Measures for dependent failures						
	Element 1	Element 2				CCF /CF	Measure for fault (A)voidance or (C)ontrol	Verifi-cation method	Does the described measure to apply?	If the described measures are not applied, why?	The (person or depart-ment) in charge	Identifi-cation date	Target comple-tion date
EPS_ SYS_ 1	Power supply (H1)	Main MCU (H2)	Intermittent oscillation of constant voltage +5 V occurs due to insufficient output of the Power Supply (H1).	It causes malfunction of Main MCU(H2). (During memory writing, if the voltage is momentarily low, it may result in incorrect writing)	There is a possibility of a violation of SG 1.	CF	(A) Use sufficient bypass capacitor capacity. (A) Use a regulator element with sufficient capacity.	Perfor-mance test, Design review	Y		(HW), SH, Lee	21.XX. XX	21.XX. XX
EPS_ SYS_ 2	Power supply (H1)	Main MCU (H2)	Unable to output '+5 V' due to faulty power supply(H1)	All devices including the Main MCU(H2) are inoperable.	There is no possibility of SG violation because it automatically enters manual state.	CF							
EPS_ SYS_ 3	Power supply (H1)	Sub MCU (H3)	Unable to output '+5 V' due to faulty Power Supply(H1)	All devices including the Sub MCU(H3) are inoperable.	There is no possibility of SG violation because it automatically enters manual state.	CF							
EPS_ SYS_ 4	Power supply (H1)	Motor Power Relay (H23)	Unable to output 'PWR_Motor' due to faulty power supply(H1)	BLDC motor is not driven	There is no possibility of SG violation because it automatically enters manual state.	CF							
~ OMIT ~													
EPS_ SYS_ x	Steerin g angle sensor (H4)	Sensor Interfac e circuit (H10)	Steering angle sensor(H4) wiring short circuit.	Inability to handle steering rotation angle. -> It may not reflect the driver's willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1.	CF	(A) Wiring redundancy	Design review	N	Validation is sufficient.			
							(C) Perform plausibility check on the steering angle sensor(H4) signal.	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
EPS_ SYS_ x	Torque sensor (H5)	Sensor interfac e circuit (H10)	An environmental defect - mechanical shock The torque sensor basically measures the force applied by the steering wheel, but at the same time, the force delivered from the tire can also be measured. However, the torque sensor does not know whether the force comes from the handle or from the tire.	Steering torque processing error. -> It may not reflect the driver's willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1.	CCF	(C) By measuring the torque generated by the BLDC motor output, the force delivered from the tire can be estimated.	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Since the effect of the impact received from the ground is expected to be instantaneously large, this is solved with the SW algorithm.	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
~ OMIT ~													

EPS_SYS_x	Main MCU (H2)	Sub MCU (H3)	Shared power supply	System shut down	There is no possibility of SG violation because it automatically enters manual state.	CCF	(A) Power supply redundancy	Fault injection test	N				
EPS_SYS_x	Main MCU (H2)	Sub MCU (H3)	Shared clock - glitch	Malfunction of main MCU (H2) or sub MCU(H3)	There is a possibility of a violation of SG 1, SG 2	CCF	(A) Main MCU(H2) and Sub MCU(H3) should use a device with built-in clock monitoring function.	Fault injection test	Y		(HW) SH, Lee	21.XX.XX	21.XX.XX
							(C) Clock monitoring is performed for each of the Main MCU(H2) and Sub MCU(H3) to cope with the clock abnormality.	Fault injection test	Y		(SW) BK. Park	21.XX.XX	21.XX.XX
~ OMIT ~													

3.2.4 하드웨어 수준의 의존 고장 분석

하드웨어 아키텍처에서 식별된 하드웨어 엘리먼트들이 분석 대상이다. DFI 및 이에 대한 조치는 하드웨어 소자 단위로 기술한다. 하드웨어 수준에 대한 의존 고장 분석의 깊이는 하드웨어 소자 수준까지 이며, 입력 물로 하드웨어 아키텍처 및 회로도가 포함된 하드웨어 설계 명세서가 필요하다. 하드웨어 수준의 의존 고장 분석 결과로 하드웨어 설계가 개선될 수 있다(단, 본 논문에서는 지면상의 이유로 개선된 하드웨어 설계에 대한 언급은 생략한다.).

Table 3 Example of hardware development level dependent failure analysis for EPS

ID	Target Element		DFI (Dependent Failures Initiators)	Effects from dependent failure	Is there a probability of violating safety goals?	Type	Measures for dependent failures						
	Element 1	Element 2				CCF /CF	Measure for fault (A)voidance or (C)ontrol	Verifi-cation method	Does the described measure to apply?	If the described measures are not applied, why?	The (person or depart-ment) in charge	Identifi-cation date	Target comple-tion date
EPS_HW_1	Power supply (H1)	Power monitor circuit (H9)	Broken “power monitor circuit (H9)” due to load dumps at vehicle start-up	Unable to monitor BAT voltage. This leads to the following: a. If the BAT voltage is abnormal, it may cause malfunction of the BLDC motor. b. There is a possibility of sending/receiving incorrect CAN messages when the BAT voltage is abnormal.	There is a possibility of a violation of SG 1, SG 2	CF	(C) Load dump is suppressed by adding a TVS protection element at the input of the power supply.	Fault injection test	Y		(HW) SH, Lee	21.XX.XX	21.XX.XX
							(C) An analog switch is added to the input of the power monitor circuit (H9) to prevent the power monitor circuit (H9) from being driven before starting the vehicle.		Y		(HW) SH, Lee	21.XX.XX	21.XX.XX
~ OMIT ~													
EPS_HW_X	Steering angle sensor (H4)	Sensor Interface circuit (H10)	ESD from outside.	Momentary steering torque processing error -> It may not reflect the driver’s willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1	CCF	(A) L.P.F filter design for ESD suppression	Fault injection test	Y		(HW) SH, Lee	21.XX.XX	21.XX.XX
							(C) Perform Plausibility Check on the Steering Angle Sensor (H4) signal.		N	No measure is required at the HW level because the plausibility check by SW.			

EPS_HW_X	Sensor interface circuit (H10)	Main MCU (H2)	Steering angle sensor(H4) signal processing error due to Sensor interface circuit(H10) fault.	Steering angle processing error. -> It may not reflect the driver's willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1	CF	(C) Perform plausibility check on the steering angle sensor (H4) signal.	Fault injection test	N	No measure is required at the HW level because the plausibility check by SW.			
~ OMIT ~													
EPS_HW_X	Vehicle speed input (H8)	CAN Interface circuit (H14)	Shared communication bus -> CAN message error	Vehicle speed processing error -> It may cause a sudden surprise to the driver due to the wrong torque output of the BLDC motor while driving.	There is a possibility of a violation of SG 1	CCF	(A) Use a device with CAN message error check function.	Design review	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
							(C) Message validity check by CAN protocol and message integrity check by ID, CRC check.	Fault injection test	N	No measure is required at the HW level because the plausibility check by SW.			
~ OMIT ~													
EPS_HW_X	Main MCU (H2	Sub MCU (H3)	Shared clock - glitch	Malfunction of main MCU(H2) or Sub MCU(H3)	There is a possibility of a violation of SG 1, SG 2	CCF	(A) Main MCU(H2) and Sub MCU (H3) should use a device with built-in clock monitoring function.	Design review	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
							(C) It performs clock monitoring for each of MCU(H2) and Sub MCU(H3) by HW and generates an interrupt when an abnormality is detected.	Fault injection test	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
EPS_HW_X	Main MCU (H2)	Sub MCU (H3)	Shared communication bus - SPI communication message error	Malfunction of sub MCU(H3)	There is a possibility of a violation of SG 1, SG 2	CCF	(C) Validity and integrity check for SPI communication.	Fault injection test	N	No measure is required at the HW level because the Plausibility Check by SW.			
~ OMIT ~													
EPS_HW_X	Main MCU (H2)	3-Phase driver output (H20)	Unintended effects from crosstalk.	Interference between adjacent lines caused by crosstalk causes the motor to operate unintentionally	There is a possibility of a violation of SG 1, SG 2	CCF	(A) The circuit is designed with a sufficient distance to prevent interference between lines.	Design review	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
EPS_HW_X	Main MCU (H2)	3-Phase driver output (H20)	Environmental impact due to ingress of dust and moisture.	Short occurs in the 3-Phase Driver Output circuit logic due to the inflow of dust or moisture. eventually, unintended motor operation occurs.	There is a possibility of a violation of SG 1, SG 2	CCF	(A) PCB coating is applied to prevent short circuit caused by dust or moisture.	Environ-mental test	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
							(A) Design a housing to prevent the inflow of dust or moisture.	Environ-mental test	Y		(ME) JB, Joo	21.XX. XX	21.XX. XX
~ OMIT ~													
EPS_HW_X	3-Phase drive output (H20)	BLDC motor (H22)	3-Phase drive output(H20) in-circuit MOSFET short	Malfunction of BLDC motor	There is a possibility of a violation of SG 1	CF	(A) Use a MOSFET with sufficient margin (A) Ensure sufficient PCB pattern thickness	Design review	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
							(C) Add the following circuit logic to enable periodic monitoring of the operating state of the BLDC Motor. a. Current monitoring circuit logic b. Motor position detection circuit logic	Fault injection test	Y		(HW) SH, Lee	21.XX. XX	21.XX. XX
~ OMIT ~													

3.2.5 소프트웨어 수준의 의존 고장 분석

소프트웨어 아키텍처에서 식별된 소프트웨어 엘리먼트들이 분석 대상이다.

소프트웨어 수준에 대한 의존 고장 분석의 깊이는 소프트웨어 아키텍처 수준까지이며, 소프트웨어 코드 수준까지는 아니다.[11] 입력물로 소프트웨어 아키텍처가 포함된 소프트웨어 설계 명세서가 필요하다. 그리고, ISO 26262-6:2018 부속서 E.2.2에 기술된 바와 같이, 일반적으로 하드웨어의 결함은 고려하지 않으나, 다음과 같은 일부 하드웨어 결함은 고려한다.[11]

1) 멀티 코어 시스템의 다른 Processing unit으로 매핑 되는 특정 소프트웨어(멀티 코어의 공유된 자원)
2) 소프트웨어 아키텍처 설계의 정적/동적 측면과 관련하여 소프트웨어가 실행되는 Processing unit의 세부 설계(멀티 테스킹에 따른 자원 공유, 인터럽트 처리. 특히 우선 순위)
3) 소프트웨어 관련 하드웨어 결함과 관련하여 선택된 소프트웨어 안전 메커니즘의 달성 가능한 진단 커버리지

소프트웨어 수준의 의존 고장 분석 결과로 소프트웨어 아키텍처 설계가 개선될 수 있다(단, 본 논문에서는 지면상의 이유로 개선된 소프트웨어 아키텍처 설계에 대한 언급은 생략한다.).

Table 4 Example of software development level dependent failure analysis for EPS

ID	Target Element		DFI (Dependent Failures Initiators)	Effects from dependent failure	Is there a probability of violating safety goals?	Type	Measures for dependent failures						
	Element 1	Element 2				CCF /CF	Measure for fault (A)voidance or (C)ontrol	Verifi-cation method	Does the described measure to apply?	If the described measures are not applied, why?	The (person or depart-ment) in charge	Identifi-cation date	Target comple-tion date
EPS_SW_1	Control logic (S1)	Power status monitoring logic (S3)	Power status monitoring logic (S3) is not executed due to the stuck of the control logic(S1). -> Although the power condition monitoring logic (S3) itself is not faulty, a fault that cannot be executed due to the control logic(S1) occurs!	Unable to monitor BAT voltage. This leads to the following: a. If the BAT voltage is abnormal, it may cause malfunction of the BLDC motor. b. There is a possibility of sending/receiving incorrect CAN messages when the BAT voltage is abnormal.	There is a possibility of a violation of SG 1, SG 2	CF	(C) Addition of an external watch-dog Timer with a window to release the stuck of the control logic.	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Switching to manual state via safety MCU(H3).		Y		(SW) BK. Park	21.XX. XX	21.XX. XX
EPS_SW_2	Control logic (S1)	Power status monitoring logic(S3)	Overlapping of variables due to the use of global variables		There is a possibility of a violation of SG 1, SG 2	CCF	(A) Memory partitioning and Restricted use of global variables.	Design review	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Memory protection through memory management unit(MMU)		N	This can be solved through memory partitioning and Restricted use of global variables.			
EPS_SW_3	Control logic (S1)	Power status monitoring logic(S3)	RAM data error due to soft fault		There is a possibility of a violation of SG 1, SG 2	CCF	(C) RAM fault control through ECC/EDC functions	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
EPS_SW_4	Control logic (S1)	Power status monitoring logic(S3)	Inability to execute the power condition monitoring logic(S3) caused by a scheduling fault(incorrect execution time assignment).		There is a possibility of a violation of SG 1, SG 2	CCF	(A) Task scheduling simulation.	Simu-lation	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Task execution check monitoring	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
~ OMIT ~													

EPS_SW_X	Control logic (S1)	Steering rotation angle processing logic(S4)	Steering rotation angle processing logic(S4) is not executed due to the stuck of the control logic(S1). -> Although the Steering rotation angle processing logic (S4) itself is not faulty, a fault that cannot be executed due to the control logic(S1) occurs!	Steering angle processing error. -> It may not reflect the driver's willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1, SG 2	CF	(C) Addition of an external watch-dog timer with a window to release the stuck of the control logic.	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Switching to manual state via Safety MCU(H3).		Y		(SW) BK. Park	21.XX. XX	21.XX. XX
EPS_SW_X	Control logic (S1)	Steering rotation angle processing logic(S4)	Unintended data corruption due to shared memory usage.	BLDC motor may malfunction due to sensor value processing error -> It may not reflect the driver's willingness to steer while driving, which may lead to an accident.	There is a possibility of a violation of SG 1, SG 2	CCF	(A)Restricted use of global variables.	Coding rule check	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Redundant calculation through Safety MCU(H3).	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
~ OMIT ~													
EPS_SW_X	Control logic (S1)	SPI COM processing logic (S10)	Sending/receiving incorrect messages due to loss or damage of SPI communication messages.	1. The system is not booted because the boot code cannot be read from the flash memory. 2. May cause malfunction of the Safety MCU(H3).	There is a possibility of a violation of SG 1, SG 2	CF	(C) Implementation of SPI protocol	Fault injection test	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Implementation of CRC code		Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) SPI Self Test : Self test is performed to check if there is any abnormality in SPI communication during initialization..		Y		(SW) BK. Park	21.XX. XX	21.XX. XX
EPS_SW_X	Control logic (S1)	SPI COM processing logic (S10)	Unintended data corruption due to shared memory usage.		There is a possibility of a violation of SG 1, SG 2	CCF	(A) Memory partitioning and restricted use of global variables.	Design review	Y		(SW) BK. Park	21.XX. XX	21.XX. XX
							(C) Memory protection through memory management unit (MMU)		N	This can be solved through memory partitioning and restricted use of global variables.			
~ OMIT ~													

4. 결 론

위 본문에서는 정성적 안전 분석 기법 중 하나인 의존 고장 분석에 대한 이해를 도모하고자 목적과 정의, 필요성과 같은 의존 고장 분석에 대한 이론을 자세히 설명하였다.

또한, 의존 고장 분석 수행을 방법을 가이드 하였으며, 현업에서 적용 가능한 의존 고장 분석 양식을 제안하였다. 특히, 제안된 양식을 사용하여 전동식 파워 스티어링(EPS)에 대한 의존 고장 분석 사례를 시스템, 하드웨어, 소프트웨어 개발 수준 별로 기술함으로써, 제안된 의존 고장 분석 양식의 현장 적용 가능성 및 효용성을 보여주었다. 이를 통해 본 논문이 산업 현장에서의 의존 고장 분석 수행에 있어 적절한 도움이 되기를 기대해 본다.

References

1) S. Chonnad, R. Iacob and V. Litovtchenko, Dependent Failure Analysis For Safety-Critical IP And SoCs, Semiconductor Engineering, November 2nd, 2020.
2) ISO 26262-11:2018, Road Vehicles Functional Safety Part 11: Guidelines on Application of ISO 26262 to Semiconductors, 2nd Edn., 2018.
3) ISO 26262-9:2018, Road Vehicles Functional Safety Part 9: Automotive Safety Integrity Level(ASIL)-Oriented and Safety-Oriented Analyses, 2nd Edn., 2018.
4) S. J. Moon, K. S. Keum, H. J. Kim, H. T. Moon and H. Y. Bhae, “ISO 26262 Dependent Failure Analysis of EPS System,” KSAE Spring Conference Proceedings, pp.340-344, 2016.
5) ISO 26262-1:2018, Road Vehicles Functional Safety Part 1: Vocabulary, 2nd Edn., 2018.
6) A. Schnellbach, Fail-Operational Automotive Systems, Ph. D. Dissertation, Graz University of Technology, 2016.
7) ISO 13849-1:2015 Safety of Machinery - Safety Related Parts of Control Systems - Part 1: General Principles for Design, 2015.
8) ISO/DIS 26262-4:2016, Road Vehicles Functional Safety Part 4: Product Development at the System Level, Draft International Standard, 2016.
9) ISO/DIS 26262-5:2016, Road Vehicles Functional Safety Part 5: Product Development at the Hardware Level, Draft International Standard, 2016.
10) ISO/DIS 26262-6:2016, Road Vehicles Functional Safety Part 6: Product Development at the Software Level, Draft International Standard, 2016.
11) ISO 26262-6:2018, Road Vehicles Functional safety Part 6: Product Development at the Software Level, 2nd Edn., 2018.