THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2014 Oct.; 25(10), 1020～1027.

http://dx.doi.org/10.5515/KJKIEES.2014.25.10.1020
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

# 자동차 기능 안전성(ISO26262)에 관한 EMC 관리계획

# Management Plan on EMC for Functional Safety of the ISO26262

신 재 곤 · 정 연 춘* · 최 재 훈**

Jaekon Shin · Yeonchoon Chung* · Jaehoon Choi**

요 약

자동차 전자 제어 장치의 확대 보급에 따라 관련 장치의 오동작으로 인해 발생하는 자동차 사고 및 인명 손실을 최소화하기 위해 ISO 26262가 제정되어 완성 차량 제작사는 물론 부품 공급사에 적용되고 있다. 이 규격에서는 자동차 전체 시스템을 대상으로 개발 초기부터 생산/폐기에 이르기까지 전체 생명주기에서의 안전 요구사항을 적용토록 요구하고 있으며, 전자파 적합성 분야도 중요한 검토 항목으로 규정되어 있다. 따라서 자동차의 설계, 제조, 검증, 사용, 유지보수 기간 동안 각 단계별로 적용할 EFS(EMC for Functional Safety)에 대한 개발과 연구가 절실히 필요한 실정이다. 본 논문에서는 ISO26262의 적용에 따라 EFS를 어떻게 적용할 수 있는가를 검토하였다. 이러한 검토 결과를 적용하여 자동차의 기능 안전성 확보를 위해 EFS 평가를 강제 법규화하거나 또는 신차 안전도 평가(NCAP) 항목으로 확대 적용함으로써 제작사 스스로가 안전성 확보를 위한 절차를 수행하도록 규정할 필요가 있다.

Abstract

ISO 26262 is applied to vehicle and electrical/electronic component manufacturers for minimizing car accidents and life damage by the extended use of electronic control equipments and their malfunctions. In this standard, safety requirements are required to be applied from the early stage of development upto manufacture and disposal stages throughout the total lifecycle of the full vehicular system, and electromagnetic compatibility must be also managed as an important consideration factor. Therefore, it is nowadays very necessary to research and develop EFS(EMC for Functional Safety) to be applied in each stage of the design, manufacture, accreditation, use, maintenance stages of cars. In this paper, how EFS can be applied for the application of ISO 26262 is described. By the enforcement of this suggestions into the legal requirement or New Car Assessment Program(NCAP) test items, it is necessary that car manufacturer have to perform some procedures for ensuring car safety by themselves.

Key words: EFS, EMC, ISO26262, NCAP, Functional Safety

## Ⅰ. 서 론

최근 들어 종래의 자동차 기술에 IT 기능과 전자 제어 기능 등의 융합을 통하여 자동차의 결함이나 사고 예방, 회피 및 충돌 등 위험 상황으로부터 운전자 및 탑승자를 보호하여 교통사고 피해를 줄일 수 있는 시스템이 등장하고 있다. 또한, 전통적으로 자동차에 사용되던 기계 제어 방식 기술은 제어의 편리성과 부품 단가의 절감을 위

「이 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비 지원(14PTSI-C054118-06)으로 연구되었음.」

교통안전공단 자동차안전연구원(Korea Automobile Testing & Research Institute)
*서경대학교 전자공학과(Department of Electronics, Seokyeong University)
**한양대학교 융합전자공학부(Department of Electronic Engineering, Hanyang University)

· Manuscript received August 18, 2014 ; Revised August 27, 2014 ; Accepted August 29, 2014. (ID No. 20140818-08S)

· Corresponding Author: Jaehoon Choi (e-mail: choijh@hanyang.ac.kr)

하여 전자 제어 방식으로 변경되고 있다. 이에 따라 자동차의 전장 부품의 비중이 현재 20~25 % 정도에서 2015년에는 40 % 이상으로 증가될 것으로 전망되고 있다[1].

이러한 전자 제어 방식의 확대 적용에 따라 발생할 수 있는 문제점 중 하나는 전자파에 의한 성능 저하나 기능적 오류이다. 특히, 좁은 공간 내에 밀집하여 설치되는 자동차 전장 부품들은 설치 특성상 전자파 간섭에 더욱 취약하다. 이러한 전자파 간섭은 전자 제어 장치의 기능적 오류와 오작동을 유발하여 심각한 사고를 초래할 수 있으며, 운전자 및 탑승자는 물론, 보행자의 안전에 큰 위해 요소가 될 수 있다[2]. 이에 따라 IEC에서는 1998년에 전자 제어 장치의 안전성과 관련한 일반 규격으로서 IEC 61508 (Functional safety of electrical/ electronic/programmable electronic safety related system)을 제정하였으며, 여러 산업 분야에서는 이러한 IEC 61508 규격을 근간으로 각 산업에서 고유하게 다루어야 할 문제를 포함하여 여러 파생 규격들을 발행하여 적용하고 있다[3].

자동차 분야의 기능 안전에 관한 EMC 분야 연구는 영국의 IET에서 수년 동안 연구를 지속하였으며 그 연구를 바탕으로 유럽에서 많은 EMC 관련 연구 및 EMC 관리계획에 관한 연구를 진행하고 있다. 또한, 영국 및 유럽의 철도 분야에 이러한 EMC 관리계획에 관한 철차를 이용하여 전자파 안전성 확보 프로젝트가 진행 중에 있다[4]. 하지만 국내에서는 기능 안전에 관한 전자파 안전성 연구가 진행이 되고 있지 않는 실정이다. 자동차 산업 분야에서는 자동차의 기능적 안전에 대한 규격인 ISO 26262가 2011년 11월에 국제표준으로 공식 발행되었으며[5], 국내에서는 2012년 12월에 "자동차 기능안전을 위한 국가표준(KS R ISO 26262)"이 제정되었다. ISO 26262에서는 자동차 전체 시스템을 대상으로, 개발 초기부터 생산/폐기에 이르기까지 전체 생명주기에서의 안전 요구사항을 규정하고 있으며, 어느 단계에서 어떻게 EFS가 적용되어야 하는지에 대해서는 구체적으로 언급되어 있지 않다. 따라서 시스템 레벨 전자파 적합성에 생소한 엔지니어들이 자동차의 기능적 안전성에 대해 전자파 적합성을 어떻게 다루어야 하는지는 매우 어려운 일이다. 따라서 본 논문에서는 기능적 안전성과 관련된 규격인 IEC 61508과 ISO 26262에 대한 전반적인 동향에 대하여 살펴보고, EMC 관점에서 기능적 안전성을 다루는데 필요한 항목 도출을 위해 요구되는 위험 분석 및 관리 절차를 제안함으로써 자동차에 관한 전자파적인 안전성 확보를 위한 향후 정책 방향에 관한 지침을 제시하고자 한다.

## Ⅱ. 기능 안전성의 기본 개념

### 2-1 IEC61508의 개요

기능 안전성에 관한 국제 규격인 IEC 61508은 ISO/IEC 가이드 51에 근거하여 2000년에 제정되었으며, IEC 61508은 ISO 12100과 마찬가지로 기능 안전성에 기초한 규격이지만, 주로 플랜트나 시스템에서 위험도를 경감시키기 위해 사용되는 전기・전자 및 소프트웨어의 신뢰성을 규정하는 규격이다. 그림 1은 IEC 61508에서의 수명 주기 동안에 적용되는 기능적 안전 절차이다.

IEC61508에서의 수명 주기 동안의 기능적 안전은 ECU (equipment under control)와 그 환경(물리적/법적)을 충분히 이해하도록 하는 것이며, 각각의 수명 주기 동안에 기능적 안전 활동이 만족스럽게 실시될 수 있도록 하는 것이다. IEC 61508에서는 리스크 경감 목표에 대해 안전도 수준(SIL: Safety Integrity Level)이라고 하는 4단계의 수치

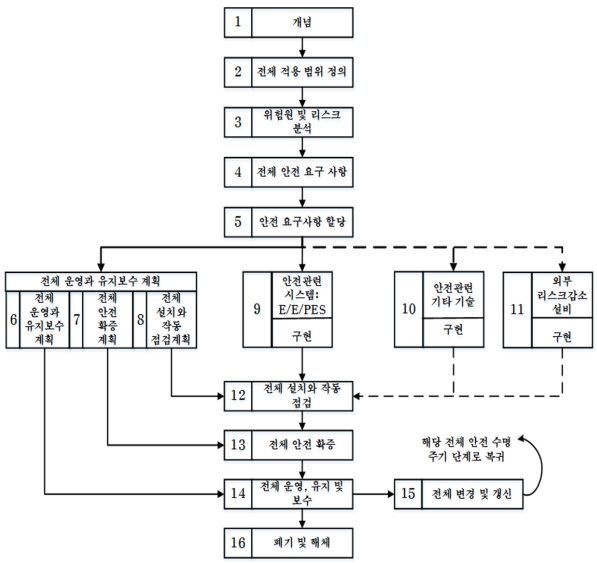


그림 1. IEC 61508에서의 수명주기 동안의 기능적 안전
Fig. 1. Functional safety of the life cycle for the IEC 61-508.

목표를 정하고 있다. 이러한 SIL의 단계는 고장이 발생하여 인명 사고로 이어지는 확률적 분포로 해당되는 리스크를 수용 가능한 리스크로 저감시키는 활동이 요구된다.

### 2-2 ISO26262의 개요

ISO 26262는 자동차 기능 안전성을 위하여 개발, 설계 단계부터 생산, 출고, 서비스 단계까지 발생될 수 있는 모든 안전 요구 사항을 분석하여 “자동차 안전 무결성 등급(ASIL)”을 산출하고, 이에 대한 대책에 대하여 기술한 지침서이다[6],[7]. 앞으로 차량 사고의 분쟁 시에 소비자가 아니라, 차량 제작사가 차량의 전체 생명주기에 걸쳐 최신의 안전기술을 이 규격에 따라 적용했음을 입증해야만 최소한의 면책을 받게 된다.

ISO 26262는 1개 이상의 전기 및 전자(E/E) 시스템을 포함하고, 자동차 총 중량이 3.5톤 이하인 승용차에 설치된 안전 관련 시스템에 적용되며, 또한 전기/전자 안전 관련 시스템의 작동 불량은 물론, 이들 시스템의 상호 작용으로 인한 발생 가능한 위험도를 규정하고 있다. 또한, ISO26262는 전기/전자 시스템의 기능 안전성 관련 규격이지만, 다른 기술에 기초한 안전 관련 시스템을 검토할 수 있는 체계를 제공한다.

ISO26262는 제품 개발 단계에 적용되는 참조 과정 모델인 V-모델에 기초한다. V-모델은 ISO 26262-3, -4, -5, -6, -7 사이의 상호 작용을 나타낸다. 제1부는 ISO 26262의 규격에 적용되는 용어, 정의, 그리고 약어를 설명하고 있다. 제2부는 기능 안전관리를 위한 요구사항을 언급하고 있으며, 기능 안전에 관련된 개발 활동을 계획, 조정, 그리고 추적하는 요건을 정의한다. 또한, 안전 문화와 같이 조직 차원에서 갖추어야 할 것에서부터 품목 개발, 양산 이후의 전체 수명 주기에 대한 기능적 안전에 대하여 기술하고 있다. 제3부의 개념 단계에서는 아이템 정의를 기반으로 위험원 분석 및 리스크 평가를 통해 자동차 안전 무결성 수준(ASIL: Automotive Safety Integrity Level) 수준을 판정하며, 안전 목표와 안전 메커니즘을 정의한다. 위험 분석, 리스크 평가 및 ASIL 결정은 불합리한 위험을 피하기 위해 아이템의 안전 목적을 규정하는 데 이용된다. 제4부는 제품 개발 단계 중 시스템 수준에서의 개발을 명시하고 있으며, 시스템 수준에서의 개발은 기본적으로 V 모델을 따른다. 제5부의 하드웨어 수준의 제품 개발에서는 시스템 설계명세를 기반으로 하여 아이템의 하드웨어 개발이 이루어지며, V 모델의 개념에 따라 개발, 통합, 검증 등에 대한 요구사항을 포함한다. 각 하드웨어 컴포넌트는 자신이 구현하는 하드웨어 안전성 요건으로부터 최고의 ASIL을 인계 받아야 한다. 또한, 안전 관련 하드웨어 컴포넌트에 발생한 고장의 비기능적 원인은 하드웨어 아키텍처 설계가 실행되는 동안 검토되어야 한다. 제6부의 소프트웨어 수준의 제품 개발에 대해서도 V 모델의 개념에 따라 개발, 통합, 검증 등에 대한 요구사항을 정의한다. 소프트웨어 개발 하위 단계와 지원 절차는 해당 요건과 각각의 ASIL을 준수하기 위한 적절한 방법을 정하는 것으로 시작된다. 이러한 방법은 지침과 도구의 지원을 받으며, 각 하위 단계와 지원 절차를 위해 결정, 계획된다. 제7부는 제품의 생산, 운영, 서비스, 그리고 폐기를 위한 요구사항을 포함하고 있다. 기능 안전성을 달성하기 위해서는 생산 과정이 진행되는 동안 개발 단계에서 정해진 아이템 또는 요소의 안전 관련 특성이 준수되어야 한다. 생산 계획 및 통제의 안전 관련 특성을 포괄하여 생산 공정이 진행되는 동안 기능 안전성이 달성되도록 보장하는 요건을 규정한다. 제8부는 안전 요구사항의 명세 및 경영, 형상 관리, 변경 관리, 검증, 문서화, 소프트웨어 도구 사용에 대한 신뢰, 사용증명 논거/주장 등에 대한 요구사항을 정의하고 있다. 제9부는 ASIL과 안전에 기반한 분석을 위한 요구사항 등을 포함한다. 위험도 저감을 위한 분해 기법과 위험 분해를 위한 요구 사항

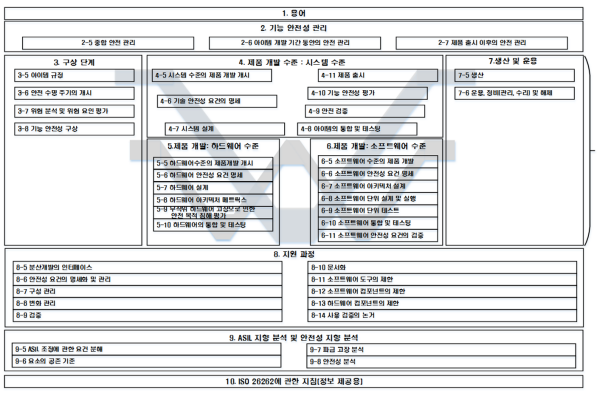


그림 2. IEC 26262 규격의 구조
Fig. 2. Structure of the ISO 26262 standard.

에 대한 내용을 포함한다. 제10부는 주요 개념, 안전 케이스, ASIL 분해 등 ISO26262의 이해에 도움이 되는 정보를 기술하고 있다.

그림 2는 ISO 26262의 전반적인 구조를 보여준다.

## Ⅲ. 기능 안전성을 위한 EMC 관리 절차

ISO26262는 자동차의 기능 안전성에 대한 중요한 요구사항을 제공하고 있지만, 위험 회피를 보장하기 위해 안전 관련 시스템에 대한 개발에서 적용되어야 하는 EMC는 명확히 정의가 되어 있지 않다[6]. 전자기적 방해 및 간섭은 CCF(Common Cause Failure)와 CF(Cascading Failure)을 야기시킬 수 있으며, 따라서 ISO26262 관점에서 각 단계별 전자파 안전성 절차를 정의하고, 자동차 및 부품에 대한 EMC 관련 요구사항에 관한 체계적인 System- Level EMC 분석 방법이 마련되어야 한다.

자동차를 구성하는 부품들이 적합한 지침에 따라 제조사의 인증을 받았음에도 불구하고, 특수한 사용 환경에 따라 기능상의 안전에 대한 성능이 부적합할 수 있다. EMC와 관련된 기능상의 안전을 제대로 통제하려면, 위험도(Risk)와 위해도(Hazard)를 평가할 필요가 있고, 다음과 같은 점을 고려해야 한다.

- 자동차의 전장 부품들이 어떤 EM 방해에 정기적으로나 부정기적으로 노출되어 있는가?
- EM 방해가 기기에 어떤 영향을 미칠 것으로 예상되는가?
- 영향을 받는 자동차 전장 부품에서 방출되는 EM 방해파가 여타 기기에 어떤 영향을 미칠 것인가?
- 위에 언급한 방해가 안전에 어떤 의미를 주는 것으로 예상되는가(위험도의 심각성과 위해도의 크기 및 요구되는 ASIL의 레벨은 어느 정도인가)?
- 위와 같은 점을 충분히 고려했고 바람직한 안전 레벨을 성취하는데 필요한 모든 조치를 취했다고 인정하려면 어느 정도의 검증이나 입증이 있어야 하는가?

이러한 위험도와 위해도 평가에서 드러난 각종 결정, 규격 활동 및 검증 사항은 안전에 관한 검증 자료로 간주되어야 하고, 결과를 문서로 작성해야 한다. 위와 같은 활동과 문서의 양과 질은 조직이나 프로젝트마다 현저히 다를 수 있다. 일반적으로 위험도와 위해도가 높을수록(즉, 안전 무결성 레벨이 높을수록), 높은 수준의 활동과 문서 작업이 요구된다. 조직에서 EMC와 안전을 관리하고 실행하는 책임자들 모두는 기능적 안전성을 위한 내용을 이해하고, 행동에 옮길 수 있는 능력을 가져야 하며, 일상적으로 업무에 적용할 필요가 있다. ISO26262에서 권고하는 ASIL의 수준을 전자파 안전성 관점에서 보면 자동차의 기능적 안전을 이해하는 핵심은 전기/전자 시스템이 전자기적 안전성을 확보하고, 전자파 안전성을 확보하기 위한 ASIL이 규정되어야 한다는 점이다. 안전 관련 시스템에 사용되는 전기/전자 장비의 안전 요건은 초기의 안전 수명 주기 동안 시스템의 위험과 리스크를 평가한 결과를 토대로 잘 규정되어야 한다. 표 1은 EMC 내성 분야의 단계에서 해결되어야 할 중요한 안전 요건으로서 단계별 내용을 설명하였다.

### 3-1 기능 안전을 위한 EMC 통제 지침

기능상의 안전을 위해 EMC를 통제하려면, 위험도와 위해도의 평가에 EM 환경과 방사성 방해 및 내성 능력을 반영해야 하고, 다음과 같은 점들을 고려되어야 한다.

- 자동차가 노출될 우려가 있는 EM 방해(간헐적인 것까지 포함)
- 방해가 자동차에 미치는 예측 가능한 영향
- 자동차에서 발생된 EM 방해가 자동차의 전장 부품이나 다른 시스템에 얼마나 영향을 미치는지 여부
- 방해가 안전에 미치는 예측 가능한 영향(위험도의 심각성과 위해도의 범위 및 적합한 안전 무결성의 레벨)
- 모든 사항이 완전히 고려되었고, 원하는 안전 레벨을 달성하기 위해 필요한 모든 조치가 취해졌다는 사실을 검증할 때 요구되는 확신

### 3-2 시스템 내부/간/외부 관리

자동차를 구성하는 전장 부품들의 증가에 따라 전장품 자체의 전자파 간섭에 의한 오동작(Inter), 자동차를 구성하는 다른 전장 부품의 전자파 방사에 따른 오동작(Intra), 자동차 외부의 고출력 무선 통신 신호에 의한 전자파 간섭(Extra)이 발생하여 자동차의 기능적 안전성에 영향을

표 1. EFS 확보를 위한 단계별 활동 내용
Table 1. Step-by-step activities for ensuring EFS.

| 단계 | 내 용 |
|---|---|
| 1 | 자동차를 운영하는 동안 겪게 될 EM 환경을 방해의 유형과 방해의 특성 면에서 미리 지정해야 한다. 표준은 특수한 EM 환경에서 중요한 방해 유형들을 소홀히 취급했을지 모르고, EM 환경도 예를 들어 할당 주파수의 변경이나 새로운 장비의 출현 또는 기존 제품/시스템/시설물의 변경으로 인해 항상 달라지기 쉽다. 표준을 안전 요건을 지정하는 근거로 활용해서는 안 된다는 점을 유념해야 한다. |
| 2 | 자동차 전장부품의 EMC 내성 능력은 관련된 EM 환경과 요구되는 안전 기능의 무결성과 기능을 모두 고려한 후 결정되어야 한다. 시스템의 안전 요건을 충분히 알고 해당 환경과 응용 분야에 대한 전문 지식과 경험을 가진 인력에 의해서 제반 기준이 신중하고 공개적으로 결정되어야 한다. |
| 3 | 내성 수준을 검증하는데 사용되는 검사 절차와 성능 기준이 지정되어야 한다. 일시적인 성능 저하나 기능의 상실조차 허용되지 않는 엄격한 분야도 있기 때문이다. |
| 4 | 서비스나 정비 보수 절차에도 안전이 요구되므로, 정비 보수나 개조 절차에서도 EMC를 고려해야 한다. |
| 5 | 소프트웨어의 변경과 업그레이드도 EMC와 기능상의 안전에 부정적인 영향을 미칠 수 있으므로, 이들은 마치 하드웨어를 정비할 때처럼 조심해서 다뤄야 한다. |
| 6 | 위와 같은 절차에서 EM 환경에 처한 자동차와 전장 부품의 내성에 대하여 다루었지만, 일부 장비들은 EM 방해파를 방사하여 주변의 EM 환경을 현저하게 악화시키고, 다른 장비의 기능을 저하시킬 수 있다는 사실을 간과해서는 안 된다. |

미칠 수 있다. 예를 들어 전기자동차의 모터를 구동하는 인버터의 경우 인버터는 내부 IGBT 회로에서 발생한 스위칭 노이즈로부터 전자파 장해에 대한 내성을 가져야 하며, 인버터에서 발생한 전자파가 자동차의 다른 장비(AM/FM 라디오, 무선 송수신기)에 간섭을 주지 않아야 하며, 자동차 외부의 송신소로부터 전달되는 EM 방해에 대한 전자파 간섭이 발생하지 않아야 한다.

이러한 분류를 위해서는 자동차의 전장 부품의 분류가 필요하며, 위험도의 등급 평가에 각 부품의 등급에 대한 분류가 요구된다. 자동차의 전장품은 아래 예시와 같이 안전도와 편리성을 바탕으로 표 2와 같이 분류할 수 있다.

표 2. 전장부품의 등급별 분류
Table 2. Rating classification of electrical component.

| 등급분류 | 설명 | 전장부품 |
|---|---|---|
| Class 3 | 자동차의 직접 제어 또는 안전과 관련된 전장 부품 | · ABS · Engine ECU<br>· EPS · ECS · IMS<br>· Auto light · A/bag<br>· Flasher unit<br>· Auto seat belt · TCS · Turn signal<br>· F/pump control relay · Intermittent wiper relay · Rear heated timer<br>· Auto(semi) transmission control unit<br>· Head & tail lamp control<br>· Automatic door lock/unlock release equipment |
| Class 2 | 품질을 향상시키는 부품과 운전자의 편리성을 제공하는 전장 부품 | · Tell-tales control<br>· Outside mirror<br>· Central door lock(ETACS)<br>· Cruise control · Trunk release<br>· FATC(SATC) · Leveling device<br>· Horn · License plate<br>· Electronic compass · Immobilizer<br>· Rear view mirror · Head up display |
| Class 1 | 운전자의 편리성을 제공하는 전장 부품 | · Audio system · CD changer<br>· Clock · Park & maker lamps<br>· Cluster · Trip odometer<br>· Navigation · A/con display<br>· Voice module · Cellular phone<br>· Fuel gauge · Chime module<br>· Keyless entry · A/V module |

각 등급의 장비들은 위험도 평가를 위하여 시스템 내부의 간섭, 다른 시스템과의 간섭, 외부 시스템에 대한 위험도 평가가 필요하다. 시스템의 분류에 따른 기능적 안전성 분류는 위험의 발견과 위험원을 판단할 수 있는 기초적인 자료가 될 수 있으며, 인터페이스 상의 전자파 간섭을 사전에 고려하여 판단할 수 있다. 자동차를 구성하는 전장 부품의 수가 많은 경우, 높은 안전성을 요구하는 부품에 한하여 적용하면 자동차의 안전성 향상에 도움이 될 것으로 판단된다. 그림 3에 도시된 절차는 EMC 관리 계획이라 할 수 있다. 이러한 관리 계획을 토대로 각 항목들에 관하여 검토를 진행한다.

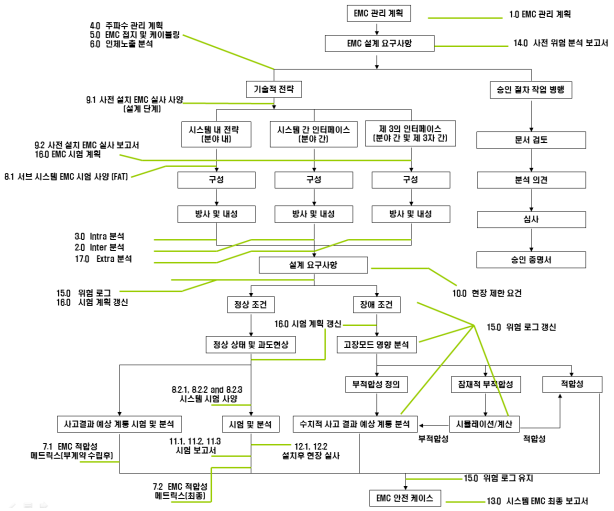


그림 3. ISO26262의 EMC 안전 관리계획
Fig. 3. EMC safety management plan of ISO26262.

그림 3은 ISO26262 및 IEC61508을 기반으로 EMC 규격의 적용 여부에 대한 검토 및 분석 방법의 일환으로 최초 신규 시스템에 대한 EMC 적용 항목 및 체계화된 필요 문서 목록과 분석을 위한 시스템적인 접근 방법이다. 이 관리계획을 통하여 자동차 시스템의 기능적 안전의 목표를 전자기적 관점에서 달성할 수 있다.

## Ⅳ. 전자파 안전성 확보를 위한 위해도 분석 기법

위해도 분석의 첫 단계는 시스템/장비의 성격과 허용 기준의 경계 및 의도하는 용도에 관한 조건을 정하는 것이다. 나중 단계의 혼선을 피하려면, 이 단계에서 명확한 결정이 요구된다. 위험한 상황의 식별은 자동차뿐만 아니라, 모든 안전 분야에서 가장 중요한 단계이다. 자동차가 정상 상태에서 작동했을 때 발생되는 내재된 위해도와 같은 지속적인 위해도와 하드웨어나 소프트웨어의 고장이나 오류에서 비롯된 위해도를 구분하는 것이 중요하다. 또한, 의도적으로 잘못 사용하여 위험을 발생시키는 것 또한 간과해서는 안 된다. 이러한 유형의 위험은 보다 정교한 식별 기법이 필요한 위험으로 간주되어야 하고, 별도의 해결 방안을 강구할 필요가 있다.

공식적이고 체계적인 절차를 활용하는 몇 가지의 정량적 위해도 식별 기법이 있다. 적절한 절차는 관련된 시스템/장비와 위험의 유형에 따라 선정된다. 식별 절차는 간단한 점검 목록을 이용하는 것부터 보다 정교한 분석까지 대상의 복잡성과 안전 요건에 따라 다양하다. 자동차의 고장이나 운전자의 실수 또는 잘못된 사용에 기인하는 위험은 다음과 같이 해야 한다.

### 4-1 위험 식별 기법

- 시스템의 수명주기 전반의 모든 단계(개념 단계부터 설계, 설치, 시운전, 사용, 정비 및 최종 해체 단계)에 걸쳐 위험을 자세히 식별하여야 한다.
- 정상 운전 상태의 운전자, 자동차 정비공, 세척 요원 등 누가 언제 위험에 노출될 수 있는지 식별하기 위해서 작업 시스템과 절차를 분석하여야 한다.
- 위험과 HAZOP(hazard and operability) 연구
- 고장모드와 효과 분석
- 업무 분석

### 4-2 위해도 분석

식별된 각 위험의 심각성과 확률이 폭넓게 분류되어 있다. 일반적으로 수학적 용어보다 서술형 용어가 사용되었다. 정량적 위험 분석 방법이 요구될 수 있는데, 이것이 규제 기관과 IEC와 ISO 등의 표준 단체들이 취하고 있는 추세다. ISO 26262의 위험도 분석은 ASIL의 등급을 결정한다. 다양한 영역의 위험을 모두 숫자로 표현할 수는 없지만, 아래의 내용은 위험의 심각성을 등급으로 매길 수 있는 대표적인 것들이다.

| | |
|---|---|
| ① 치명적 | EMC 문제로 인한 인명의 손상 |
| ② 심각함 | EMC 문제로 인한 중요한 시스템 또는 환경상의 손상 |
| ③ 경미함 | EMC 문제로 가벼운 시스템 또는 환경상의 손상 |
| ④ 무시 가능함 | 하찮은 상해를 입은 사람의 숫자나 환경상의 손상 |

앞서 언급한 것과 같이 위험은 완벽히 사라지거나 제거되지 않을 수 있다. 따라서 허용 가능한 수준의 위험에 대한 저감이 요구되는데, 허용 가능한 위험에 대한 내용을 IEC 61508의 5부에서는 그림 4와 같이 위험을 3가지 레벨로 나누어 구분한다.

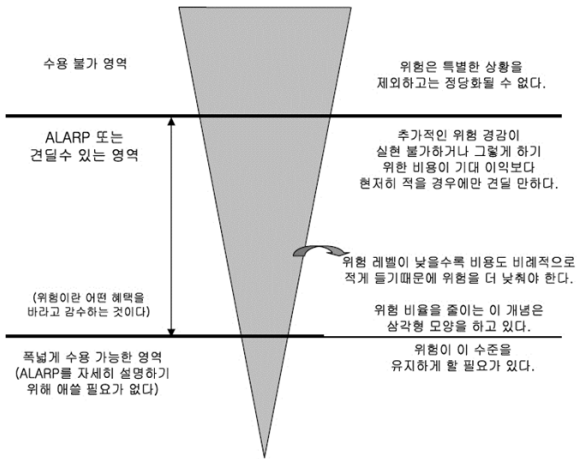


그림 4. ALARP(As Low As Reasonably Practicable) 레벨
Fig. 4. ALARP(As Low As Reasonably Practicable) Level.

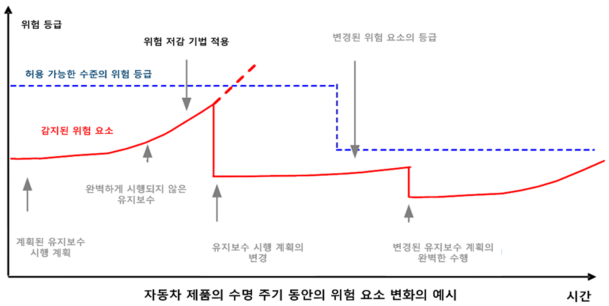


그림 5. 자동차 수명 주기 동안 위험 요소 변화
Fig. 5. Changes in risk factors for automobile life cycle.

수용 불가한 위험을 저감하기 위하여 허용 가능한 수준으로 관리하기 위한 방법이 요구된다. ALARP 영역 이하의 위험을 유지하기 위하여 계획된 유지 보수 계획이 수행되어야 한다. 그림 5에서 보는 것과 같이 자동차의 수명 주기 동안 유지보수가 계획대로 지켜지지 않은 경우, 별도의 위험 저감 기법이 필요하다.

감지된 위험 요소를 제품의 수명 주기 동안 허용 가능한 수준으로 관리를 해야 한다. 특히 유지 보수 기간 동안에 각 위험 요소들의 변화를 관리하는 지침과 허용 가능한 수준의 위험 등급 이내에 있음을 기록하여야 한다. 또한, 이러한 허용 가능한 위험 수준은 자동차 수명 주기에 따라 변화될 수 있음을 간과하지 않아야 한다.

## Ⅴ. 결 론

자동차에 있어서 기능 안전성의 확보는 운전자나 승객에 있어서 매우 중요하며, ISO26262의 절차에 따라 차량을 시스템 레벨에서 안전을 관리하고 위험요소를 저감시킬 필요가 있다. 예를 들어, 사회적인 이슈가 되고 있는 급발진 추정 사고가 발생하고 있음에도 불구하고, 현재는 사고 원인 규명의 책임이 소비자에게 있으나, 앞으로는 차량 제작사가 차량의 전체 생명주기에 걸쳐 최신의 안전기술을 적용했음을 입증해야만 최소한의 면책을 받게 된다. 따라서 차량 제작사는 위험에 대한 체계적인 관리와 저감 기법을 적용하여 기능 안전성을 확보해야만 하는 상황에 있다고 판단한다.

특히 통신, 전자기술의 비약적인 발전으로 향후 개발되고 있는 첨단 자동차나 자율 주행 자동차의 안전도 확보를 위하여 전자파 간섭으로 인한 위험을 체계적으로 관리할 필요가 있다. 전자파로 인한 위험으로부터 자동차의 기능 안전성 확보를 위하여 설계, 제조, 검증, 사용, 유지보수 기간 동안 각 단계별로 전자파 요구사항에 대한 개발과 연구가 필요하다. 위험원을 분석하는 단계에서 자동차가 운행되는 전자기 환경에 따른 요구사항이 개발되어야 하며, 설계 단계에서 안전 확보를 위한 EMC 요구사항과 검증에 따른 사항들을 개발할 필요가 있다. 위험의 분석과 관리 절차에 있어서 자동차와 전장 부품들이 전자파적인 위험으로 인하여 발생하는 기능적 오류를 목록화할 필요가 있다. 차량 및 전장 부품의 EMC 규격 인증이 전자파 간섭으로 인한 기능적 오류를 발생시키지 않음을 보증하는 최소한의 요구 사항일 뿐이지 기능적 안전을 보증하지는 않는다. 또한, 자동차 제작사에 의해 안전성 검사가 완료된 이후에도 자동차의 운행 및 유지, 개조 단계에서 발생할 수 있는 위험에 대하여 관리할 수 있는 절차가 필요하다.

마지막으로 정부에서는 첨단 전자 장치의 확대 적용에 따른 자동차 전기·전자 장치의 기능 안전 확보를 위하여 전자파 안전성 평가를 법규화 하거나 또는 신차 안전도 평가(NCAP) 항목으로 확대 적용하여 제조사 스스로가 안전성 확보를 위한 절차를 수행하도록 권장하는 등 자동차 인명 사고의 위험을 저감시킬 수 있도록 법제화의 노력이 필요하다고 판단된다.

자동차의 기능적 안전성의 확보로 인명 사고 위험을

단 1 %라도 저감할 수 있도록 정부와 제조사 간의 유기적인 협조를 통하여 자동차의 안전성을 확보할 수 있는 노력이 절실히 요구된다.

## References


[1] 전황수, "지능형 안전시스템 기술 동향", 정보통신산업진흥원 주간기술동향, 1558호, 2012.

[2] Keith Armstrong, "New guidance on EMC-related functional safety", *IEEE International Symposium*, *London*, pp 774-779, 2001.

[3] IEC 61508 first edition, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, 2005.

[4] IET, *Electromagnetic Compatibility for Functional Safety*, www.theiet.org, The Institution of Engineering and Technology, 2008.

[5] ISO 26262 part 1～10, *Road vehicles - Functional safety*, 2011.

[6] R. Kadom, J. J. Nelson, and W. Taylor, "Impact of functional safety on EMC : ISO26262", *SAE International*, Apr. 2013.

[7] L. Whalen, "Lessons from the front-runners on their ISO 26262 implementation efforts, practices and procedures", *Car T. Ins. Con. on ISO 26262*, Troy, MI, Jun. 2012.



신 재 곤

1987년 2월: 인하대학교 전자공학과 (공학사)
2001년 2월: 아주대학교 전자공학과 (공학석사)
2006년 2월: 한양대학교 전자통신전파공학과 박사수료
1986년～1993년: 현대자동차 제품개발연구소 근무
1993년～현재: 교통안전공단 자동차안전연구원 부연구위원
[주 관심분야] EMC, 자동차 전기/전자 시스템 평가, 안테나

정 연 춘

1984년 2월: 경북대학교 물리학과 (이학사)
1986년 2월: 경북대학교 물리학과 (이학석사)
1999년 8월: 충남대학교 전자공학과 (공학박사)
1985년 12월～2001년 5월: 한국표준과학연구원 전자기환경그룹 그룹장 (책임연구원)
2000년 3월～2001년 2월: Univ. of York, Visiting Academics
2001년 6월～2002년 2월: (주)익스팬전자 중앙연구소장
2002년 2월～현재: 서경대학교 전자공학과 교수
2005년 6월～2008년 11월: 한국전자진흥협회 EMC기술지원센터장(겸임)
[주 관심분야] EMI/EMC 측정 및 대책 기술, 전자파 재료

최 재 훈

1980년: 한양대학교 전자공학과 (공학사)
1986년: 미국 Ohio State University 전자공학과 (공학석사)
1989년: 미국 Ohio State University 전자공학과 (공학박사)
1989년～1991년: 미국 Arizona State University 연구교수
1991년～1995년: 한국통신위성사업단 연구팀장
1995년～현재: 한양대학교 융합전자공학부 교수
[주 관심분야] 안테나 및 마이크로파 회로 설계, EMC