신뢰성응용연구 신뢰성기술
제14권, 제1호, pp.81-91, 2014

기능안전을 위한 IEC 61508의 안전수명주기에 관한 연구

김성규*, 김용수**†
경기대학교 대학원 산업경영공학과* · 경기대학교 산업경영공학과*

A Study on a Safety Life Cycle of IEC 61508 for Functional Safety

Sung Kyu Kim*, Yong Soo Kim**†
*Dept. of Industrial and Management Engineering, Graduate School, Kyonggi University**
*Dept. of Industrial and Management Engineering, Kyonggi University***

<Abstract>
The IEC 61508 standard was established to specify the functional safety of E/E/PE safety-related systems. Safety life cycle to provide the framework and direction for the application of IEC 61508 is included in this standard. In this paper, we describe overviews, objects, scopes, requirements and activities of each phase in safety life cycle. In addition, we introduce safety integrity level(SIL) which is used for verifying the safety integrity requirements of E/E/PE system and perform a case study to estimate hardware SIL by FMEDA. The SIL is evaluated by two criteria. One of them is the architectural constraints which restrict the maximum SIL by combination of SFF and HFT. The other is the probability of failure which is classified into PFD and PFH based on frequency of demand and calculated by safe or dangerous failure rates.

Key Words: IEC 61508, Safety Integrity Level, Safety Life Cycle, Functional Safety.

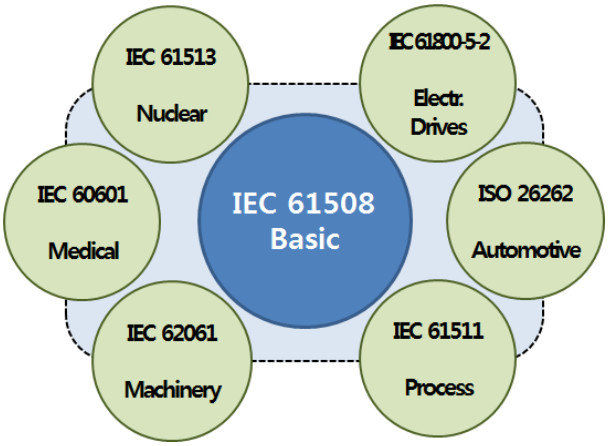
1. 서 론

기술의 발전으로 부품 및 시스템의 신뢰도는 지속적으로 발전되고 있으나, 발전소, 플랜트 등과 같은 각종 산업현장에서 발생되는 안전사고는 단일 결함만으로도 막대한 재산 및 인명피해를 야기한다. 이러한 사고를 방지하고자 산업현장에서는 안전제어시스템(Safety Instrumented System)을 설치하여 안전사고를 미연에 방지하는 기능을 수행하도록 하고 있다. 이러한 안전제어시스템은 만일 작동이 요구될 시 반드시 정상적인 기능을 수행해야 하므로 매우 높은 수준의 안전성과 신뢰도가 요구된다(Kim and Kim (2013)).

이러한 요구에 따라, 2000년 국제기구인 IEC (International Electrotechnical Commission)는 IEC 61508을 제정하여 전기/전자/프로그램 가능한 전자 시스템에 대한 기능안전을 명시하였으며 지난 2010년 개정되었다. IEC 61508은 기능안전의 대표적인 표준으로서, 전자기기, 원자력, 의료기기, 프로세스 산업, 자동차 등으로 구분되는 다양한 기능안전 표준의 중추적인 역할을 수행하고 있다(<그림 1> 참조).

IEC 61508(2010)에서는 안전수명주기를 통하여 시스템의 개념단계에서 구현, 양산, 관리, 폐기에 이르기까지의 전사적 과정을 명시하고 있다. 안전제어시스템은 개발부터 운영환경 및 다양한 상황에서 잠재된 위험원을 도출하고 위험원을 허용할 수 있는 수준까지 감소시키고자한다. 이처럼 위험원을 도출하고 감소시키기 위한 다양한 기법들이 개발 및 발전되고 있으며, 도출된 요구사항을 바탕으로 이에 적합한 안전제어시스템이 설계되었는가를 하드웨어 및 소프트웨어 나아가 시스템 수준에서의 평가가 이뤄지게 된다.

† 교신저자 : kimys@kgu.ac.kr
본 연구는 2013학년도 경기대학교 학술연구비(일반연구과제) 지원에 의하여 수행되었음
논문접수일 : 2014년 1월 18일 논문수정일 : 2014년 2월 28일 게재확정일 : 2014년 3월 14일



<그림 1> 기능안전을 명시한 산업분야별 국제 표준

이러한 안전무결성의 도출 및 평가의 기준으로 IEC 61508은 Safety Integrity Level(SIL)을 명시하고 있다. 이는 안전제어시스템의 안전무결성으로서, 위험원에 따라 요구되는 수준이 결정되고 이는 다시 정성적 및 정량적인 기법들을 통하여 평가된다. 이때의 SIL은 4등급으로 구분되고 높은 등급을 가질수록 엄격한 수준의 안전무결성이 요구된다.

IEC 61508은 요구된 SIL에 대한 적합여부를 검증함에 있어 두가지 측도를 명시하고 있다. 먼저, 구조적 측도는 시스템의 결함허용 수준인 HFT(Hardware Fault Tolerance)와 진단비율인 SFF(Safe Failure Fraction)에 고려함으로써 시스템의 구조적 강건성을 평가하게 된다. 다른 하나의 측도로는 시스템의 고장확률 측면에서 평가가 이뤄진다. 이 경우 시스템의 작동 요구 빈도에 따라 PFD(Probability of dangerous Failure on Demand)와 PFH(Frequency of dangerous Failures per Hour)로 구분되고 각각 다른 평가기준을 갖게 된다.

IEC 61508은 일반적인 표준이 갖는 특성상 내용의 이해 및 적용에 많은 어려움이 존재한다. 따라서, 본 연구에서는 IEC 61508에 대한 일반적인 구성 및 내용과 안전수명주기, 그리고 SIL의 평가 기준에 대하여 소개하고 안전수명주기의 각 단계별 목적 및 요구사항을 살펴보고자 한다. 또한, 안전수명주기의 한 단계인 하드웨어 SIL 검증을 위하여 가스탐지기를 대상으로 사례연구를 실시하였다.

2. 문헌연구

IEC 61508(2010)은 안전기능을 수행하는 전기/전자/프로그램 가능한 전자 시스템을 위한 안전수명주기를 제안하고 각 단계에 따른 활동에 대한 일반적인 접근방법을 제안하고 있다. 또한, SIL을 통하여 전기/전자/프로그램 가능한 전자 시스템의 기능안전에 대한 평가를 수행할 수 있도록 제시하고 있으며, 다양한 장치산업을 위한 기능안전의 중추적인 위치에 있다.

SIL을 요구하는 모든 안전제어시스템은 먼저 위험원 분석을 통하여 안전 요구사항이 결정되어야 한다. 따라서, 다양한 위험원 분석 기법을 활용한 안전제어시스템의 안전 요구사항 도출에 관한 다수의 연구가 수행되었다. 김정환 외 (2011)는 사고의 위험이 높은 화학공장에 리스크를 감소시키기 위하여 Hazard and Operability(HAZOP)와 Layer of Protection Analysis (LOPA)를 단계적으로 적용함으로써, 최악의 시나리오 도출 및 위험도를 정량적으로 산출하여 수용할 수 있는 목표 SIL을 결정하는 연구를 수행하였다. Labovský et al. (2007)은 화학 플랜트 고장을 대상으로 HAZOP을 바탕으로한 새로운 방법론을 제안 및 적용하는 사례연구를 실시하였다. 김기영 외 (2010)는 IEC 61508에서 구분하는 작동모드에 따라 개별적으로 정량적인 평가 플로우차트 및 정량적인 평가가 어려운 대상에 대한 정성적 평가 플로우차트를 제안하였으며, 화학플랜트를 대상으로 사례연구를 실시하였다. 또한, Summers (1998)은 이러한 안전 요구사항인 목표 SIL을 결정하기 위한 6가지 기법에 관한 개요 및 방법론을 정리하였다. 그밖에 이익성 (2010)은 위험원 분석 기법 가운데 하나인 As Low As Reasonably Possible (ALARP)을 활용하여 수용할 수 있는 수준으로 리스크를 감소시키는 사례연구를 수행함으로써, 안전경영시스템에 활용하고자 하는 연구를 수행하였다.

도출된 설계된 안전제어시스템은 안전 요구사항에서 요구하는 SIL의 달성여부에 대한 검증이 요구되며, 이에 대한 많은 기법 및 사례연구가 수행되었다. Goble and Brombacher (1999)은 정량적 SIL 평가 기법인 Failure Mode, Effect and Diagnostic Analysis (FMEDA)를 활용하여 고장률을 안전여부 및 진단여부

에 따라 구분하고 프로그램 가능한 전자시스템의 진단범위를 산출하는 연구를 수행하였다. FMEDA를 통하여 산출되는 인자들은 IEC 61508에 명시된 SIL 평가 기준 및 수식과 일치하여 적용에 유리한 기법으로 알려져 있다. 이러한 FMEDA를 관한 사례연구로는 Catelani et al. (2010)은 복합 시스템의 하드웨어 안전무결성 요구사항의 만족여부를 검증하기 위하여 FMEDA를 활용한 연구를 수행하였다. 김병철, 김영진 (2012)은 전극식 수위 측정시스템에 대하여 MIL-HDBK-217을 활용함으로써, 고장률을 추정하고 FMEDA를 적용함으로써, SIL을 평가하는 사례연구를 수행하였다. 또한, 신덕호 외 (2007)는 철도신호 제어기에 적용되는 워치독타이머에 대하여 Failure Mode and Effect Analysis(FMEA)와 Fault Tree Analysis(FTA)를 활용하여 고장률을 도출함으로써, 목표하는 SIL에 만족함을 검증하는 연구를 수행하였다. 마찬가지로 FTA 기법을 활용하여 415V Diesel Bus(진상화 외 (2002)) 및 열차방호장치와 건널목보안장치간의 인터페이스(신덕호 외 (2005))에 대한 SIL 평가 사례연구가 실시되었다. 또한, Kim and Kim (2013)은 양산 안전제어시스템에 대한 하드웨어 SIL을 결정하기 위하여 안전요구사항 도출에서부터 FMEDA 적용을 통한 검증에 이르는 평가 프로세스를 제안하였다.

IEC 61508에서 명시하는 안전수명주기는 안전제어시스템의 개발에서 양산, 폐기에 이르는 전사적 과정을 일괄적으로 나타내고 있다. 이와 관련하여 Lundteigen et al. (2009)은 IEC 61508에서 명시하는 안전수명주기와 기존에 RAMS 기법과 접합한 새로운 제품 개발 모델을 제안하였으며, 강신주, 이종우 (2013)는 IEC 61508에서 명시하는 안전수명주기에 따라 열차 제어장치용 PE시스템의 하드웨어 및 소프트웨어를 구현하기 위한 방법과 구조를 제시하는 연구를 수행하였다.

그밖에도 서순근 (2012)은 SIL 평가를 위해 IEC 61508에서 명시하는 n-out of-k 구조 별 수식에 대한 고찰 및 산출 값에 대한 정확도를 분석함으로써, IEC 61508에서 제공되는 수식들이 상대적으로 과대평가되고 있음을 증명하였다.

3. 기능안전을 위한 프로세스

3.1 IEC 61508의 구조

IEC 61508은 Part 0부터 Part 7까지 총 8개의 Part로로 구성되어 있으며, 각 Part의 내용은 아래 <표 1>과 같다. Part 0 '기능안전과 IEC 61508'은 기능안전에 대한 일반적인 개념을 정의하고 각 Part의 개요 및 구성에 관하여 명시되어 있다.

'Part 1 일반 요구사항'은 안전수명주기에 따른 목적, 적용범위, 입력 및 산출물을 명시함으로써, 기능안전을 위한 전체 프레임워크를 정의하고 있다. 'Part 2 전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 요구사항'은 안전제어시스템에 요구되는 안전 요구사항을 결정하기 위한 다양한 기법의 적용 및 SIL의 등급화에 관한 내용이 수록되어 있다. 'Part 3 소프트웨어 요구사항'은 안전제어시스템을 개발함에 있어 하드웨어가 아닌 소프트웨어에 적용되는 안전기능과 SIL에 대하여 명시되어 있다. 'Part 4 정의와 약어'는 IEC 61508에 사용되는 용어에 대한 정의 및 설명을 다루고 있다. 'Part 5 안전무결성수준 결정 방법의 예'에서는 리스크와 안전무결성의 개념에 대한 설명과 함께 두 개념간의 관계를 명시하고 안전무결성을 결정할 수 있는 다양한 방법론들에 관하여 예시를 들어 소개되어 있다. 'Part 6 IEC 61508 Part 2와 Part 3의 적용 지침'에서는 Part 2와 Part 3 적용의 기능적 단계와 두 가지 작동모드하에서의 하드웨어 고장 확률 평가 기법, 진단 범위 및 안전 고장비율 계산 예, 그리고 소프트웨어 안전무결성에 관하여 명시되어 있다. 'Part 7 기법과 수단의 개요'는 Part 2 및 Part 3와 관련된 다양한 안전기법에 관한 설명을 제공함으로써, 하드웨어 우발 고장에 대한 제어, 시스템 고장의 회피, 소프트웨어 안전무결성 달성을 위한 기법 및 방법에 대하여 명시하고 있다. 이렇게 8개의 Part들은 상호보완적으로 구성되어 있어 안전제어시스템에 적용을 위해서는 표준의 전체 Part에 대한 이해가 요구된다.

<표 1> IEC 61508의 구성 Part

구분	내용
Part 0	기능안전성과 IEC 61508
Part 1	일반 요구사항
Part 2	전기/전자/프로그램 가능한 전자장치 안전관련 시스템의 요구사항
Part 3	소프트웨어 요구사항
Part 4	정의와 약어
Part 5	안전무결성수준 결정 방법의 예
Part 6	IEC 61508 Part 2와 Part 3의 적용 지침
Part 7	기법과 수단의 개요

3.2 IEC 61508의 안전수명주기

IEC 61508(2000)은 E/E/PE 안전관련 시스템에 필요한 안전무결성수준을 달성하기 위한 모든 활동을 체계적인 방법으로 다루기 위하여 <그림 2>와 같은 안전수명주기를 명시하고 있다. 이러한 안전수명주기는 1단계 개념에서부터 16단계 폐기 또는 해체에 이르는 안전관련 시스템의 수명주기를 전사적으로 나타내고 있으며, 각 단계별 요구사항에 따른 산출 정보는 문서화하여야 한다.

‘1단계 개념’에서는 Equipment Under Control(EUC)의 이해수준과 환경을 발전시켜 다른 안전수명주기 활동을 만족스럽게 수행할 수 있도록 하는 것이 목적이다. EUC와 EUC가 작동하는 물리적 및 법적 규제와 같은 환경들을 적용 대상으로 하며, 대상에 대한 완벽한 이해와 위험원에 대한 정의 및 관련 정보를 수집하여야 한다. 또한, 국가 또는 국제적 안전규정에 대한 정보를 수집하는 활동이 요구된다.

‘2단계 전체 적용범위 정의의 목적’은 EUC와 EUC 제어 시스템의 경계를 결정하고 3단계의 위험원 및 리스크 분석의 적용범위를 명시하는 것이다. 위험원 및 리스크 분석에 포함되어야 하는 물리적 장비 및 위험원과 연관된 세부 시스템, 고장 메커니즘 등을 고려하는 것이 요구된다.

‘3단계 위험원 및 리스크 분석’에서는 예측 가능한 모든 상황에서의 EUC와 EUC 제어 시스템의 위험원과 위해 사건을 도출하여야 한다. 도출된 사건별로 그에 따른 영향을 정의하고 해당 리스크 수준을 결정하여야 한다.

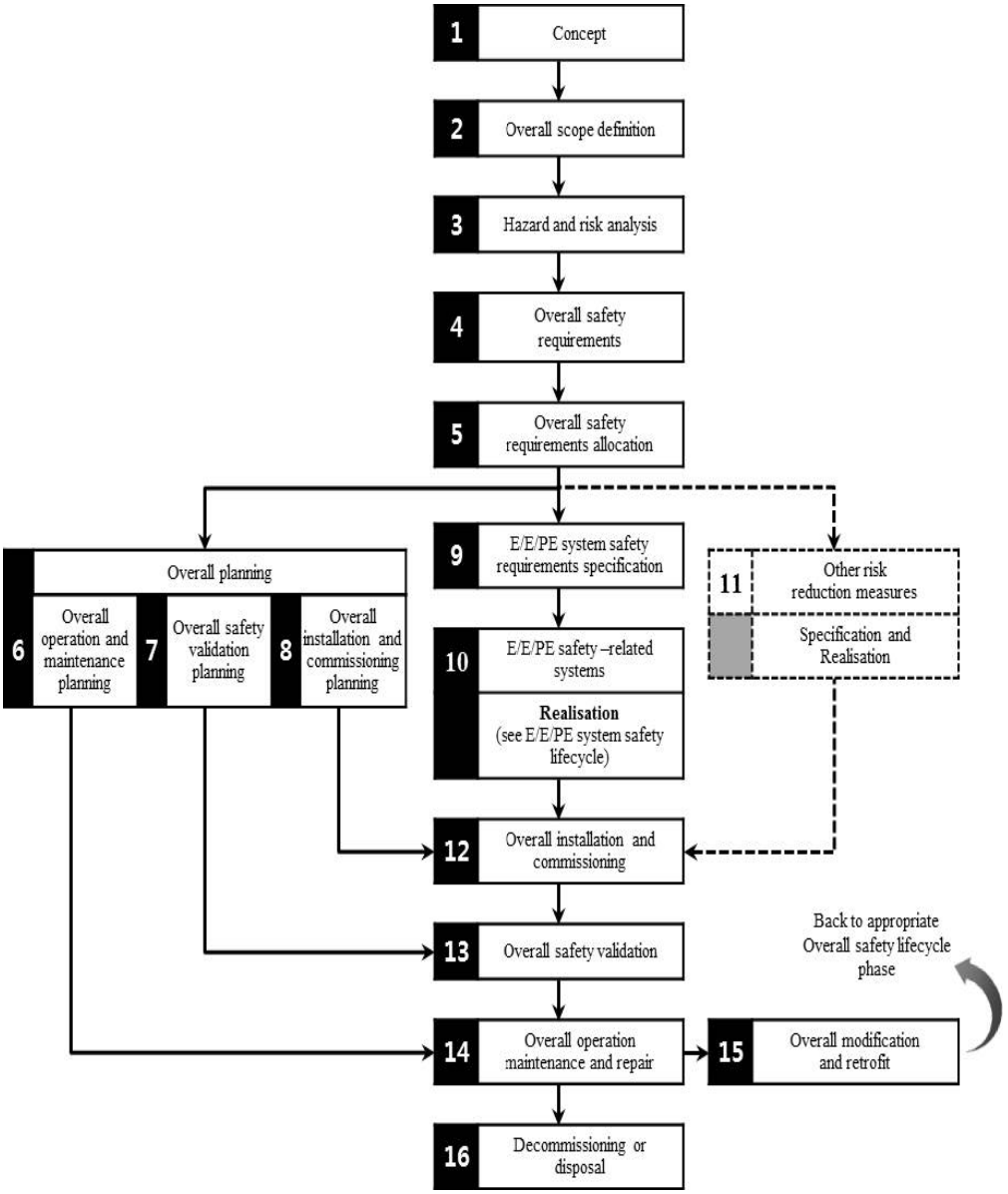
‘4단계 전체 안전 요구사항’은 3단계에서 결정된 위험원 및 리스크에 따라 이를 감소시킬 수 있는 방법이 결정하는 구체적인 안전 요구사항을 도출하는 단계이다. 3단계와 4단계에서는 위험원을 도출하고 감소시키기 위한 다양한 정량 및 정성적 위험도 분석 기법들이 적용될 수 있다. 대표적인 위험도 분석기법으로는 HAZOP, LOPA, ALRAP, Risk graph, Risk matrix등이 존재하며, Part 5에 자세한 설명 및 예가 소개되어 있다. 이러한 기법들은 단일 적용되기도 하나 보다 많은 잠재 위험원 도출을 위하여 두 기법 이상을 복합적으로 적용되기도 한다.

‘5단계 안전 요구사항 할당’은 4단계에서 도출된 전체 안전 요구사항을 바탕으로 안전기능에 각각의 SIL을 할당하는 단계이다. 이 경우 E/E/PE 시스템과 함께 외부 리스크 감소 방법을 고려하여 안전 요구사항을 할당함으로써, 기존의 리스크를 낮추고 목표하는 기능안전을 만족할 수 있다.

‘6단계 전체 운영과 유지보수 계획’은 운영 및 유지보수 기간 중 요구되는 기능이 안전하게 유지될 수 있도록 계획을 수립하는 단계이다. 이를 위하여 기존 기능안전을 위한 일반적인 활동뿐만 아니라 고장발생 및 돌발적인 상황에서 리스크를 감소시키기 위한 활동을 수립하여야 한다. 또한, 결함을 사전에 발견하기 위한 체계적인 유지보수 계획의 수립이 요구된다.

‘7단계 전체 안전 확증 계획’은 전체 안전 요구사항 할당의 결과를 바탕으로 E/E/PE 시스템의 확증을 위한 계획을 수립하는 단계이다. 이때, EUC의 작동모드 및 방법, 환경에 대한 명세가 포함되어야 하며, 하드웨어 및 소프트웨어의 평가를 위한 다양한 분석적 기법 중 활용 기법이 결정되어야 한다.

‘8단계 전체 설치 및 작동점검 계획’은 안전관련 E/E/PE 시스템의 설치 일정, 설치 엔지니어, 호환성 등을 고려하여 설치를 위한 계획과 작동점검에 대한 구체적인 계획을 수립하는 단계로서, 요구되는 기능안전을 달성하여야 한다.



<그림 2> IEC 61508의 안전수명주기(IEC 61508(2010))

‘9단계 E/E/PE 시스템 요구사항 명세서’는 E/E/PE 시스템의 구현에 앞서 도출된 안전 요구사항을 바탕으로 이를 달성하기 위하여 E/E/PE 시스템의 안전기능 및 안전무결성을 명세하여 개발자에게 제공하는 단계이다. 해당 명세서에는 목표하는 안전기능 및 안전무결성뿐만 아니라 보증기간 및 수명, 요구 및 제약사항, 보증시험을 위한 설비, 노출가능성이 있는 극한의 환경조건 등을 포함되어야 한다.

‘10단계 구현: E/E/PE 시스템’은 현 단계까지 도출된 E/E/PE 시스템의 안전 요구사항을 바탕으로 하드웨어 및 소프트웨어를 구현하는 단계이다. 하드웨어와 소프트웨어가 충족하여야 하는 요구사항 및 방법론에 대하여 각각 Part 2와 Part 3에 명시되어 있다. 10단계에서는 하드웨어와 소프트웨어에 대한 구현이 병렬적으로 진행되며, 소프트웨어의 경우 확증 단계 이전에 하드웨어와 통합한 안전 요구사항 검증이 요구된다. 하드웨어에 대한 안전 요구사항은 정량적인 평가 및 분석을 통하여 SIL을 결정하게 되며, 본 장의 3절에서 소개하였다. 반면, 소프트웨어의 경우 정량적인 평가보다는 체크리스트를 통한 요구 또는 권장 기법을 명

시하는 방식으로서 높은 SIL가 요구될수록 요구되는 기법의 수가 증가되게 된다.

‘11단계 외부 리스크 감소 방법: 명세 및 구현’은 안전제어시스템의 안전 요구사항과 목표 SIL에 부합하기 위하여 추가적인 안전관련 시스템을 구현하는 단계로서, 추가적인 안전관련 시스템은 안전 요구사항에 따른 리스크 감소를 위하여 유압, 공압과 같은 E/E/PE 시스템 또는 배수로, 방화벽 같은 물리적인 기술에 기초하여 고려되어야 한다. 단, 이러한 리스크 감소 방법에 대한 내용은 IEC 61508에서는 포함되어 있지 않다.

‘12단계 전체 설치 및 작동점검’은 8단계에서 수립된 계획에 따라 안전관련 E/E/PE 시스템의 실질적인 설치 및 작동점검을 수행하는 단계이다. 모든 단계와 마찬가지로 수행되는 모든 활동들은 반드시 기록되어야 한다.

‘13단계 전체 안전 확증’은 5단계에서 할당된 안전요구사항에 10단계에서 하드웨어 및 소프트웨어별 안전 확증을 마친 후 E/E/PE 시스템의 전체적인 안전 확증을 수행하여 전체 안전 요구사항 명세에 대한 만족여부를 판단하는 단계이다.

‘14단계 전체 운영 및 유지보수’는 앞서 수립된 운영계획에 따라 요구되는 기능안전을 만족시키기 위한 활동을 수행하는 단계이다. 이러한 활동을 통하여 안전관련 E/E/PE 시스템의 지속적인 정상운영을 유지하고 기록함으로써, 추후 보완사항을 도출하고 변경 및 갱신활동이 이뤄질 수 있도록 관리하는 단계이다.

‘15단계 전체 변경 및 갱신’은 만일 대상 안전관련 E/E/PE 시스템의 변경 및 추가적인 기능이 요구될 경우 이를 위한 활동 및 활동 후의 기능안전을 보장하는 단계이다. 변경 및 갱신이 요구될 경우 이에 대한 영향분석이 실시되어야 하며, 수정된 부분에 대한 위험도 분석 및 검증 절차를 수행하여야 한다.

‘16단계 폐기와 해체’는 대상 EUC의 제거에 따른 주변 EUC 및 기능안전에 미치는 영향을 측정하는 영향분석을 수행으로 진행된다. 폐기와 해체 작업으로 인한 영향과 작업 이후 잔여 EUC에 대하여 요구되는 안전기능이 수행여부를 평가하기 위하여 폐기 및 해체가 발생되는 하드웨어, 소프트웨어 및 시스템 수준의 단계의 안전수명주기로 되돌아가 순차적인 안전요구사항, 평가, 위험원 분석 등이 실시가 요구된다.

3.3 안전무결성수준

IEC 61508(2010)의 두가지 핵심개념은 안전상태를 유지하기 위하여 사고방지 및 리스크 감소를 수행하는 안전기능과 이러한 안전기능이 얼마만큼 만족스럽게 수행될 수 있는지에 대한 수준인 안전무결성이다. 본 절에서는 이 가운데 작동이 요구되는 시에 반드시 작동하여야 하는 안전기능의 안전무결성을 구분하는 측도인 SIL에 대한 소개와 평가 기준에 대하여 설명하고자 한다.

SIL은 총 4등급으로 구분되고 SIL 1보다 SIL 4가 훨씬 높은 수준의 안전무결성을 갖는다. IEC 61508은 SIL 평가 측도에 관하여 고장률에 기반한 수식을 제공하고 있다. 따라서, 수식을 적용하기 위해서는 표준에서 요구하는 다양한 고장률 산출이 우선되어야 한다. 이를 위하여 고장률 평가 방법인 FMEDA, FTA, Event Tree Analysis(ETA) 등과 같은 분석 기법들이 활용되고 있다.

SIL은 일반적으로 구조적인 측도와 확률적인 측도에 의하여 결정되게 되는데 먼저 구조적인 측도는 해당 안전제어시스템의 구조상 가질 수 있는 최대 SIL로서, Architectural Constraints이 된다. 즉, 확률적 측도에 따라 보다 높은 SIL로 평가되더라도 구조적 측도에 따른 SIL을 초과할 수 없게 된다.

구조적 측도는 HFT와 SFF에 의하여 결정되며, HFT는 E/E/PE 시스템의 구조적인 중복을 수치로 나타난 것이라 할 수 있다. 즉, 단일 결함으로 고장이 발생하는 단일 구조의 경우 ‘0’으로 표시하고 이후 이중화, 삼중화에 따라 ‘1’, ‘2’로 나타낸다. SFF는 안전제어시스템이 갖는 전체 고장률을 안전여부 및 탐지여부에 따라 4가지 고장률로 구분하였을 때, 전체 고장률 대비 안전고장률 및 탐지가능한 위험고장률의 비율을 의미하며, 식 (1)과 같이 산출하게 된다. 이때, λ_S은 안전고장률의 합이며, λ_{DU}는 탐지불가능한 위험고장률의 합, λ_{DD}는 탐지가능한 위험고장률의 합을 의미한다.

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \quad (1)$$

구조적 측도를 결정함에 있어 모든 서브시스템 및 컴포넌트는 Type A 또는 Type B로 구분되어야 한다. 만일 대상의 구성 요소에 대한 높은 이해를 바탕으로 고장모드 및 고장영향에 대한 정의가 완전할 경우, 또한 충분히 신뢰할 수 있는 고장데이터를 확보할 수 있는 경우에는 Type A로 구분하게 된다. Type A로 구분되지 않은 대상은 자연스럽게 Type B로 구분되며, 구성품 가운데 Type B가 하나라도 포함되어 있을 경우에도 Type B로 구분되어 진다. HFT 및 SFF에 대한 정의하고 Type이 결정되면 <표 2>와 같이 Architectural Constraints인 구조적 최대 가능 SIL이 결정된다.

SIL을 결정하는 또 다른 측도인, 확률적 측도는 먼저 E/E/PE 시스템의 작동모드에 따라 구분된다. IEC 61508에서는 안전기능의 수행이 요구되는 빈도가 연간 1회 이하일 경우나 보증시험 빈도보다 2배 이상 낮은 경우 저요구(Low Demand) 작동모드로 구분하고 만일 이보다 높을 경우에는 고/연속요구(High/Continuous demand) 작동모드로 구분되어 각각 PFD 및 PFH로 평가 측도를 산출하게 된다. 본 절에서는 IEC 61508에서 명시하는 확률적 측도 산출 수식 가운데 E/E/PE 시스템이 단일구조, 1oo1일 경우의 수식을 소개하며, 해당 수식은 식 (2), (3), (4)와 같다. 여기서, t_{CE}는 등가 평균 정지시간을 의미하며, T_1은 보증시험주기, MRT는 평균 수리 시간, $MTTR$은 평균 복원 시간을 의미한다. <표 3>은 PFD와 PFH에 따른 SIL 판정기준에 대하여 명시되어 있다.

$$PFD_{1oo1} = (\lambda_{DU} + \lambda_{DD}) t_{CE} \quad (2)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}} \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}} MTTR \quad (3)$$

$$PFH_{1oo1} = \lambda_{DU} \quad (4)$$

4. 사례연구

본 장에서는 안전수명주기의 '10단계 구현: E/E/PE 시스템'에 명시된 하드웨어 SIL 평가 사례를 소개하고자 한다. 하드웨어 SIL 평가는 안전제어시스템의 안전요구사항에 대한 만족여부를 검증하는 단계로서, 본

<표 2> 하드웨어 구조적 측도에 따른 최대 허용 가능 SIL(IEC 61508(2010))

안전무결성 수준	하드웨어 결함 허용					
	type A			type B		
	0	1	2	0	1	2
< 60%	SIL 1	SIL 2	SIL 3	-	SIL 1	SIL 2
60% ~ 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% ~ 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

<표 3> 확률적 측도 PFD 및 PFH에 따른 SIL 결정(IEC 61508(2010))

안전무결성 수준	작동모드	
	저요구 작동모드 (PFD)	고요구 및 연속 작동모드 (PFH)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

연구에서는 FMEDA를 활용하여 검증을 실시하였다. 또한, 부품 고장률은 Telcordia SR-332(2011)을 활용하였으며, 작동환경을 고려한 고장률 보정을 위하여 Method I을 적용하였다.

사례연구 대상인 가스탐지기는 가스의 누설 위험이 있는 지역에 설치되어 상시, 지속적으로 가스를 탐지하기 위하여 독성가스를 생산 또는 사용하는 공장, 가스저장소 등 산업현장에서 발생되는 각종 가스를 탐지하여 사고를 미연에 방지하는 안전제어시스템이다.

가스탐지기는 총 10개의 서브시스템으로 구성되어 있으며, 각각의 서브시스템은 가스의 감지, 처리, 출력 등과 같은 기능을 수행한다. 각 서브시스템의 보안상의 이유로 각 F1~F10으로 명명하였다.

FMEDA를 실시하기 위한 선행 단계로서 FMEA를 실시하였으며 실무자와의 인터뷰를 통하여 가스탐지기의 부품별 고장모드 및 영향을 결정하였다. 또한, IEC 61508에서 명시하고 있는 안전 및 위험고장의 판정기준에 따라 각 고장의 안전여부 및 탐지여부를 결정하였다. 단, 탐지가능 고장의 경우 반드시 탐지방법이 정의함으로써, 진단범위를 결정하였다. 고장률 보정은 Method I에서 명시하는 온도, 전기적 스트레스, 품질, 환경인자를 고려하여 보정된 부품 고장률을 산출하였으며, 보정된 고장률 산출 수식은 식 (5)와 같다. 이때, λ_{SS}는 안정상태의 고장률, λ_G는 부품의 기본 고장률, π_Q는 품질인자, π_S는 전기적 스트레스인자, π_T는 온도인자, π_E는 환경인자를 의미한다. <표 4>는 부품별 고장률 보정 결과를 나타낸다. 또한, 각 고장모드에 대한 고장분포를 결정하기 위하여 FMD-97(1997)을 활용하였다.

$$\lambda_{SS} = \lambda_G \pi_Q \pi_S \pi_T \pi_E \quad (5)$$

보정된 부품 고장률을 바탕으로 SIL을 평가하기 위하여 3.3절에서 명시된 기준을 적용하였다. 각 서브시스템들은 모두 Type B에 해당하였으며 단일 구조로 구성되어 있으므로 HFT는 '0'이 된다.

<표 4> 작동환경을 고려한 부품별 보정된 부품고장률의 산출

No.	부품명	Curve m	p1	πs	πT	πQ	πE	λG	λSS
1	THERMISTOR SENSOR	-	-	1.00	4.40	1.00	1.50	5.10	33.66
2	CHIP RESISTOR	1.3	0.0003	0.52	1.50	1.00	1.50	0.08	0.09
3	CHIP CERAMIC CAPACITOR	4.1	0.0016	0.13	1.10	1.00	1.50	0.10	0.02
4	LEAD CONNECTOR	-	-	1.00	4.40	1.00	1.50	11.00	72.60
5	FERRITE BEAD INDUCTOR	-	-	1.00	1.50	1.00	1.50	0.10	0.23
6	CHIP RESISTOR	1.3	0.0018	0.52	1.50	1.00	1.50	0.08	0.09
7	DIP SWITCH	1.3	0.0010	0.52	4.40	1.00	1.50	5.86	20.22
8	CHIP RESISTOR	1.3	0.0000	0.52	1.50	1.00	1.50	0.08	0.09
9	AXIAL RESISTOR	1.30	0.0000	0.52	1.50	1.00	1.50	0.08	0.09
10	CHIP RESISTOR	1.3	0.0000	0.52	1.50	1.00	1.50	0.08	0.09
11	CHIP CERAMIC CAPACITOR	4.1	0.0000	0.13	1.10	1.00	1.50	0.10	0.02
12	LINEAR IC	-	-	1.00	13.58	1.00	1.50	0.24	4.89
13	CHIP FET	2.4	0.0010	0.30	1.80	1.00	1.50	11.00	8.97
14	REGULATOR/LDO IC	-	-	1.00	13.37	1.00	1.50	0.31	6.22
15	CHIP CERAMIC CAPACITOR	4.1	0.0500	0.16	1.10	1.00	1.50	0.10	0.03
16	CHIP RESISTOR	1.3	0.0960	0.59	1.50	1.00	1.50	0.08	0.11
17	ADC/DAC IC	-	-	1.00	13.41	1.00	1.50	0.34	6.84
18	CHIP CERAMIC CAPACITOR	4.1	0.1000	0.19	1.10	1.00	1.50	0.10	0.03
19	CHIP RESISTOR	1.3	0.0000	0.52	1.50	1.00	1.50	0.08	0.09
20	FERRITE BEAD INDUCTOR	-	-	1.00	1.50	1.00	1.50	0.10	0.23

<표 5> 가스검출기의 하드웨어 SIL 평가를 위한 FMEDA의 일부

Sub system	Component	Failure distribution (%)	Failure mode	Failure effect	Failure rate (FIT)	SM	DE	Detec -tion method	DC	λ_{SD} (FIT)	λ_{SU} (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)
F1	THERMISTOR SENSOR	71.07	opened	Wrong temperature value sensing	23.92	1	0			0.00	23.92	0.00	0.00
		28.93	drift	Exceed the value of the temperature sensing accuracy	9.74	1	0			0.00	9.74	0.00	0.00
	CHIP RESISTOR	81.15	opened	wrong temperature value detection	0.08	1	0			0.00	0.08	0.00	0.00
		13.71	high value	wrong temperature value detection	0.01	1	0			0.00	0.01	0.00	0.00
		5.14	shorted	wrong temperature value detection	0.00	1	0			0.00	0.00	0.00	0.00
	CHIP CERAMIC CAPACITOR	37.62	opened	no effect on system	0.01	1	0			0.00	0.01	0.00	0.00
		62.38	shorted	wrong temperature value detection	0.01	1	0			0.00	0.01	0.00	0.00
F2	LEAD CONNECTOR	33.33	opened	no detection of gas	24.20	0	1	DM-01	99	0.00	0.00	23.96	0.24
		33.33	shorted	no detection of gas	24.20	0	1	DM-01	99	0.00	0.00	23.96	0.24
		33.33	power pin shorted	no detection of gas	24.20	0	1	DM-01	99	0.00	0.00	23.96	0.24
	FERRITE BEAD INDUCTOR	59.75	opened	no detection of gas	0.13	0	0			0.00	0.00	0.00	0.13
		40.25	shorted	no effect on system	0.09	1	0			0.00	0.09	0.00	0.00
	FERRITE BEAD INDUCTOR	59.75	opened	no detection of gas	0.13	0	0			0.00	0.00	0.00	0.13
		40.25	shorted	no effect on system	0.09	1	0			0.00	0.09	0.00	0.00
	FERRITE BEAD INDUCTOR	59.75	opened	no detection of gas	0.13	0	0			0.00	0.00	0.00	0.13
		40.25	shorted	no effect on system	0.09	1	0			0.00	0.09	0.00	0.00
	CHIP RESISTOR	81.15	opened	no reading sensor output signal	0.08	1	1	DM-01	99	0.08	0.00	0.00	0.00
		13.71	high value	no reading sensor output signal	0.01	1	1	DM-01	99	0.01	0.00	0.00	0.00
		5.14	shorted	no reading sensor output signal	0.00	1	1	DM-01	99	0.00	0.00	0.00	0.00
	DIP SWITCH	100.00	opened	no detection of gas	20.22	0	1	DM-02	99	0.00	0.00	20.01	0.20
	CHIP RESISTOR	81.15	opened	no detection of gas	0.08	0	1	DM-02	99	0.00	0.00	0.08	0.00
		13.71	high value	no detection of gas	0.01	0	1	DM-02	99	0.00	0.00	0.01	0.00
		5.14	shorted	no effect on system	0.00	1	0			0.00	0.00	0.00	0.00
	CHIP RESISTOR	81.15	opened	no detection of gas	0.08	0	0			0.00	0.00	0.00	0.08
		13.71	high value	no detection of gas	0.01	0	0			0.00	0.00	0.00	0.01
		5.14	shorted	no effect on system	0.00	1	0			0.00	0.00	0.00	0.00
	CHIP RESISTOR	81.15	opened	no detection of gas	0.08	0	0			0.00	0.00	0.00	0.08
		13.71	high value	no detection of gas	0.01	0	0			0.00	0.00	0.00	0.01
		5.14	shorted	no effect on system	0.00	1	0			0.00	0.00	0.00	0.00
	CHIP RESISTOR	81.15	opened	no detection of gas	0.08	0	1	DM-02	99	0.00	0.00	0.08	0.00
		13.71	high value	no detection of gas	0.00	0	1	DM-02	99	0.00	0.00	0.00	0.00
		5.14	shorted	no effect on system	0.00	1	0			0.00	0.00	0.00	0.00

FMEDA를 통하여 각 서브시스템의 탐지가능한 안전고장, 탐지불가한 안전고장, 탐지가능한 위험고장, 탐지불가한 위험고장을 도출하였으며, 이를 바탕으로 1oo1 구조 PFD 수식에 대입하였다. 이때, MRT과 $MTTR$은 모두 8시간으로, T_1은 1년으로 가정하였다. 산출된 PFD 값은 3.00×10^{-4}으로 <표 3>에 따라 SIL 3에 만족하였으나, F2, F3, F5, F9 서브시스템의 최대허용가능 SIL이 SIL 2를 만족하므로 시스템의 최대허용가능 SIL도 마찬가지로 SIL 2로 결정되게 된다. 따라서, 본 사례연구 대상인 가스탐지기의 하드웨어 SIL은 SIL 2를 만족하다고 할 수 있다. <표 5>와 <표 6>은 가스탐지기와 각 서브시스템의 FMEDA 시트 및 FMEDA 결과를 나타내고 있다.

5. 결 론

기능안전의 국제적인 관심과 필요성에 의하여 제정된 IEC 61508은 국내외의 높은 관심 속에 나날이 적용분야를 넓혀가고 있다. 최근에는 자동차 관련 기능안전을 명시하는 표준이 제정됨에 따라 향후에도 지속적인 개정 및 타 분야로의 확장이 예상되고 있다. 그러나, 기능안전의 모표준이라 할 수 있는 IEC 61508은 판정 및 적용에 대한 설명이 다소 모호하여 이와 관련된 많은 연구들이 수행되고 있다. IEC 61508의 핵심이라 할 수 있는 위험도 분석 및 안전무결성의 판정 분야에서는 기존의 정성적 및 정량적 기법을 적용한 사례연구뿐만 아니라 새로운 기법을 제안하는 연구가 많이 수행되고 있다.

본 연구에서는 이러한 IEC 61508에 대한 이해를 돕고자 표준의 구성 및 안전수명주기에 대하여 설명하고자 하였다. 안전수명주기는 안전관련 E/E/PE 시스템의 전사적 수명주기에 관한 것으로 개념 단계에서 폐기 및 해체 단계에 이르기까지 단계적으로 설명하였으며, SIL의 개요와 판정 기준 및 수식을 함께 명시하였다. 또한, FMEDA를 적용하여 안전제어시스템인 가스탐지기의 하드웨어 SIL을 정량적으로 평가하는 사례연구를 실시하였다. 그 결과, 가스탐지기의 하드웨어 SIL은 확률적 측도에 따른 SIL은 SIL 3에 해당하였으나 구조적 측도에 따른 최대허용 SIL이 SIL 2로 결정되어 최종 SIL 2로 평가되었다.

IEC 61508의 안전수명주기는 아직 개발되지 않은 신규 안전제어시스템에 적용하는 것을 기본으로 하고 있다. 그러나 이미 개발이 완료되었거나 양산단계의

<표 6> 가스탐지기 및 각 서브시스템의 FMEDA 결과 요약

항목	SFF (%)	HFT	Architectural constraints	DC (%)	$\sum\lambda_S$ (FIT)	$\sum\lambda_D$ (FIT)	$\sum\lambda_{DD}$ (FIT)	$\sum\lambda_{DU}$ (FIT)
가스 탐지기	99.40	B, N=0	SIL 2	98.87	4607.15	5194.06	5135.12	58.94
F1	100.00	B, N=0	SIL 3	100.00	33.78	0.00	0.00	0.00
F2	98.27	B, N=0	SIL 2	98.17	6.77	116.82	114.67	2.14
F3	93.87	B, N=0	SIL 2	93.62	0.20	4.95	4.63	0.32
F4	99.06	B, N=0	SIL 3	99.00	93.84	1325.27	1311.98	13.29
F5	97.00	B, N=0	SIL 2	96.69	8.37	80.13	77.47	2.65
F6	99.13	B, N=0	SIL 3	98.77	3.17	7.57	7.47	0.09
F7	99.18	B, N=0	SIL 3	99.00	26.74	122.95	121.72	1.23
F8	99.95	B, N=0	SIL 3	99.00	248.59	12.86	12.74	0.13
F9	98.91	B, N=0	SIL 2	98.89	50.05	3503.89	3465.00	38.89
F10	100.00	B, N=0	SIL 3	99.00	4135.64	19.63	19.44	0.20

안전제어시스템의 SIL을 평가함에 있어 그 적용이 쉽지 않다. 이러한 경우 안전수명주기를 거슬러 해당 단계를 찾아 신규 안전제어시스템과 같은 절차를 진행하여야 한다. 따라서, 개발 완료된 안전제어시스템에 대하여 보다 원활히 안전수명주기를 적용할 수 있는 연구가 요구된다.

참고문헌

[1] 강신주, 이종우 (2013), IEC 61508에 의한 열차제어장치용 PES 구성에 관한 연구, 전기학회논문지, 62권, 8호, 1169-1176.

[2] 김기영 외 (2010), 플로우차트 기반 안전무결성수준 평가 절차, 신뢰성응용연구, 10권, 2호, 107-122.

[3] 김철, 김영진 (2012), FMEDA 기법을 적용한 SIL 등급 판정에 관한 사례연구, IE interface, 25권, 4호, 376-381.

[4] 김정환 외 (2011), SIL(Safety Integrity Level) 선택에 의한 리스크 감소에 관한 연구, 한국가스학회지, 15권, 5호, 57-62.

[5] 신덕호, 이재훈, 이기서 (2005), 자동열차방호장치와 건널목보안장치간의 인터페이스 안전요구사항에 관한 연구, 철도저널, 8권, 2호, 161-169.

[6] 신덕호 외 (2007), 철도신호 내장형제어기 안전성 향상을 위한 워치독타이머 설계 및 평가, 철도저널, 10권, 6호, 730-734.

[7] 이익성(2010), 리스크분석에 의한 철도물류 운영기관의 안전경영시스템에 관한 연구, 신뢰성응용연구, 10권, 1호, 73-91.

[8] 진상화 외 (2002), 신뢰도 분석에 근거한 SIS 평가 방법론 개발, 한국가스학회지, 6권, 1호, 66-73.

[9] Catelani, M., Ciani, L. and Luongo, V. (2010), The FMEDA approach to improve the safety assessment according to the IEC61508, Microelectronics Reliability 50, 1230-1235.

[10] FMD-97 (1997), Failure Mode/ Mechanism Distributions 1997.

[11] Goble, W.M. and Brombacher, A.C. (1999), Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems, Reliability Engineering & System Safety 66, 145-148.

[12] IEC 61508 (2010), Functional safety of electrical/ electronic/programmable electronic safety-related systems.

[13] Kim, S.K. and Kim, Y.S. (2013), An evaluation approach using a HARA and FMEDA for the hardware SIL, Journal of Loss Prevention in the Process Industries 26, 1212-1220.

[14] Labovský, J., Svandová, Z., Markos, J., and Jelemenský, L. (2007), Model-based HAZOP study of a real MTBE plant. Journal of Loss Prevention in the Process Industries 20, 230-237.

[15] Lundteigen, M.A., Rausand, M. and Utne, I.B. (2009), Integrating RAMS engineering and management with the safety life cycle of IEC 61508. Reliability Engineering & System Safety 94, 1894-1903.

[16] Summers, A.E. (1998), Techniques for assigning a target safety integrity level, ISA Transactions 37, 95-104.

[17] Telcordia SR-332 (2011), Reliability Prediction Procedure for Electronic Equipment.