KOSHA GUIDE
D - 69 - 2020

안전계장시스템(SIS)을 이용한 화학설비 안전성 향상에 관한 기술지침

2020. 12.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자: 전남대학교 정창복, 장희, 안전보건공단 권현길

○ 제 · 개정 경과

- 2020년 10월 화학안전분야 제정위원회 심의(제정)

○ 관련 규격 및 자료

- ISA S84.01, “Application of Safety Instrumented Systems for the Process Industries”, 1996
- IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”, 2010
- IEC 61511 “Functional safety — Safety instrumented systems for the process industry sector”, 2016

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www.kosha.or.kr)의 안전보건기술지침 소관분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자: 2020년 12월
제 정 자: 한국산업안전보건공단 이사장

KOSHA GUIDE
D - 69 - 2020

안전계장시스템(SIS)을 이용한 화학설비 안전성 향상에 관한 기술지침

1. 목적

이 지침은 반응기 등 유해위험이 큰 화학설비의 안전성을 향상하고자 안전계장시스템을 설치하는 경우에 관련설비의 신뢰도 확보 및 유지를 위하여 설치 전·후 단계에서 필요한 사항을 제시하는데 그 목적이 있다.

2. 적용범위

이 지침은 화학공정의 주요 단위공정 모든 설비에 대하여 안전계장시스템을 통하여 안전성을 확보하고자 하는 경우에 적용한다.

3. 정의

이 지침에서 사용되는 용어의 정의는 다음과 같다.

3.1 공통 용어

(가) “결함 (Fault)”이라 함은 요구대로 수행할 수 없게 만드는 내부 상태를 말한다.

(나) “결함배제 (Fault exclusion)”라 함은 고장모드의 가능성이 낮아 결함을 더 이상의 고려 대상에서 제외하는 것을 말한다.

(다) “결함허용 (Fault tolerance)”이라 함은 결함 또는 오류 존재 시 필요한 기능을 계속 수행하는 장치의 능력을 말한다.

(라) “결함회피 (Fault avoidance)”라 함은 SIS 안전수명주기의 모든 단계 중 결함의 도입을 피하기 위한 방법 또는 절차의 사용을 말한다.

(마) “고장 (Failure)”이라 함은 요구된 대로 수행하는 능력의 상실을 말한다.

(바) “고장모드 (Failure mode)”라 함은 고장이 발생하는 방식, 형태를 말한다.

(사) “공정 리스크 (Process risk)”라 함은 비정상적인 사건(BPCS 오작동 포함)으로 야기되는 공정 조건으로 인한 리스크를 말한다.

(아) “공정 안전시간 (Process safety time)”이라 함은 SIF가 수행되지 않을 때 공정 또는 BPCS에서 위험사건을 야기할 가능성이 있는 고장 발생 시점과 위험사건 발생 시점 간의 시간 간격을 말한다.

(자) “리스크 (Risk)”라 함은 위해 발생의 확률과 위해 심각도의 조합을 말한다.

(차) “방호계층 (Protection layer)”이라 함은 제어, 예방(Prevention) 또는 완화(Mitigation)를 통해 리스크를 감축하는 독립적인 메커니즘을 말한다.

(카) “안전 (Safety)”이라 함은 허용될 수 없는 위험(Risk)로 부터 벗어난 것(Freedom) 것을 말한다.

(타) “안전기능 (Safety function)”이라 함은 특정 위험사건에 관하여 공정의 안전상태를 달성 또는 유지하기 위하여 하나 이상의 방호계층에 의해 구현되는 기능을 말한다.

(파) “안전매뉴얼 (Safety manual)”이라 함은 SIS 장치, 서브시스템 또는 시스템을 안전하게 적용할 수 있는 방법을 정의한 매뉴얼을 말한다.

(하) “안전상태 (Safe state)”라 함은 안전이 달성되었을 때의 공정 상태를 말한다.

(거) “완화 (Mitigation)”라 함은 위험사건의 영향을 감축하기 위한 행위를 말한다.

(너) “위해 (Harm)”라 함은 사람의 부상이나 건강 손상, 재산 피해나 환경 피해를 말한다.

(더) “위험사건 (Hazardous event)”이라 함은 위해를 야기할 수 있는 사건을 말한다.

(러) “유해위험요인 (Hazard)”이라 함은 위해의 잠재적 원천을 말한다.

(머) “인적 오류 (Human error)”라 함은 의도하지 않은 부적절한 결과를 초래하는 사람의 행위 또는 의도적으로 행위를 하지 않아 발생하는 실수를 말한다.

(버) “진단 (Diagnostics)”이라 함은 결함을 찾기 위해 (공정안전시간에 비하여) 자주 행하는 자동 시험을 말한다.

(서) “허용가능 리스크 (Tolerable risk)”라 함은 현재의 사회적 가치 및 기준에 따라 허용 가능한 리스크 수준을 말한다.

3.2 안전계장시스템 및 운영관련 용어

(가) “감시기 (Watchdog)”라 함은 프로그램가능 전자장치(PE)의 운전을 감시하여 결함 검출 시 조치를 취하기 위한 진단 장치와 출력 장치의 조합을 말한다.

(나) “계장시스템 (Instrumented system)”이라 함은 센서, 논리해결기, 최종요소로 구성된 시스템을 말한다.

(다) “고정 프로그램언어 (Fixed program language, FPL)”라 함은 미리 정의되고 고정된 적은수의 파라미터 집합만을 사용자가 조정할 수 있는 언어로서 생산 공정 규격으로 이용 가능한 전용기능시스템을 말한다.

(라) “구성관리 (Configuration management)”라 함은 시스템의 요소의 변화를 제어하고 각 요소와 그 배치를 파악하고 수명주기 동안 시스템의 연속성과 변경 사항의 추적가능성을 유지하는 활동을 말한다.

(마) “기능안전 (Functional safety)”이라 함은 공정 및 그와 관련된 장비를 안전한 상태로 유지하거나 달성하기 위하여 필요한 활동을 수행하는 SIS 또는 기타 방호계층의 올바른 기능 작동에 해당하는 부분을 말한다.

(바) “기능안전감사 (Functional safety audit)”라 함은 기능안전 요건 특유의 절차가 계획된 순서를 따르고 있는지, 효과적으로 실행되는 지, 규정된 목적 달성에 적합한지 여부를 결정하기 위한 체계적이고 독립적인 조사를 말한다.

(사) “기능안전평가 (Functional safety assessment, FSA)”라 함은 하나 이상의 SIS 또는 다른 방호계층에 의해 달성되는 기능안전을 평가하기 위한 증거 기반의 조사를 말한다.

(아) “기본공정제어시스템 (Basic process control system, BPCS)”라 함은 공정, 그 연관 장치, 프로그램가능시스템, 운전자로부터의 입력신호에 대응하여 공정을 원하는 방식으로 운전되도록 만드는 출력신호를 발생시키지만 안전계장기능(SIF)은 수행하지 않는 시스템을 말한다.

(자) “내장소프트웨어 (Embedded software)”라 함은 제조자가 공급하는 시스템의 일부로서 최종 사용자가 프로그램 수정 목적으로 접근할 수 없는 소프트웨어를 말한다.

(차) “논리기능 (Logic function)”이라 함은 (입력기능이 제공하는) 입력 정보와 (출력기능에서 쓰이는) 출력 정보 간 변환을 수행하는 기능을 말한다.

(카) “논리해결기 (Logic solver)”라 함은 하나 이상의 논리기능을 수행하는 BPCS 또는 SIS의 한 부분을 말한다.

(타) “단계 (Phase)”라 함은 SIS 안전수명주기 내에서 IEC 61511 시리즈에 기술된 특정 활동이 발생하는 기간을 말한다.

(파) “보상대책 (Compensating measure)”이라 함은 공정 운전 또는 유지보수 기간 중의 SIS 성능 저하를 알고 있을 경우, 미리 계획하여 문서화된 리스크 관리법의 임시 적용을 말한다.

(하) “사전사용 (Prior use)”이라 함은 과거 비슷한 운전환경에서의 운전 경험에 의거하여 해당 장치가 SIS용으로 적합하고 필요한 기능 및 안전무결 요건을 충족한다고 하는 사용자의 문서화된 평가를 말한다.

(거) “센서 (Sensor)”라 함은 공정 조건을 측정 또는 검출하는 BPCS나 SIS의 일부분을 말한다.

(너) “소프트웨어 (Software)”라 함은 데이터처리 시스템의 운전과 관련된 프로그램, 절차, 데이터, 규칙 및 관련 문서를 말한다.

(더) “시스템 (System)”이라 함은 설계에 따라 상호 작용하는 요소의 세트로서 시스템의 요소는 서브시스템이라 불리는 또 다른 시스템이라 할 수 있다. 이는 제어하는 시스템 또는 제어되는 시스템일 수 있으며 하드웨어, 소프트웨어 및 사람의 상호 작용하는 집합을 말한다.

(러) “안전계장기능 (Safety instrumented function, SIF)”이라 함은 기능안전을 달성하는데 필요한 규정된 안전무결성 수준을 가지는 전기/전자/프로그램 가능 전자장치 기능으로서 안전계장시스템(SIS)에 의해 구현되는 안전기능을 말한다.

(머) “안전계장시스템 (Safety instrumented system, SIS)”이라 함은 하나 이상의 SIF를 구현하는 데 사용되는 계장시스템을 말한다.

(버) “안전구성 PE 논리해결기 (Safety configured PE logic solver)”라 함은 안전분야에서 사용할 목적으로 구성된 범용 산업등급 PE 논리해결기를 말한다.

(서) “안전요건명세서 (Safety requirements specification, SRS)”라 함은 SIF의 기능요건과 그에 관련된 안전무결성수준을 포함하는 명세서를 말한다.

(어) “영향분석 (Impact analysis)”이라 함은 기능, 구성요소의 변화가 시스템 또는

다른 시스템의 기능이나 성분에 미치는 효과를 결정하는 활동을 말한다.

(저) “완전가변성언어 (Full variability language, FVL)”라 함은 일반용 컴퓨터를 바탕으로 하는 시스템으로 컴퓨터 프로그래머가 이해할 수 있도록 설계되고 매우 다양한 함수 및 응용프로그램을 구현하는 능력을 제공하는 언어로서 컴퓨터전문가에 의한 특수한 응용에 적합하다.

(처) “우회 (Bypass)”라 함은 SIS 기능의 모두 또는 일부가 실행되지 않도록 막는 행위 또는 설비를 말한다.

(커) “운전자 인터페이스 (Operator interface)”라 함은 운전자와 SIS 간 정보 소통 수단을 말한다.

(터) “유지보수/엔지니어링 인터페이스 (Maintenance/engineering interface)”라 함은 적정한 SIS 유지보수 또는 변경을 위해 제공되는 하드웨어 및 소프트웨어를 말한다.

(퍼) “유틸리티 소프트웨어 (Utility software)”라 함은 응용프로그램의 개발, 유지보수 및 문서화를 위한 소프트웨어 도구를 말한다.

(허) “응용프로그램 (Application program, AP)”이라 함은 사용자 응용을 위한 특유의 프로그램으로서, 일반적으로 SIS 기능 요건 충족에 필요한 입력, 출력, 계산, 결정을 제어하는 논리 순서(Sequence), 허용(Permissives), 한계(Limits), 식(Expressions)을 담고 있는 프로그램을 말한다.

(고) “응용프로그램 수명주기 (Application program life-cycles)”라 함은 응용프로그램이 고안되어 영구적으로 폐기될 때까지의 기간 동안 발생하는 활동을 말한다.

(노) “입력기능 (Input function)”이라 함은 논리해결기에 정보를 제공하기 위하여 공정 및 관련 장치를 감시하는 기능을 말한다.

(도) “입증 (Validation)”이라 함은 점검 및 객관적 증거를 통해 해당시스템의 사용에 대한 요건이 충족되었음을 밝히는 것으로 계획, 개선사항을 실행한 후 실제 효과를 확인하는 것을 말한다.

(로) “제한가변성언어 (Limited variability language, LVL)”라 함은 사용자들이 자신의 특수한 요구사항으로 시스템을 조정할 수 있는 보다 유연성 있는 시스템으로 처리 능력이 제한된 상업용 및 산업용 프로그램가능 전자제어기를 위한 프로그래밍 언어를 말한다.

(모) “채널 (Channel)”이라 함은 지정된 기능을 독립적으로 수행하는 장치 또는 장치 그룹을 말한다.

(보) “최종요소 (Final element)”라 함은 안전한 상태를 달성 또는 유지하는 데 필요한 물리적 동작을 구현하는 계장시스템(BPCS 또는 SIS)의 일부분을 말한다.

(소) “출력기능 (Output function)”이라 함은 논리기능으로부터의 출력 정보에 따라 공정 및 관련 장치를 제어하는 기능을 말한다.

(오) “프로그램가능 전자시스템 (Programmable electronic system, PES)”이라 함은 하나 이상의 프로그램가능 전자장치(PE)를 기반으로 하는 제어, 보호 또는 감시 시스템으로서 전원 공급 장치, 센서 및 다른 입력 장치, 데이터 하이웨이 및 다른 통신 경로, 구동기 및 다른 출력 장치와 같은 장치를 포함하는 시스템을 말한다.

(조) “프로그램가능 전자장치 (Programmable electronics, PE)”라 함은 컴퓨터 기술에 기반 하여 하드웨어, 소프트웨어, 입출력 장치로 구성된 장치를 말한다.

(초) “현장장치 (Field device)”라 함은 공정에 직접 연결되거나 공정 인근에 위치한 SIS 또는 BPCS를 말한다.

(코) “확인 (Verification)”이라 함은 SIS 안전수명주기의 각 단계에서 특정 입력에 대한 특정 출력이 모든 측면에서 해당 단계의 목표 및 요건을 충족한다는 것을 분석 또는 시험의 활동으로 계획, 개선사항을 실행하기 전에 효과를 사전 평가, 증명하는 것을 말한다.

(토) “SIS 서브시스템 (SIS subsystem)”이라 함은 그 기능 상실로 인한 위험한 고장이 SIS의 위험한 고장으로 귀결되는 SIS의 독립적인 부분을 말한다.

(포) “SIS 안전수명주기 (SIS safety life-cycle)”라 함은 프로젝트의 개념 단계에서 시작하여 모든 SIF를 더 이상 사용할 수 없어 끝나는 시점까지의 기간 동안 SIF 구현에 관련된 필수 활동을 말한다.

3.3 안전무결성 산정 및 시스템 설계 관련 용어

(가) “가용도 (Availability)”라 함은 시스템(예: SIS, 압력방출시스템 등)이 작동 요구 시 지정된 기능을 수행할 수 있는 확률을 말한다.

(나) “검출 (Detected)”이라 함은 어떤 수단(예: 진단시험, 보증시험, 운전자 개입 검사)에 의해 밝혀진(revealed) 고장 또는 결함에 사용되는 수식어이다.

(다) “고 요구모드 (High demand mode)”라 함은 1년에 1회를 넘는 요구 시에만 공정을 지정된 안전한 상태로 전환하기 위해 SIF를 수행하는 운전모드를 말한다.

(라) “공통모드고장 (Common mode failures)”이라 함은 동일한 고장 모드를 보이는 다른 장치들의 동시 고장을 말한다.

(마) “공통원인고장 (Common cause failures, CCF)”이라 함은 단일 사건으로 발생하는 장치들의 동시 고장을 말한다.

(바) “다양성 (Diversity)”이라 함은 요구된 기능을 수행하는 다른 수단으로서 다른 물리적 방법이나 설계접근법 등을 말한다.

(사) “리스크감축인자 (Risk reduction factor, RRF)”라 함은 특정 위험요인에 대한 리스크를 허용가능 리스크로 줄이기 위해 필요한 감축 비율을 말한다.

(아) “목표고장척도 (Target failure measure)”라 함은 안전 무결성 요건에 대하여 달성하여야 하는 위험한 고장모드의 계획된 확률을 의미하며, 저 요구모드 운전의 경우 평균 요구 시 고장확률(PFDavg), 고 요구모드 또는 연속모드 운전의 경우 평균 위험한 고장 빈도(PFH)로 나타낸다.

(자) “무작위 하드웨어 고장 (Random hardware failure)”이라 함은 하드에어에서 하나 이상의 열화(degradation) 메커니즘에 따라 무작위적인 시간에 발생하는 고장을 말한다.

(차) “보증시험 (Proof test)”이라 함은 SIS 자체의 위험한 결함을 검출하기 위하여 주기적으로 수행하는 시험을 말하며, 필요 시 수리를 통해 시스템을 ‘새롭게(As new)’ 또는 새로운 상태와 가장 가까운 상태로 회복시킬 수 있다.

(카) “불검출 (Undetected)”이라 함은 진단시험, 보증시험, 운전자 조정을 통하여 밝혀지지 않은 고장 또는 결함에 사용되는 수식어이다.

(타) “시스템 고장 (Systematic failure)”이라 함은 이미 존재하는 결함과 관련되어 특정 조건에서 일관되게 발생하는 고장으로서, 설계, 제조 공정, 운전 절차, 문서화 또는 다른 관련 인자를 조정하여 결함을 제거해야만 막을 수 있는 고장을 말한다.

(파) “시스템 능력 (Systematic capability, SC)”이라 함은 장치가 안전매뉴얼에서 정한 지침에 맞춰 적용되었을 때 장치의 시스템 안전무결성이 지정된 안전기능에 대해 지정된 SIL 요건을 충족할 것이라는 신뢰의 척도를 말하며, SC1에서 SC4

까지의 4 단계로 표현한다.

(하) “시스템 안전무결성 (Systematic safety integrity)”이라 함은 SIS의 안전무결성 중 위험한 고장 모드에서 시스템 고장에 관련된 부분을 말한다.

(거) “아키텍처 (Architecture)”라 함은 시스템 내 하드웨어 및 소프트웨어의 특정 구성(configuration)을 말한다.

(너) “아키텍처 제약조건 (Architectural constraints, AC)”이라 함은 주장된 안전기능의 SIL을 달성하기 위해 필요한 아키텍처 면에서의 제약조건을 말하며, 최소한의 하드웨어 결함허용(HFT)과 같은 의미로 간주된다.

(더) “안전고장 (Safe failure)”이라 함은 안전관련 시스템을 위험하거나 기능마비 고장상태로 만들 잠재력을 가지지 않는 고장으로서 이미 지정된 안전 조치가 작동되는 고장을 말한다.

(러) “안전고장분률 (Safe failure fraction, SFF)”이라 함은 안전고장(λ_S)과 진단에 의해 검출 고장(λ_{Dd})이 전체 고장($\lambda_S + \lambda_{Dd} + \lambda_{Du}$)에서 차지하는 분율(($\lambda_S + \lambda_{Dd}$)/($\lambda_S + \lambda_{Dd} + \lambda_{Du}$))을 말한다.

(머) “안전무결성 (Safety integrity)”이라 함은 명시된 모든 조건하에서 요구되는 안전계장기능(SIF)을 만족스럽게 수행할 수 있는 확률(SIS 능력)을 말한다.

(버) “안전무결성수준 (Safety integrity level, SIL)”이라 함은 SIS에 의해 달성되는 안전 무결성 요건을 결정하기 위하여 SIF에 할당되는 4가지 수준(1등급에서 4등급 중 하나)을 말한다.

(서) “안전무결성요건 (Safety integrity requirements)”이라 함은 SIS에 의해 구현되는 SIF의 SIL을 확보하기 위하여 해당 SIS가 충족해야 할 IEC 61511 요건들의 집합을 말한다.

(어) “연속모드 (Continuous mode)”라 함은 정상운전의 일환으로 공정을 안전상태로 유지하도록 SIF를 수행하는 운전모드를 말한다.

(저) “요구시 위험한 고장 확률 (Probability of dangerous failure on demand, PFD)”이라 함은 공정으로부터의 요구 발생 시, 지정된 안전기능을 수행하지 못할 확률을 말한다.

(처) “위험한 고장 (Dangerous failure)”이라 함은 주어진 안전 동작을 방해하거나 작동하지 못하도록 하는 고장을 말한다.

(커) “저 요구모드 (Low demand mode)”라 함은 1년에 1회 이하의 요구 시에만 공정을 지정된 안전한 상태로 전환하기 위해 SIF를 수행하는 운전모드를 말한다.

(터) “종속적인 고장 (Dependent failure)”이라 함은 고장을 야기하는 개별 사건들의 무조건부 확률의 단순 곱으로 확률을 나타낼 수 없는 고장을 말한다.

(퍼) “중복성 (Redundancy)”이라 함은 요구된 기능을 수행하거나 정보를 표현하는 수단이 둘 이상 존재하는 것을 말한다.

(허) “진단범위 (Diagnostics coverage)”이라 함은 진단에 의해 검출되는 위험한 고장의 가능성(비율)을 말한다.

(고) “최대허용수리시간 (Maximum permitted repair time, MPRT)”이라 함은 결함이 검출된 후 수리에 허용되는 최대 시간을 말한다.

(노) “평균수리시간 (Mean repair time, MRT)”이라 함은 전체 수리시간의 평균값을 말한다.

(도) “평균 시간당 위험한 고장 빈도/시간당 고장확률 (Average frequency of a dangerous failure per hour/ Probability of failure per hour(PFH))”이라 함은 지정된 안전기능을 수행하지 못할 시간당 횟수의 평균값을 말한다.

(로) “평균 요구시 위험한 고장 확률 (Average probability of dangerous failure on demand, PFDavg)”이라 함은 공정으로부터의 요구가 있을 때 지정된 안전기능을 수행하지 못할 확률의 평균값을 말한다.

(모) “하드웨어 결함허용 (Hardware fault tolerance, HFT)”이라 함은 하드웨어의 결함 시에도 필요한 기능을 계속 수행하는 장치의 능력으로서, HFT N이란 최대 N개까지의 하드웨어 결함을 허용함을 말한다.

(보) “하드웨어 안전무결성 (Hardware safety integrity)”이라 함은 SIS의 안전무결성 중 위험한 고장모드에서 무작위 하드웨어 고장과 관련된 부분을 말한다.

3.4 기타 이 지침에서 사용하는 용어의 정의는 특별한 규정이 있는 경우를 제외하고는 「산업안전보건법」, 같은 법 시행령, 같은 법 시행규칙 및 「산업안전보건기준에 관한 규칙」 및 관련고시에서 정의하는 바에 의한다.

4. 안전계장시스템(SIS)의 안전수명주기

4.1 SIS 안전수명주기 단계 및 개요

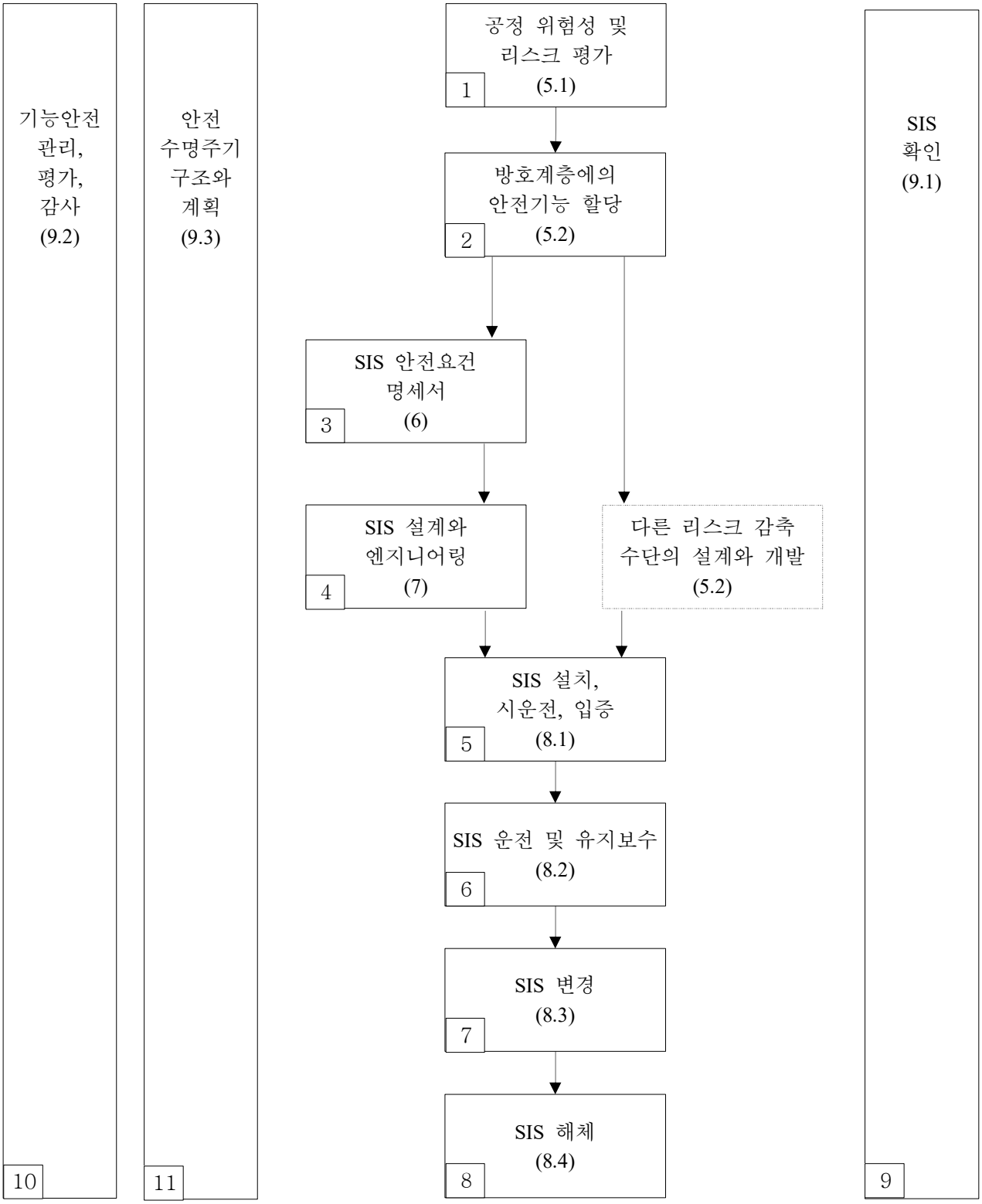
(1) [그림 1]은 공정 프로젝트의 진행 과정에서 SIS와 관련된 다양한 활동을 단계적으로 구분한 작업흐름도이다(각 박스 하단 왼쪽의 작은 박스는 안전수명주기의 단계(phase) 번호를, 괄호는 이 단계와 관련된 이 지침의 섹션 번호를 각각 담고 있음).

(2) 단계 1~8은 프로젝트의 진행 순서에 따른 활동을 나타내고, 단계 9~11은 모든 주기에 걸쳐 지속적으로 수행해야 하는 활동을 나타낸다.

(3) <표 1>은 각 단계 별 활동의 목적, 입력 및 출력을 개괄적으로 나타내었다.

4.2 SIS 응용프로그램 안전수명주기 단계 및 개요

(1) [그림 2]는 SIS에서 구현되는 응용프로그램(AP)과 관련된 다양한 활동을 단계적으로 구분한 응용프로그램 안전수명주기(점선으로 그린 박스 내)와 아울러 SIS 안전수명주기의 다른 활동과의 관계를 보이고 있다(각 박스 왼쪽의 작은 박스와 괄호는 이 단계와 관련된 이 지침의 섹션 번호를 담고 있음)



[그림 1] SIS 안전수명주기 단계

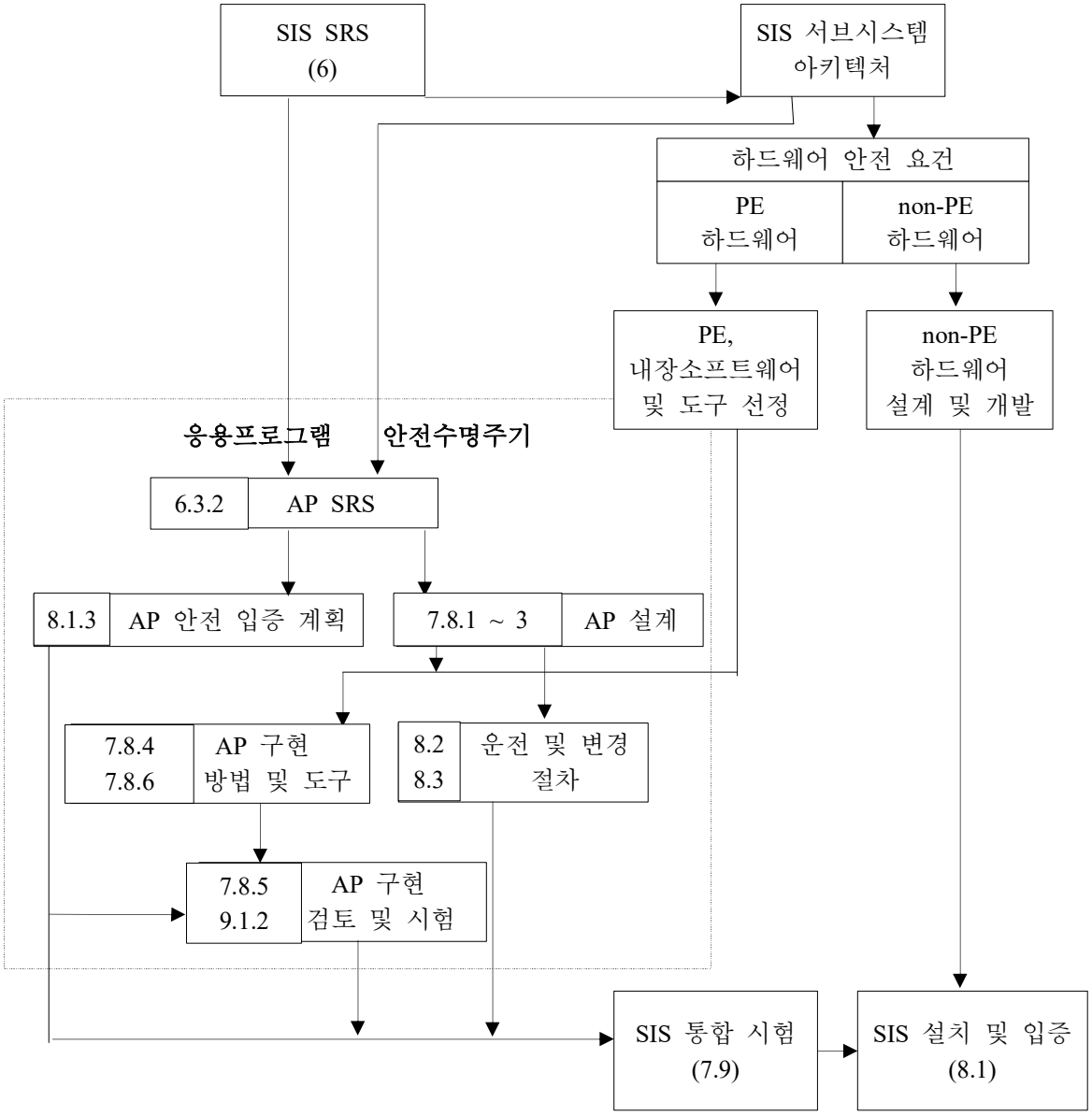
(2) <표 2>는 각 단계 별 활동의 목적, 입력 및 출력을 개괄적으로 나타내었다.

<표 1> SIS 안전수명주기 개요

안전수명주기 단계 또는 활동		목적	관련 섹션	입력	출력
박스 번호	제목				
1	H & RA (공정위험성 및 리스크 평가)	· 공정과 관련 장치의 위험요인과 위험사건 · 위험사건에 이르는 사건의 연속 · 위험사건과 관련된 공정 리스크 · 리스크 감축 요건 · 필요한 리스크 감축 달성을 위한 안전기능의 결정	5.1	· 공정 설계 · 배치도 · 인력배치 요건 · 안전 목표	· 위험요인 · 필요한 안전기능 · 관련 리스크 감축의 설명
2	방호계층에의 안전기능 할당	· 방호계층에 안전기능 할당 · 각 SIF에 관련 SIL 할당	5.2	필요한 SIF와 관련 안전무결성 요건에 관한 설명	안전요건 할당에 관한 설명
3	SIS 안전요건 명세서	필요한 안전기능을 달성하기 위해 각 SIS의 요건을 필요한 SIF와 그에 연관된 안전무결성으로 지정	6	안전요건 할당에 관한 설명	· SIS 안전요건 · 응용프로그램 안전요건
4	SIS 설계와 엔지니어링	SIF와 그 관련된 안전무결성 요건을 충족하도록 SIS 설계	7	· SIS 안전요건 · 응용프로그램 안전요건	· SIS 안전요건에 부합하는 SIS 하드웨어 및 응용프로그램 설계 · SIS 통합시험 계획
5	SIS 설치, 시운전, 입증	· SIS 통합 및 시험 · SIS가 필요한 SIF와 관련된 안전무결성으로 나타낸 안전요건의 모든 측면을 충족함을 입증	8.1	· SIS 설계 · SIS 통합시험 계획 · SIS 안전 입증 계획	· SIS 안전요건에 부합하여 완전히 기능하는 SIS · SIS 통합시험의 결과 · 설치, 시운전, 입증 활동의 결과

(<표 1> 계속)

안전수명주기 단계 또는 활동		목적	요건 조항	입력	출력
박스 번호	제목				
6	SIS 운전 및 유지보수	운전 및 유지보수 중 SIS의 기능안전이 유지되도록 보장	8.2	·SIS 안전요건 ·SIS 설계 ·SIS 운전 및 유지 보수계획	운전 및 유지보수 활동의 결과
7	SIS 변경	SIS의 수정, 기능 제고, 적응을 통해 필요한 SIL의 달성 및 유지를 보장	8.3	개정된 SIS 안전요건	SIS 변경의 결과
8	SIS 해체	·적정한 검토, 구역 구성 보장 ·적절한 SIF 유지 보장	8.4	·설치 상태의 안전 요건 ·공정 정보	SIS 서비스 해제
9	SIS 확인	주어진 단계의 출력의 시험 및 평가를 통해 해당 단계의 입력으로 제공된 제품과 표준에 견주어 정확성과 일관성이 있음을 보장	9.1	각 단계에서의 SIS 안전 계획	각 단계에서의 SIS 확인 결과
10	기능안전 관리, 평가, 감사	SIS에 의해 달성되는 기능안전을 조사하여 판단을 내림	9.2	·SIS FSA 계획 ·SIS 안전요건	SIS FSA 결과
11	안전수명주기 구조와 계획	수명주기 단계 달성 방식의 확립	9.3	해당사항 없음	안전 계획



[그림 2] 응용프로그램 안전수명주기와 SIS 안전수명주기와의 관계

<표 2> 응용프로그램(AP) 안전수명주기 개요

안전수명주기 단계 또는 활동		목적	관련 섹션	입력	출력
박스 번호	제목				
6.3.2	AP 안전 요건	· 요구된 SIF 구현에 필요한 각 SIS의 AP 안전 요건 지정 · SIS에 할당된 각 SIF를 위한 AP 요건 지정	6.3.2 7.3	· SIS 안전 요건 · 선정된 SIS의 안전매뉴얼 · SIS 아키텍처	· SIS AP SRS · 확인 정보
8.1.3	AP 안전 입증 계획	AP 입증을 위한 계획 개발	8.1.3	SIS AP 안전 요건	· SIS 안전 입증 계획 · 확인 정보
7.8.1 ~ 7.8.3	AP 개발	· 아키텍처 · 지정된 AP 안전 요건을 충족하는 AP 아키텍처 생성 · SIS의 하드웨어 아키텍처에 의해 부과된 AP 요건의 검토 및 평가 · AP 개발 절차 지정	7.8.1 7.8.2	· SIS AP 안전 요건 · SIS 하드웨어 아키텍처 설계 제약조건	· 아키텍처 설계의 설명 · AP 아키텍처 및 서브시스템 통합 시험 요건 · 확인 정보
	AP 설계	· AP 설계 개발 · AP 안전수명주기에 걸친 구성, 라이브러리, 간리, 모사 및 시험 도구의 적절한 집합 파악	7.8.3	· SIS AP 안전 요건 · 아키텍처 설계의 설명 · SIS 매뉴얼 · 선정된 SIS 논리해결기의 안전매뉴얼	· AP 설계 · 프로그래밍 중 사용할 절차 · 사용할 표준(제조자) 라이브러리 함수의 설명 · 확인 정보
7.8.4 7.8.6	AP 구현	· 응용 개발 및 응용 모듈 개발 · 지정된 응용 안전 요건을 충족하는 AP 구현 · 적절한 지원 도구와 프로그래밍 언어의 사용	7.8.4 7.8.3(4) 7.8.6	· 설계의 설명 · AP와 함께 사용할 선정된 논리해결기의 매뉴얼 및 프로시저 목록	· AP · AP 모사와 통합 시험 · 특수 목적 AP 안전 요건 · 확인 정보
7.8.5 9.1.2	AP 확인	· AP 안전 요건 달성의 확인 · 모든 SIS AP 간 상호작용이 적절하여 의도된 기능을 수행하고 의도하지 않은 기능은 수행하지 않음을 보임	7.8.5 9.1.2	· AP 모사와 통합 시험 요건 (구조기반시험) · AP 아키텍처 통합시험 요건	· AP 시험 결과 · 확인되고 시험된 AP 시스템 · 확인 정보
7.9	SIS 통합 시험	AP를 대상 논리해결기에 통합 (현장장치의 표본 집합 또는 모사기와의 상호작용 포함)	7.9	AP 및 논리해결기 통합 시험 요건	AP 및 논리해결기 통합 시험의 결과

5. SIS 안전수명주기 단계별 활동 요건

5.1 공정 위험성 및 리스크 평가(H&RA)

5.1.1 목적

안전한 공정을 보장하기 위한 안전기능의 필요성과 관련 목표고장척도의 확립을 위해 다음 사항을 결정하여야 한다.

(1) 공정 및 관련 장치의 위험요인과 위험사건

(2) 위험사건에 이르는 사건의 연속

(3) 위험사건과 관련된 공정리스크

(4) 리스크 감축 요건

(5) 필요한 리스크 감축을 달성하는 데 필요한 안전기능

(6) 어떤 안전기능이 SIF인지 여부

5.1.2 요건

(1) H&RA의 출력

물질, 공정 및 장치에 대해 H&RA를 수행하여 다음 결과를 출력하여야 한다.

(가) 파악된 각각의 위험사건과 그에 기여하는 요인들의 설명

(나) 각 위험사건의 가능성과 피해의 설명

(다) 공정 운전모드(예: 정상운전/운전개시/셧다운/유지보수 등)에 대한 검토

(라) 필요한 기능안전의 달성에 필요한 추가적인 리스크 감축의 결정

(마) 리스크 분석 과정에서의 가정(예: 방호계층에 대한 요구율, 개시원인의 평균 위험한 고장 빈도 등)과 운전상 제약조건 또는 운전자 개입에 대해 취한 크레딧의 상세한 설명

(바) SIF가 담당하는 각 안전기능의 파악

(2) BPCS 위험한 고장 빈도

개시원인으로서 BPCS의 평균 위험한 고장 빈도를 10^{-5}/hr 미만으로 가정하여서는

안된다.

(3) H&RA 기록

H&RA 출력 사항들 간의 관계가 분명하고 추적 가능하도록 기록하여야 한다.

(4) 보안 리스크 평가

SIS의 보안 취약성을 파악하기 위하여 보안 리스크 평가를 수행하여 다음 사항을 도출하여야 한다.

(가) 보안 리스크 평가에서 다루는 장치의 설명

(나) 취약성을 이용하여 보안 사건을 초래할 수 있는 파악된 위협의 설명

(다) 보안 사건의 잠재적 영향과 발생 가능성의 설명

(라) 설계/구현/시운전/운전/유지보수 등 다양한 단계의 검토

(마) 추가적인 리스크 감축 요건의 결정

(바) 위협을 감소 또는 제거하기 위한 대책의 설명 또는 그에 관한 정보 문헌

5.2 방호계층에 안전기능 할당

5.2.1 목적

(1) 안전기능을 방호계층에 할당

(2) 필요한 SIF 결정

(3) 각 SIF에 대해 관련 안전무결성요건 결정

5.2.2 할당 과정의 요건

(1) 할당 사항

(가) 리스크 감축에 필요한 안전기능을 특정 방호계층에 할당

(나) 리스크 감축 또는 평균 위험한 고장 빈도를 각 SIF에 할당

(2) 필요한 SIL 도출

SIF가 제공해야 할 요구시 위험한 고장 확률(PFD) 또는 평균 시간당 위험한 고장 빈도(PFH)를 감안하여 필요한 SIL을 도출하여야 한다.

(3) 요구모드 SIF의 SIL 지정

요구모드로 운전되는 각 SIF에 대하여 <표 3> 또는 <표 4>에 따라 필요한 SIL을 지정하여야 한다.

<표 3> 안전무결성요건: 평균 요구시 위험한 고장 확률(PFD_{avg})

요구모드 운전		
안전무결성수준(SIL)	PFD_{avg}	필요한 리스크 감축
4	$\geq 10^{-5}$ - $< 10^{-4}$	> 10,000 - ≤ 100,000
3	$\geq 10^{-4}$ - $< 10^{-3}$	> 1,000 - ≤ 10,000
2	$\geq 10^{-3}$ - $< 10^{-2}$	> 100 - ≤ 1,000
1	$\geq 10^{-2}$ - $< 10^{-1}$	> 10 - ≤ 100

(4) 연속모드 SIF의 SIL 지정

연속모드로 운전되는 각 SIF에 대하여 <표 4>에 따라 필요한 SIL을 지정하여야 한다.

<표 4> 안전무결성요건: 평균 시간당 위험한 고장 빈도(PFH)

요구모드 운전	
안전무결성수준(SIL)	PFH [1/hr]
4	$\geq 10^{-9}$ - $< 10^{-8}$
3	$\geq 10^{-8}$ - $< 10^{-7}$
2	$\geq 10^{-7}$ - $< 10^{-6}$
1	$\geq 10^{-6}$ - $< 10^{-5}$

(5) SIL4 회피를 위한 응용 재검토

(가) SIL 산정 과정에서 단일 SIS, 다중 SIS, 또는 SIS와 BPCS의 조합에 대한 요건으로 SIL4 도출 시, 해당 응용(예: 공정, 다른 방호계층)을 재검토하여 SIL4를 회피할 수 있는지 검토하여야 한다(SIL4 등급의 성능을 안전수명주기 내내 유지하기 어려움.

(나) 재검토 시 고려 사항

① 공정이나 용기, 배관 작업을 변경하여 위험요인을 그 원천에서 제거 또는 감축할 수 있는지 여부

② 계장에 기반을 두지 않는 추가적인 안전 관련 시스템 또는 다른 리스크 감축 수단을 도입할 수 있는지 여부

③ 결과의 심각도를 낮출(예: 위험물질의 양 축소) 수 있는지 여부

④ 위험사건의 발생 가능성을 낮출 수 있는지 여부

(6) 방호계층을 이용한 SIL4 달성

(가) 재검토 후에도 여전히 SIL4 필요 시 복수의 방호계층을 사용한 안전무결성요건 달성을 검토하여야 한다.

(나) 다중 방호계층의 요건

(다) 방호계층 간 독립성을 유지하거나 결여 시 평가를 통해 리스크 감축 요건에 비해 충분히 낮은 리스크임을 입증하여야 한다.

(라) 평가 시 고려 사항

① SIS 고장과 요구 간 공통원인

② SIS와 다른 방호계층 간 공통원인 고장

③ 공통된 운전/유지보수/검사/시험 활동 또는 보증시험 절차 및 시기에 의해 도입되는 종속성

(7) SIL4 구현 시의 추가적인 리스크 평가

(가) SIL4에 해당하는 리스크 감축을 구현하려면 정량적 방법을 사용하여 추가적인 리스크 평가를 수행하여야 한다.

(나) 이 평가에서 고려해야 할 사항

① SIS간 종속성과 공통원인 고장

② 위험사건의 가능성을 낮추는 다른 SIS 또는 리스크 감축수단

③ 고장 시 SIS에 대한 요구를 부과할 다른 방호계층

(8) 단일 SIS 내의 다중 SIF

위에 필요한 리스크 감축을 단일 SIS 내의 다중 SIF에 할당 시 전체 리스크 감축 요건을 충족하여야 한다.

(9) 할당 과정 결과의 기록

할당 과정의 결과를 기록하여 SIF를 공정의 기능적 요구 사항과 리스크 감축 요

건 면에서 설명하여야 한다.

5.2.3 방호계층으로서 BPCS의 요건

(1) BPCS 방호계층

BPCS는 [그림 3]에 보인 것처럼 방호계층으로 간주할 수 있다.

(2) 리스크 감축 한계

BPCS 방호계층에 의한 리스크 감축은 10 이하로 인정되어야 한다.

(3) 10을 넘는 리스크 감축에 대한 요건

BPCS 방호계층에 대해 10을 초과하는 리스크 감축을 인정하려면 IEC 61511 시리즈에 따라 BPCS를 설계하고 관리하여야 한다.

(4) BPCS 방호계층의 수

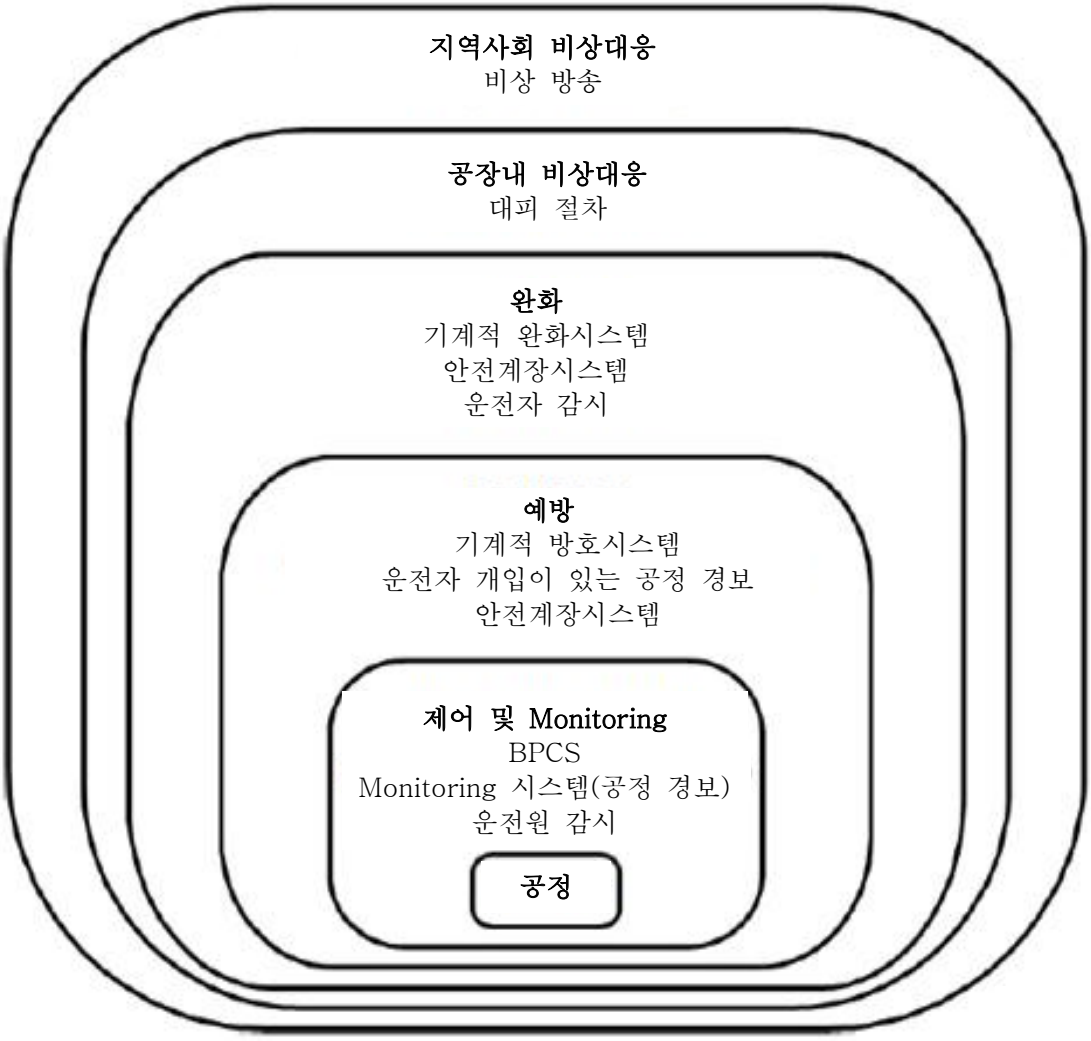
BPCS를 IEC 61511 시리즈 요건에 부합되지 않을 경우는 다음을 인정할 수 없다.

(가) BPCS가 방호계층의 요구 개시원일 때 위험사건에 이르는 동일한 연속 사건에 대해 2개 이상의 BPCS를 방호계층으로 인정할 수 없음([그림 4] 참조).

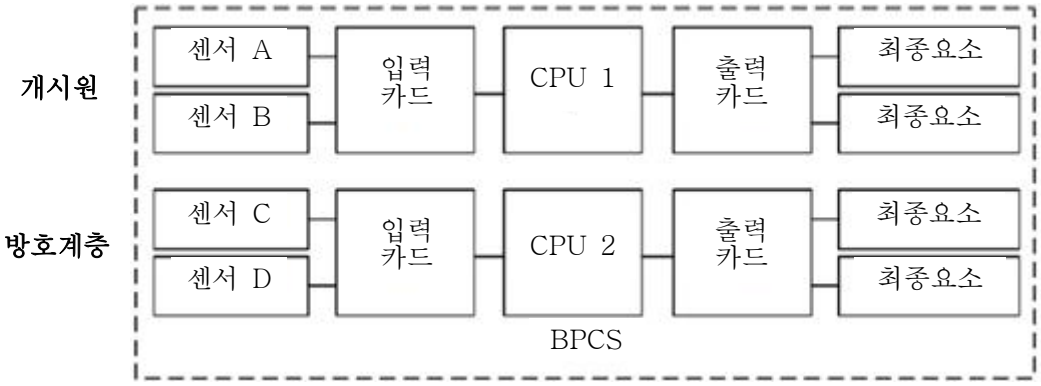
(나) BPCS가 방호계층의 요구 개시원이 아닐 때 위험사건에 이르는 동일한 연속 사건에 대해 3개 이상의 BPCS를 방호계층으로 인정할 수 없음([그림 5] 참조)

(5) BPCS 방호계층의 독립성

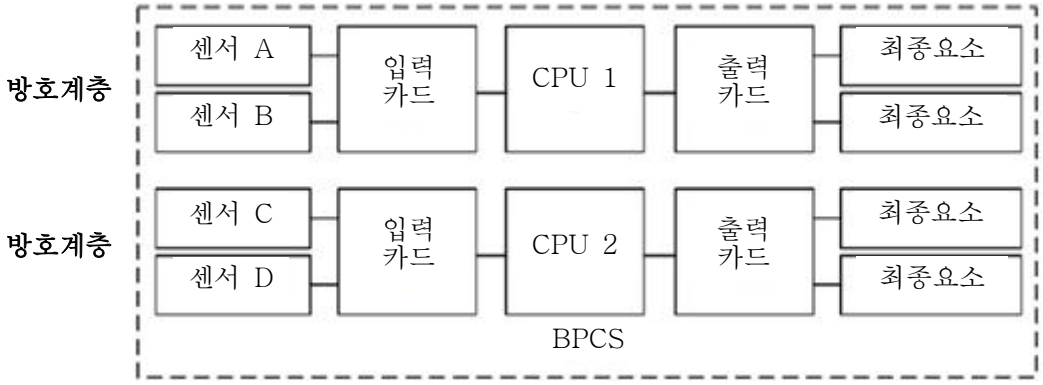
(4)항을 적용할 때 각 BPCS 방호계층은 다른 방호계층이나 개시 원인과 독립적으로 분리되어야 한다.



[그림 3] 전형적인 방호계층과 리스크 감축 수단



[그림 4] BPCS 개시원과 BPCS 방호계층의 독립성



[그림 5] 두 BPCS 방호계층의 독립성

5.2.4 공통원인, 공통모드 및 종속적인 고장 방지를 위한 요건

(1) 방호계층 설계 평가

(가) 방호계층의 설계를 평가하여 방호계층 간 및 방호계층과 BPCS 간 공통원인, 공통모드 및 종속적인 고장의 가능성이 전체 안전무결성요건에 비해 충분히 낮도록 설계하여야 한다.

(나) SIL4를 적용하지 않는 한 평가는 정성적 또는 정량적으로 가능하다.

(2) 평가 시 고려 사항

(가) 방호계층 간 독립성

(나) 방호계층 간 다양성

(다) 다른 방호계층 간 물리적 분리

6. SIS 안전요건 명세서(SRS)

6.1 목적

사용자가 자신이 원하는 각 SIF의 설계 및 SIS 내 통합 방식을 정의할 수 있도록 아키텍처 및 응용프로그램(AP)을 포함하는 SIS 요건을 지정하는 것이 목적이다.

6.2 일반 요건

(1) H&RA에서 파악된 요건과 SIF 할당으로부터 안전요건을 도출하여야 한다.

(2) SIS 및 AP 요건은 다음과 같다.

(가) 명료/정확/확인가능/유지가능/실현가능 하도록 구성하여야 함

(나) 임의의 수명주기 단계에서 그 정보를 활용할 사람들의 이해 및 해석을 도울 수 있도록 표현하여야 함

6.3 SIS 안전 요건

6.3.1 SRS 내용

(1) 기능안전을 설명하는 데 필요한 모든 SIF의 설명(예: 원인결과도, 논리서술)

(2) 각 SIF에 관련된 공장 입출력 장치의 목록(예: 현장 태그 목록)

(3) 공통원인고장의 파악 및 반영 요건

(4) 각 SIF에 대한 공정의 안전상태 정의

(가) 개별적으로는 안전하나 동시 발생 시 별도의 위험요인을 생성하는 개별 안전상태의 정의

(나) 각 SIF에 대해 가정한 요구원과 요구율

(다) 보증시험 간격에 관한 요건

(라) 보증시험 구현에 관한 요건

(마) 공정안전시간 내에 공정을 안전상태로 이전하기 위한 각 SIF의 응답시간 요건

(바) 각 SIF의 운전모드(요구/연속)와 SIL 요건

(사) SIS의 공정 측정, 범위, 정확성 및 연동점의 설명

(아) SIF 공정 출력 동작과 성공적 운전 기준(예: 밸브의 누설율)의 설명

(자) 공정 입력과 출력 간 함수 관계의 설명

(차) 각 SIF의 수동 셧다운 요건

(카) 각 SIF의 동력공급연동(Energize to trip)과 동력중단연동(De-energize to trip) 요건

(타) 셧다운 후 각 SIF의 리셋 요건

(파) 각 SIF에 대한 최대 허용 오연동율

(하) 각 SIF의 고장모드와 바람직한 SIS 응답

(거) SIS 개시 및 재개시 절차에 관한 특정 요건

(너) SIS와 다른 시스템(BPCS와 운전자 포함) 간의 모든 인터페이스

(더) 공장 운전모드의 설명 및 각 모드에서 SIF 운전에 관한 요건

(러) 우회된 상태에서 적용할 관리대책과 잇따르는 해소 방법을 설명하는 절차서를 포함하는 우회 요건

(머) SIS의 결함 검출 시 모드 관련된 인적 요인을 감안하여 공정의 안전상태를 달성 또는 유지하는 데 필요한 동작의 지정

(버) 이동 시간, 위치, 예비부품 보유, 용역 계약, 환경 제약조건을 감안할 때 SIS에 대해 실현가능한 평균수리시간(MRT)

(서) 회피하여야 할 SIS 출력 상태의 위험조합의 파악

(어) SIS의 선적, 저장, 설치, 운전 중 직면할 가능성이 있는 모든 극단적 환경조건의 파악(온도, 습도, 오염물, 접지, 전자기 간섭, 충격, 진동, 번개, 홍수 등)

(저) 공장 전체와 개별 공장의 운전 절차를 위한 정상 및 비정상 공정 운전모드의 파악

(처) 중대사고를 견뎌내기 위해 필요한 SIF 요건(예: 화재 중 밸브가 작동을 유지해야 할 시간)의 정의

6.3.2 AP SRS

(가) SIS의 SRS와 선정된 아키텍처(배치 및 내부 구조)로부터 AP의 안전요건을 도출하여야 한다.

(나) SIS 아키텍처와 일치하는 SIF를 구현하는 각 프로그램가능 SIS 장치에 대해 AP 안전요건을 지정하여야 한다.

(다) AP 안전요건은 SRS 또는 별도의 문서(AP SRS)에 둘 수 있다.

(라) AP SRS는 다음 사항을 포함하여야 한다.

① AP에 의해 지원되는 SIF와 그 SIL

② 지정된 시간 내에 수신해야 하는 실시간 성능 파라미터

③ 프로그램 순서와 시간 지연

④ 장치와 운전자 간 인터페이스와 그 운전가능성

⑤ 모든 관련된 공정 운전모드

⑥ 불량한 공정변수에 대해 취할 동작

⑦ AP 내에서 수행되는 외부장치의 검증 및 진단 시험을 가능케 하는 기능

⑧ 자체감시

⑨ SIS 내 다른 장치(예: 센서, 최종요소)의 감시

⑩ 공정 운전 중 SIF의 주기적 시험에 관한 요건

⑪ 입력 문서에 대한 참조

⑫ 통신 인터페이스에 관한 요건

⑬ AP에 의해 발생되는 공정 위험상태의 파악 및 회피

⑭ 각 SIF에 대한 공정변수 입증 기준의 정의

7. SIS 설계와 엔지니어링

7.1 목적, 일반 및 시스템거동 요건

7.1.1 목적

지정된 안전요건을 충족하면서 SIF를 제공하는 단일 또는 다중 SIS의 설계

7.1.2 일반 요건

(1) SIS 설계 요건

7항 요건을 감안하여 SIS SRS에 따라 SIS를 설계하여야 한다.

(2) SIF와 non-SIF를 모두 구현하는 SIS

SIS가 SIF와 non-SIF를 모두 구현하는 경우 정상 및 결함 조건에서 SIF에 부정적인 영향을 미칠 수 있는 모든 하드웨어, 내장소프트웨어, 응용프로그램을 SIS의 일부로 취급하고 영향을 받는 SIF의 최상위 SIL 요건에 따라 설계하여야 한다.

(3) 다른 SIL을 갖는 SIF

(가) SIS가 다른 SIL을 갖는 여러 SIF를 구현하는 경우 공유된 또는 공통의 하드웨어, 내장소프트웨어, 응용프로그램은 가장 높은 SIL에 부합하여야 한다.

(나) 이 경우 SIF와 SIL에 명확한 분류 표식(label)을 부착하여야 한다.

(4) BPCS와 SIS 간 독립성

(가) IEC 61511 시리즈에 따른 자격을 BPCS에 부여하지 않을 의도라면 SIS의 안전 무결성을 위태롭게 하지 않는 범위 내에서 분리되고 독립적인 SIS를 설계하여야 한다.

(나) BPCS와 SIS의 분리 사유

① 공통원인/공통모드/시스템 고장을 줄여 BPCS 고장이 SIS에 미치는 영향을 최소화

② BPCS에 관련된 변경, 유지보수, 시험 문서화의 유연성 유지

③ SIS 장치의 식별과 관리를 촉진하여 SIS의 입증과 FSA가 더 단순하고 명확해짐

④ SIS에 대한 접근 보안을 지원하고 사이버 보안을 강화하여 BPCS 함수 또는 데이터를 개정해고 SIS에 영향을 주지 않음

⑤ SIS와 BPCS의 적정 설계, 확인, 관리를 보장하기 위해 수행해야 할 분석량을 줄임

(다) BPCS와 SIS의 분리 대상 및 방법

① 일반적으로 현장 센서, 최종 요소, 논리해결기 및 배선(wiring)의 4 영역에 대해 적용

② BPCS와 SIS에 같은 기술을 사용하는 동종(identical) 분리 또는 다른 기술을 사용하는 이종(diverse) 분리를 사용할 수 있음

(5) 운전가능성 등의 요건

(가) 위험한 고장의 가능성을 낮추기 위하여 SIS 설계 중 운전/유지보수/진단/검사/시험 가능성 요건을 다루어야 한다.

(나) 계기나 장치가 오작동 또는 고장 날 수 있는 것처럼 사람도 실수를 하거나 과업을 수행하지 못할 수 있으므로 인적 수행도 하나의 시스템 설계 및 무결성 인자

이다.

(다) 인적 오류를 야기하는 조건을 파악하고 과오율(error rate) 추정치를 얻기 위한 인간 신뢰도 분석(HRA)을 수행하여야 한다.

(6) 인적 요인

(가) SIS 설계는 사람의 능력 및 한계를 감안하고, 운전자와 유지보수자에게 배정된 과업에 적합해야 한다.

(나) 운전자 인터페이스 설계는 좋은 인적 요인 관행을 따르고 운전자가 받아야 하는 훈련 수준을 수용하여야 한다.

(다) 리셋 전 안전상태 유지

SRS에 별다른 지시가 없는 한 SIS에 의해 안전상태에 놓인 공정이 리셋 개시 전까지는 안전상태를 유지하도록 SIS를 설계하여야 한다.

(7) 수동 수단

SRS에 별다른 지시가 없는 한 논리해결기와 독립적인 수동 수단(예: 비상 중지 푸시버튼)을 제공하여 SIS 최종요소를 구동시킬 수 있어야 한다.

(8) 독립성과 종속성

SIS와 BPCS 간 및 SIS와 다른 방호계층 간 독립성과 종속성을 고려하여 SIS를 설계하여야 한다.

(9) BPCS와 SIS 간 장치 공유

BPCS에서 사용되는 장치의 고장이 SIF에 대한 요구 또는 SIF의 위험한 고장을 초래할 수 있을 때는 분석을 수행하고 그 결과, 전체 리스크가 허용가능함을 확인한 후에 SIS에 사용해야 한다.

(10) 유틸리티 중단

유틸리티(예: 전력, 공기, 유압 등) 중단 시 안전상태로 고장(fail safe) 나지 않는 SIS 장치에 대해 유틸리티 중단의 검출 및 경보와 7.1.3항에 따른 조치를 취하여야 한다.

(11) 보안 리스크

파악된 보안 리스크(5.1.2 (4)항 참조)에 대해 필요한 회복력(resilience)을 제공하도록 SIS를 설계하여야 한다.

(12) 안전매뉴얼

SIS에 관련된 운전, 유지보수, 결함 검출 및 제약조건을 다루어 의도한 장치 구성 및 운전환경을 제시하는 안전매뉴얼을 마련하여야 한다.

(13) 통신

필요한 SIL을 충족하기 위하여 안전 응용에 적합한 기법을 사용하여 SIL 구현에 사용되는 모든 통신을 확립하여야 한다.

7.1.3 결함 검출 시 시스템 거동 요건

(1) 보상대책

(가) 진단시험, 보증시험 또는 다른 수단에 의해 SIS 내의 위험결함 검출 시 안전운전을 유지하기 위한 보상 대책을 수행하여야 한다.

(나) 안전운전을 유지할 수 없을 때 공정의 안전상태를 달성 또는 유지하기 위한 지정된 조치를 수행하여야 한다.

(2) 경보

(가) 보상대책이 경보에 대응하여 지정된 조치를 취하는 운전자에 의존할 경우 이 경보를 SIS의 일부분으로 고려하여야 한다.

(나) 이 경보에 대한 적절한 보증시험 및 변경요소관리가 필요하다.

7.2 하드웨어 결함허용(HFT)

7.2.1 최소 HFT

(1) SIS는 자신이 구현하는 각 SIF에 대해 최소한의 HFT를 가져야 한다.

(2) 이는 아키텍처가 무작위 하드웨어 결함과 일부 시스템 결함에 대해 필요한 결함허용을 갖도록 보장하기 위한 것으로서 아키텍처 제약조건(Aarchitectural constraints, AC)라고도 불린다.

7.2.2 SIS 서브시스템의 HFT

SIS를 독립적인 SIS 서브시스템으로 나눌 수 있을 때 SIS 서브시스템 수준에서 HFT을 할당할 수 있다.

7.2.3 HFT 요건 조항

SIS 또는 SIS 서브시스템은 다음 세 조항 중 하나에 부합하여야 한다.

(1) IEC 61508-2:2010 7.4.4.2 (route 1H)

(가) 먼저 시스템 또는 서브시스템의 성분 장치의 유형을 아래 정의에 따라 Type A 또는 Type B로 분류함

① Type A: 안전기능을 달성하는 데 필요한 성분들에 대해 다음을 모두 충족하는 장치(예: 스위치, 솔레노이드, 릴게이)

㉮ 모든 구성 성분들의 고장모드가 잘 정의되어 있음

㉯ 결함 조건에서 성분의 거동을 완전히 결정할 수 있음

㉰ 주장된 검출 및 미검출 위험한 고장률 뒷받침할 수 있을 만큼의 충분한 고장률 데이터가 있음

② Type B: Type A가 아닌 장치(예: 마이크로프로세서 기반 장치)

(나) 다음, 장치 유형별로 <표 5> 또는 <표 6>에 보인 안전고장분률(SFF), 하드웨어 결함허용(HFT), 안전무결성수준(SIL) 간 관계를 만족하여야 함

<표 5> Type A의 성분 또는 서브시스템에 의해 수행되는 안전기능의 최대 허용 안전무결성수준

안전고장분률 (SFF)	하드웨어 결함허용(HFT)		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% - < 90%	SIL2	SIL3	SIL4
90% - < 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

<표 6> Type B의 성분 또는 서브시스템에 의해 수행되는 안전기능의 최대 허용 안전무결성수준

안전고장분률 (SFF)	하드웨어 결함허용(HFT)		
	0	1	2
< 60%	허용불가	SIL1	SIL2
60% - < 90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

(2) IEC 61508-2:2010 7.4.4.3 (route 2H)

최종 사용자로부터 피드백(feedback)된 구성성분 장치의 신뢰도 데이터에 의거하여 지정된 안전무결성수준을 위해 증가된 신뢰수준을 갖는 HFT

(3) 7.2.5 ~ 7.2.9

* (3)은 공정산업 부문을 위해 (2)로부터 도출되었음

7.2.4 결함배제

(1) HFT 요건 결정 시 특정 결함의 발생 가능성이 안전무결성요건과 관련하여 매우 낮으면 그 결함을 배제할 수 있다.

(2) 이런 결함배제의 타당성을 입증하고 문서화하여야 한다.

7.2.5 SIL 별 최소 HFT

지정된 SIL의 SIF를 구현하는 SIS 또는 그 서브시스템에 필요한 최소 HFT는 <표 7>과 (적절한 경우) 7.2.6 항과 7.2.7 항에 부합하여야 한다.

<표 7> SIL 별 최소 HFT 요건

안전무결성수준(SIL)	최소 HFT
1 (임의 모드)	0
2 (저요구모드)	0
2 (고요구모드 또는 연속모드)	1
3 (임의 모드)	1
4 (임의 모드)	2

7.2.6 HFT 축소

(1) FVL 또는 LVL 프로그램가능 장치를 사용하지 않는 SIS 또는 SIS 서브시스템에서 <표 7>에 지정된 최소 HFT가 추가적인 고장을 초래하여 전체 공장 안전이 감소한다면 HFT를 축소할 수 있다.

(2) 이때 제안된 아키텍처가 의도된 목적에 적합하고 안전무결성 요건을 충족한다는 증거를 제시하고 문서화하여야 한다.

7.2.7 HFT가 0일 때의 타당성 입증

7.2.6 항 적용 시 결함허용이 0이라면 7.2.6 항에서 요구하는 타당성 입증 때 잠재적인 시스템 고장을 포함하여 관련된 위험한 고장 모드를 7.2.4 항에 따라 배제할 수 있다는 증거를 제시하여야 한다.

7.2.8 FVL/LVL 장치의 진단범위

FVL 및 LVL 프로그램가능 장치는 60% 이상의 진단범위를 가져야 한다.

7.2.9 신뢰도 데이터

고장척도 계산에서 사용되는 신뢰도 데이터는 70% 이상의 통계적 신뢰한계의 상한값으로 결정하여야 한다.

7.3 장치 선정 요건

7.3.1 목적

(1) SIS의 일부로 사용할 장치의 선정에 관한 요건 지정

(2) SIS 아키텍처로의 장치 통합을 가능케 하는 요건 지정

(3) 장치의 수용 기준을 관련 SIF와 안전무결성요건 면에서 지정

7.3.2 일반 요건

(1) SIS 장치의 요건 조항

지정된 SIL을 갖는 SIS의 일부로 사용할 장치는 IEC 61508-2:2010과 IEC 61508-3:2010 또는 7.3.3~7.3.6 항에 부합하여야 한다.

(2) 운전환경

(가) 모든 장치는 제조자의 문서, SRS 내의 제약조건, 7.7 항에서 가정한 신뢰도 파라미터의 검토를 통해 결정되는 대로 운전환경에 적합하여야 한다.

(나) 선정된 장치의 적합성은 항상 운전환경의 맥락에서 검토하여야 한다.

7.3.3 사전사용에 기반한 장치 선정 요건

(1)장치 적합성 증거

장치가 SIS 내에서 사용하기 적합하다는 적절한 증거를 마련하여야 한다.

(2) 적합성 증거 포함 사항

(가) 제조자의 품질 및 구성 관리시스템에 대한 검토

(나) 적절한 장치 식별과 명세서

(다) 비슷한 운전환경에서 장치 성능의 입증

(라) 운전 경험의 양

(3) 변경요소관리

(가) 사전사용에 기반하여 선정된 모든 장치는 지정된 개정 번호로 식별하고 변경요소관리 절차로 통제하여야 한다.

(나) 장치가 변경된 경우 그 심각성을 평가하여 사전사용 증거가 계속 타당함을 입증하여야 한다.

7.3.4 사전사용에 기반한 FPL 프로그램가능 장치의 선정 요건

(1) SIL1, SIL2, SIL3의 요건

SIL1, SIL2, SIL3의 경우 7.3.2 항, 7.3.3 항 및 다음 (2)~(4) 조항을 준수하여야 한다.

(2) 장치 구성 옵션

(가) 안전에 영향을 미칠 수 있는 장치의 모든 구성 옵션을 파악하고 검토하여야 한다.

(나) 구체적 설정값이 정의되지 않았으면 기본 설정(Default settings)이 적절한지 확인하여야 한다.

(다) 사용하지 않은 장치 특성을 적합성 증거에서 파악하여 이 특성이 필요한 SIF를 위협하지 않을 것임을 입증하여야 한다.

(3) 적합성 증거

장치의 특정 구성과 운전환경에 대한 적합성 증거에서 다음 사항을 고려하여야 한다.

(가) 입출력 신호의 특성

(나) 사용 모드

(다) 사용한 기능과 구성

(라) 비슷한 운전환경에서의 사전사용

(4) SIL3 응용

SIL3 응용에 대해서는 FPL 장치를 평가하여 다음 사항을 입증하여야 한다.

(가) FPL 장치가 요구된 기능을 수행할 수 있고, SIS의 일부로 사용 시 무작위 하드웨어 고장이나 하드웨어 또는 소프트웨어의 시스템 고장으로 인해 위험사건을 야기하는 방식으로 고장 날 확률이 충분히 낮음

(나) 하드웨어와 소프트웨어의 적절한 표준이 적용되었음

(다) 의도한 운전 개요(Profile)를 위한 대표적인 구성 내에서 FPL 장치가 시험되었음

7.3.5 사전사용에 기반한 LVL 프로그램가능 장치의 선정 요건

(1) SIL1 또는 SIL2의 요건

SIL1 또는 SIL2, SIF를 구현하는 SIS에서 사용할 프로그램가능 장치는 다음 (2)~(6)항을 준수하여야 한다.

(2) 7.3.4 항을 준수하여야 함

(3) 운전환경

과거에 경험한 장치의 운전환경과 SIS 내 사용 시 운전환경 간에 차이가 날 경우 그 차이를 파악하고 적절한 분석 및 시험을 통해 평가함으로써 SIS에 사용 시 시스템 결함의 가능성이 충분히 낮음을 입증하여야 한다.

(4) 운전 경험

적합성 입증에 필요한 운전 경험은 다음 사항을 감안하여 결정하여야 한다.

(가) SIF의 SIL

(나) 장치의 복잡성과 기능성

(5) 안전구성 PE 논리해결기

SIL1 또는 SIL2 응용에서 다음의 추가 단서가 충족되면 안전구성 PE 논리해결기를 사용할 수 있다.

(가) 불안전 고장모드의 이해

(나) 파악된 고장모드를 다루는 안전구성 기법 사용

(다) 안전 응용에서 우수한 사용실적이 있는 내장소프트웨어

(라) 허가받지 않거나 의도하지 않은 변경에 대한 보호

(6) SIL2용 PE 논리해결기 평가

SIL2 응용에 사용되는 PE 논리해결기에 대한 공식 평가를 통해 다음 사항을 입증하여야 한다.

(가) LVL 장치가 요구된 기능을 수행할 수 있고, SIS의 일부로 사용 시 무작위 하드웨어 고장이나 하드웨어 또는 소프트웨어의 시스템 고장으로 인해 위험사건을 야기하는 방식으로 고장 날 확률이 충분히 낮음

(나) 프로그램 실행 중 결함을 검출하고 적절한 대응을 개시하는 대책이 구현됨

7.3.6 FVL 프로그램가능 장치 선정 요건

FVL을 사용하는 프로그래밍이 수행되는 응용에서 PE 장치는 IEC 61508-2:2010과 IEC 61508-3:2010에 부합하여야 한다.

7.4 현장장치

7.4.1 선정과 설치

(1) 현장장치는 운전환경 조건으로 인해 부정확한 정보를 야기할 수 있는 고장을 최소화할 수 있도록 선정 및 설치하여야 한다.

(2) 이때 다음과 같은 운전환경 조건을 검토하여야 한다.

(가) 부식

(나) 배관 내 물질의 동결

(다) 부유 고형물

(라) 중합

(마) 코킹

(바) 극단적 온도 및 압력

(사) 건식 레그(Dry-leg) 충격관(Impulse line)에서의 응축

(아) 습식 레그(Wet-leg) 충격관에서의 불충분한 응축

7.4.2 동력공급연동 회로

동력공급연동 회로에서 회로와 전력 공급의 무결성을 보장하는 수단을 적용하여야 한다.

7.4.3 스마트 센서

스마트 센서는 부주의로 인한 변경을 방지하기 위해 쓰기 보호(Write-protected)를 하여야 한다.

7.5 인터페이스

7.5.1 일반 사항

SIS 인터페이스는 다음 요소들을 포함한다.

(1) 운전자 인터페이스

(2) 유지보수/엔지니어링 인터페이스

(3) 통신 인터페이스, 등

7.5.2 운전자 인터페이스 요건

(1) 구성

운전자와 SIS 간 정보 교환에 사용되는 운전자 인터페이스는 다음으로 구성된다.

(가) 디스플레이

(나) 전등, 푸시버튼, 스위치 등을 담은 패널

(다) 경보기(시각적 및 청각적))

(라) 프린터

(마) 이들의 조합

(2) BPCS 운전자 인터페이스 고장

SIS 운전자 인터페이스가 BPCS 운전자 인터페이스를 통해 이루어질 때 BPCS 운전자 인터페이스에서 발생 가능한 고장을 감안하여야 한다.

(3) 운전자 조치 최소화

(가) 위험요인이 존재하는 동안 운전자의 옵션 선택과 시스템 우회의 필요성을 최소화하도록 SIS를 설계하여야 한다.

(나) 운전자 조치 필요 시 운전자 과오에 대한 보호 기능을 설계에 포함하여야 한다.

(4) 우회 수단의 보호

우회 스위치 또는 수단의 미허가 사용을 방지하기 위한 보호 대책(키 잠금장치 또는 패스워드 등)이 필요하다.

(5) SIS 상태 정보

(가) SIF 유지를 위해 중요한 SIS 상태 정보를 운전자 인터페이스의 일부로서 사용 가능하여야 한다.

(나) 포함 정보

① 공정 순서(Sequence) 상의 현 위치

② SIS 보호 조치가 발생하였음을 알리는 표시

③ 보호 기능의 우회되었음을 알리는 표시

④ 자동 조치가 발생하였음을 알리는 표시

⑤ 센서와 최종요소의 상태

⑥ 안전에 영향을 미치는 에너지 공급 중단

⑦ 진단 결과

⑧ SIS 지원에 필요한 환경 공조장치의 고장

(6) SIS AP 변경 방지

SIS 응용프로그램의 변경을 방지하도록 SIS 운전자 인터페이스를 설계하여야 한다.

(7) 정보 전달

BPCS로부터 SIS로 정보가 전달되는 경우 정확한 정보 전달과 SIS의 안전무결성 유지를 확인하는 시스템, 장치 또는 절차를 적용하여야 한

(8) 잘못된 정보 제공

BPCS 운전자 인터페이스를 통한 SIS 운전자 인터페이스 설계 시 BPCS로부터 SIS로 잘못된 정보의 제공이 안전을 위협하지 않도록 하여야 한다.

7.5.3 유지보수/엔지니어링 인터페이스 요건

(1) 인터페이스 고장

(가) SIS 유지보수/엔지니어링 인터페이스 설계 시 이 인터페이스의 고장이 필요한 SIF를 수행하는 SIS의 능력에 부정적인 영향을 미치지 않도록 보장하여야 한다.

(나) 이를 위해 정상적인 SIS 운전 중 프로그래밍 패널과 같은 유지보수/엔지니어링 인터페이스의 연결을 끊는 것이 필요할 수 있다.

(2) 접근 보안 보호

유지보수/엔지니어링 인터페이스는 다음 각 기능에 대한 접근 보안 보호를 제공하여야 한다.

(가) SIS 운전모드, 프로그램 데이터, 경보 전달 무능화 수단, 시험, 우회, 유지보수

(나) SIS 진단, 투표와 결함 처리 서비스

(다) 응용프로그램 추가, 삭제 또는 변경

(라) SIS 고장 검사(Troubleshoot)에 필요한 데이터

(마) 경보와 수동 셧다운 기능을 훼손하지 않는 우회 설치

(3) 운전자 인터페이스로 사용 금지

유지보수/엔지니어링 인터페이스를 운전자 인터페이스로 사용하면 안 된다.

(4) 읽기-쓰기 접근권한 지정 방식

읽기-쓰기 접근(Access)을 가능 또는 불가능으로 지정하는 작업은 다음과 같은 구성 관리 과정에 의해서만 수행하여야 한다.

(가) 유지보수/엔지니어링 인터페이스 사용

(나) 적절한 문서화

(다) 신원 증명과 사용자 보안 채널과 같은 보안 대책

7.5.4 통신 인터페이스 요건

(1) 인터페이스 고장

SIS 통신 인터페이스 설계 시 이 인터페이스의 고장이 필요한 SIF를 수행하는 SIS의 능력에 부정적인 영향을 미치지 않도록 보장하여야 한다.

(2) BPCS 및 주변장치(peripherals)와의 통신

SIS가 BPCS 및 주변장치와 통신할 수 있을 때 통신 인터페이스, BPCS 또는 주변장치의 고장이 SIS 내 SIF에 부정적인 영향을 미치면 안된다.

(3) 전자기 간섭에 대한 강건성(Robustness)

통신 인터페이스는 SIS의 위험한 고장을 야기하지 않도록 전력급증(Ppower surge)을 포함하여 전자기 간섭에 견딜 수 있도록 충분히 강건하여야 한다.

(4) 다른 접지퍼텐셜을 갖는 장치 간 통신

통신 인터페이스는 서로 다른 전기적 접지퍼텐셜을 기준점으로 삼는 장치 간의 통신에 적합하여야 한다.

7.6 유지보수 또는 시험 설계 요건

7.6.1 SIS 시험 부위와 온라인 시험

(1) SIS 전체(End-to-end)(센서 쪽 공정 유체에서 구동기 쪽 공정 유체 까지) 또는 부분별(In segments) 시험을 할 수 있도록 SIS를 설계하여야 한다.

(2) 예정된 공정 셧다운 간 간격이 보증시험 간격보다 클 때는 온라인 시험 설비가 필요하다.

7.6.2 온라인 시험 설비

온라인 보증시험 필요 시 시험 설비는 SIS 설계의 중요한 일부분이 되어야 한다.

7.6.3 시험 또는 우회 설비

SIS 내에 시험 또는 우회 설비가 포함되어 있을 때 이 설비들은 다음 사항을 충족하여야 한다.

(1) SIS에 정의된 유지보수 및 시험 요건에 따라 SIS 설계

(2) SIS의 일부분이 우회될 때 경보 또는 운전절차를 통해 운전자에게 알림

7.6.4 최대 우회 허용시간

공정의 안전 운전이 지속되는 동안 SIS가 우회 상태(수리 또는 시험)로 있을 수 있는 최대 시간을 정의하여야 한다.

7.6.5 우회 시 보상 대책

SIS가 우회 상태에 있을 때 지속적인 안전운전을 보장하는 보상대책을 7.1.3 항에 따라 마련하여야 한다.

7.6.6 강제적인 입력 및 출력

(1) PE SIS에서 입력 및 출력의 강제(Forcing)를 응용프로그램, 운전절차 및 유지보수의 일부로 사용하지 않아야 한다.

(2) SIS 서비스를 중단하지 않은 상태에서 강제적인 입력 및 출력은 절차와 접근 보안에 의해 보안되지 않는 한 허용되지 않아야 한다.

(3) 이런 강제 시 공표(Announce) 또는 경보 발령이 필요하다.

7.7 무작위 고장의 정량화

7.7.1 SIF의 고장척도

(1) 각 SIF에 대해 계산된 고장척도는 SRS에서 지정한 SIL과 관련된 목표고장척도와 같거나 더 나아야 한다.

(2) 이 요건을 계산에 의해 결정하여야 한다.

7.7.2 고장척도 기여 요인

무작위 고장으로 인한 각 SIF의 고장척도 계산 시 다음 기여 요인들을 감안하여야 한다.

(1) 고려중인 각 SIF와 관련된 SIS 또는 SIS 서브시스템의 아키텍처

(2) SIS의 위험한 고장에 기여하지만 진단시험에서 검출되는 무작위 하드웨어 고장으로 인한 각 고장모드의 추정 고장률(λ_{Ddd})

(3) SIS의 위험한 고장에 기여하지만 진단시험이 아닌 보증시험에서 검출되는 무작위 하드웨어 고장으로 인한 각 고장모드의 추정 고장률(λ_{Ddp})

(4) SIS의 위험한 고장에 기여하지만 진단시험 및 보증시험에서 검출되지 않는 무작위 하드웨어 고장으로 인한 각 고장모드의 추정 고장률(λ_{Du})

(5) 보증시험 자체에 의해 야기되는 SIS의 고장 가능성

(6) SIS의 공통원인고장 가능성

(7) 주기적 진단시험의 진단범위와 시험 간격, 진단 설비의 고장 확률

(8) 주기적 보증시험의 검증율과 시험 간격, 시험 설비와 절차의 신뢰도

(9) 검출 고장의 수리시간과 수리 중 SIS 상태(온라인 또는 오프라인)

(10) SIS의 위험한 고장을 야기하는 통신 과정의 위험한 고장률 추정값

(11) 운전자 대응이 SIS의 위험한 고장을 야기할 가능성의 추정값

(12) SIS에 필요한 유틸리티의 신뢰도

7.7.3 신뢰도 데이터

무작위 고장의 효과를 정량화할 때 사용되는 신뢰도 데이터는 믿을 만하고, 추적가능하며, 문서화되어 있고, 타당성이 입증되어야 하며 비슷한 운전환경에서 비슷한 장치의 사용에 따른 현장 피드백(Feedback)에 기반 하여야 한다.

7.7.4 신뢰도 데이터의 불확실성

(1) 신뢰도 데이터의 불확실성을 평가하여 고장척도 계산에 반영하여야 한다.

(2) 고장척도 계산을 위해 다음의 기법을 사용할 수 있다.

(가) 고장척도에 대한 보수적인 점추정값(Point estimate)을 얻기 위해 각 입력 신뢰도 파라미터의 평균값 대신 70 % 신뢰한계의 상한값 사용

(나) 입력 신뢰도 파라미터의 확률분포 함수를 사용하여 Monte Carlo 모사를 수행하여 고장척도의 분포를 나타내는 히스토그램을 얻은 다음 이 분포로부터 보수적인 값을 평가함

7.7.5 목표고장척도 미달성 시의 조치

특정 설계에 대해 관련 SIF의 목표고장척도가 달성되지 않으면 다음 조치를 수행하여야 한다.

(1) 고장척도에 기장 많이 기여하는 장치 또는 파라미터의 파악

(2) 파악된 장치 또는 파라미터에 대한 가능한 개선 대책의 효과 평가(예)

(가) 더 신뢰할 만한 장치 사용

(나) 공통모드고장에 대한 추가 방어

(다) 중복성(Redundancy) 증가

(라) 진단 또는 검증 시험의 성공률

(마) 단축된 보증시험 간격

(바) 시차(Staggered) 시험

(3) 새로운 결과를 확립하기 위한 개선 대책의 선정 및 구현

(4) 새 결과와 목표고장척도를 비교하여 보수적인 장식으로 충족될 때 까지 1)~3)의 절차 반복

7.8 SIS 응용프로그램 개발

7.8.1 목적

응용프로그램 개발을 위한 요건을 정의한다.

7.8.2 일반 요건

(1) AP 요건 조항

SIS 응용프로그램은 응용프로그램 안전요건(6.3.2 (2))과 SIL1~SIL3를 위한 이 조항의 모든 요건에 부합하여야 한다.

(2) AP 요건의 검토

(가) 응용프로그래머는 SRS 내의 정보와 응용프로그램 안전요건을 검토하여 이 요건이 포괄적이고, 명확하며, 이해가능하고 일관되도록 보장하여야 한다.

(나) 응용프로그램 안전요건 상의 결점을 파악하여 해석하고, 이 요건에 변경이 가해진 경우에는 영향 분석을 수행하여야 한다.

(3) IEC 61511 시리즈 적용 대상

(가) IEC 61511 시리즈는 LVL 프로그래밍과 FPL을 사용하는 장치의 사용을 다루고 있으나, FVL과 SIL4 응용프로그래밍은 다루지 않는다.

(나) 기능블록이 FVL로 작성된 경우 IEC 61508-3: 2010에 따라 개발 및 변경하여야 한다.

(4) 비안전기능 구현 시 요건

SIS 응용프로그램이 안전기능과 비안전기능을 모두 구현 시 응용프로그램의 모든 부분을 SIS의 일부로 간주하여 이 표준을 준수하고, 또한 평가와 시험을 통해 비안전기능이 안전기능에 지장을 주지 않음을 입증하여야 한다.

(5) SIS 리셋 전 공정 안전상태 유지

일단 SIS가 공정을 안전상태로 놓은 후에는 SRS가 달리 지시하지 않는 한 리셋 전까지 동력 중단 또는 동력 회복을 포함한 모든 상황에서 공정의 안전상태를 유지할 수 있도록 응용프로그램을 설계하여야 한다.

(6) SIS 기동 중 상태

SIS 기동 중 응용프로그램은 SRS가 달리 지시하지 않는 한 리셋 개시 전까지 안전출력이 안전상태에 머무르도록 보장하여야 한다.

(7) 응용프로그램 주사(Scan)

(가) 안전매뉴얼에서 지원되는 별도의 특정 요건이 있지 않는 한 각 응용프로그램 주사 때 모든 부분이 실행되도록 응용프로그램을 설계하여야 한다.

(나) 이때 공정 안전시간을 고려하여야 한다.

(8) AP 변경 등의 절차

SIS 응용프로그램과 데이터는 변경, 개정 통제, 버전 관리, 백업, 회복 절차에 따라 관리하여야 한다.

(9) SIS 사용자와 통합자를 위한 프로그래밍 요건

응용프로그램은 SIS 사용자와 통합자를 위한 다음과 같은 응용프로그래밍 요건을 지정하여야 한다.

(가) AP의 설계 및 개발 중 적용할 SIS 안전수명주기 단계와 활동

(나) AP의 입증에 관한 정보를 SIS 통합을 수행할 조직에게 전달

(다) SIS의 운전과 유지보수를 위해 사용자가 필요로 하는 AP 관련 정보와 절차의 준비

(라) AP의 변경을 수행할 조직이 충족해야 할 절차와 명세

7.8.3 응용프로그램 설계

(1) SIS 운전모드와 논리

응용프로그램 설계 시 각 SIF의 모든 운전모드를 포함하여 모든 SIS 논리를 다루어야 한다.

(2) AP 설계 시 입력

(가) 입력은 AP 요건을 포함한 SRS(6항), SIS 아키텍처(7항), AP 설계 개발용 수단과 도구(7.8.6항)이어야 한다.

(나) AP 설계는 SRS와 일치하고 그에 역추적 가능하여야 한다.

(3) AP 기능안전 평가

AP 설계에서 기능안전 평가를 수행하도록 허용하여야 한다.

(4) AP 설계 방법

응용프로그램 설계 시 다음 사항을 포함하여 그 요건 구현 방법을 다루어야 한다.

(가) 공정의 안전상태를 달성 또는 유지하는 기능

(나) 파악된 모든 AP 성분의 명세와 그들 간 연결 및 상호작용의 설명

(다) AP 기능과 프로그램 주사 시간 내 구현과 관련된 시간 제약조건

(라) 사용된 표준 라이브러리 모듈의 상세 설명

(마) 사용된 응용 특유의 모듈의 상세 설명

(바) 메모리 할당 방식의 설명

(사) 전역변수 목록과 그 무결성 보호 방법

(아) 모든 non-SIF와 AP의 비안전 부분과의 인터페이스의 파악

(자) 태그 목록과 그 데이터 유형을 포함한 입력 및 출력 인터페이스의 정의

(차) SIS AP와 운전자 인터페이스 간에 교환된 데이터의 상세 사항

(카) SIS AP와 BPCS 및 주변 장치 간 교환된 데이터의 상세 사항

(타) 외부 및 내부 진단 정보의 처리 및 일지 기록 방법

(파) 운전 및 유지보수 인터페이스의 구현 방법과 경보의 우선등급 결정, 표시 및 수용 방법의 상세 설명

(하) SIS 요건 충족을 위해 구현되는 외부 감시기(Watch dogs), 응용 데이터 무결성 검사, 센서 입증과 같은 응용 수준의 진단에 관한 상세 설명

(거) 예상되는 하드에어 장치와 소프트웨어 모듈의 존재와 접근가능성을 포함한 시스템 구성 검사

(너) AP 설계의 복잡성 최소화 방법

(더) SIS 서브시스템 내 결함의 검출, 공표 및 관리에 관련된 기능

(러) SIF의 주기적 온라인 시험에 관련된 기능

(머) SIF의 주기적 오프라인 시험에 관련된 기능

(버) SIS의 안전한 유지보수 수행을 허용하는 기능

(서) AP 설계 명세서의 기반 문서에 대한 참조

(5) 기타 요건

AP 설계 시 SRS와 그 의도된 목적에 관한 완결성과 정확성이 요구되며, 애매 모호하거나 설계 결함이 없도록 하여야 한다.

7.8.4 응용프로그램 구현

(1) AP 개발 방법론

AP 개발 방법론은 AP가 사용될 SIS PE 서브시스템의 제조자에 의해 주어지는 개발도구와 제약조건에 부합하여야 한다.

(2) AP 포함 정보

다음 정보를 응용프로그램 또는 관련 문서에 포함시켜야 한다.

(가) 응용프로그램 원 개발자

(나) AP 목적의 설명

(다) 사용한 안전매뉴얼 버전

(라) 각 SIF가 AP 모듈에 대해 갖는 의존성의 설명

(마) AP SRS로의 추적가능성

(바) 각 SIF와 그 SIL의 파악

(사) 사용 기호, 논리 규약, 표준 라이브러리 함수, 응용 라이브러리 함수의 파악 및 설명

(아) SIS 논리해결기 입력 및 출력 신호의 파악

(자) 전체 SIS가 통신을 활용할 경우 통신 정보 흐름의 설명

(차) 입출력 서브시스템에 대한 데이터의 논리적 처리 순서와 주사 시간에 의해 부과되는 제한을 포함하여 프로그램 구조에 대한 설명

(카) SRS 요구 시 현장 데이터와 송신한 데이터의 정확성과 통신의 보안성을 보장하기 위한 수단

(타) 버전 식별과 변경 기록

(3) 이미 개발된 AP 라이브러리 함수의 사용

이미 개발된 AP 라이브러리 함수를 설계의 일부로 사용하려면 그 적합성을 IEC 61508 또는 IEC 61511의 사전사용 요건에 따라 입증하여야 한다.

(4) AP 생산

응용프로그램은 다음 사항을 달성할 수 있도록 구조화된(Structured) 방식으로 생산하여야 한다.

(가) 기능성의 모듈 분해

(나) SIF 응용프로그램의 복잡성을 필요한 SIF의 복잡성 수준에 맞게 최소값으로 유지

(다) AP의 기능성(결함허용 특성 포함)과 내부 구조의 시험가능성

(라) 응용 기능과 관련 제약조건의 추적가능성 및 설명

(마) 하드웨어 아키텍처와 AP 아키텍처의 일대일 맵핑

7.8.5 응용프로그램 확인(검토와 시험) 요건

(1) 확인 계획

확인 계획은 9.1 항에 따라 수행하여야 한다.

(2) AP 검토

AP와 그 문서는 원 개발에 참여하지 않은 능숙한 사람이 검토하고, 그 방법과 결과를 문서화하여야 한다.

(3) AP 확인의 목적, 방법 및 내용

AP 기능이 SRS를 충족하고, 의도하지 않은 기능이 실행되지 않으며, SIF에 관한 의도하지 않은 부작용이 없음을 확인하기 위하여 문서화된 절차 및 시험 명세를 사용하는 검토, 분석, 모사 및 시험 기법을 통해 다음 사항을 확인하여야 한다.

(가) AP 설계 명세서, 정의된 수단 및 절차, 안전 확인 및 시험 계획 요건의 준수

(나) AP의 모든 부분의 실행연습(Exercising)

(다) 대표적인 데이터 조건의 범위 실행연습

(라) 고장 조건의 시험(부정적(Negative) 시험)

(마) SIS의 송수신 시험(발생 가능한 통신 과부하 조건의 확인 및 시험)

(바) 오프라인 AP를 논리해결기 하드웨어 및 PE와 통합

(사) 논리해결기가 단지 겉보기로서가 아니라 예상대로 작동함을 확인하기 위한 내부데이터 흐름 검사

(아) 가능한 경우 AP와 제3자(Third party) 장치의 통합

(4) 입출력 데이터

AP 입출력 데이터의 맵핑, 유형 및 범위를 확인하여야 한다.

(5) 변경 영향 분석

위한 영향 분석을 수행하여야 한다.시험 중 영향을 받는 모든 AP 요소와 필요한 재설계 및 재확인 활동을 결정하기

(6) AP 시험 결과 문서화

다음 사항을 포함하는 AP 시험 문서를 작성하여야 한다.

(가) 시험을 받는 AP의 버전과 그 지원 문서

(나) 지원 소프트웨어의 버전과 시험 도구

(다) 시험의 설명, 검토 및 수행 날짜

(라) 시험 결과

(마) 시험의 목적과 기준의 충족 여부

(바) 시험 중 고장 발생 여부, 고장 발생 이유, 고장의 분석 및 그 수정 기록, 재시험 요건

7.8.6 응용프로그램 방법론과 도구의 요건

(1) 안전매뉴얼

AP 개발은 적용 가능한 안전매뉴얼 내의 제약조건에 부합하여야 한다.

(2) 목적, 방법 및 도구

(가) 목적

① AP 내 결함 도입 리스크 최소화

② AP 내의 기존 결함 발견 및 제거

③ AP 내 잔류하는 결함이 수용 불가능한 결과를 야기하지 않도록 실현가능한 정도까지 보장

④ SIS 수명주기 전반에 걸친 AP 변경관리 수단의 제고

⑤ AP가 요구되는 품질을 갖고 있다는 증거 제공

(나) 방법과 도구

① 구성과 버전 통제

② 요건 관리 데이터베이스

③ 설치상태(As-built) 문서의 갱신

④ 문서 통제와 변경 관리

⑤ 추적가능성과 변경 책임의 추적

⑥ 자동시험 모음(Suites)

7.9 공장 수용 시험(Factory acceptance test, FAT)

7.9.1 목적

SRS에 정의된 요건 충족을 보장하기 위한 SIS 장치의 시험

7.9.2 권장 사항

(1) 필요성 지정 시기

FAT의 필요성은 프로젝트의 안전계획 중 지정하여야 한다.

(2) FAT 계획의 내용

(가) 수행할 시험의 유형

① 블랙박스 시스템 기능성 시험

② 성능 시험

③ 내부 점검

④ 환경 시험

⑤ 인터페이스 시험

⑥ 악화된 또는 결함 조건에서의 시험

⑦ 예외(Exception) 시험

⑧ 동력 중단 시 안전 반응 시험(동력 회복 후 재개 포함)

⑨ SIS 유지보수 및 운전 매뉴얼 적용

(나) 시험 사례, 시험 설명과 시험 데이터

(다) 다른 시스템/인터페이스에의 의존성

(라) 시험 환경과 도구

(마) 논리 해결기, 센서, 최종요소 구성

(바) 시험 종료 판단 기준

(사) 시험 인력의 능숙도

(아) 물리적 위치

(자) 시험에 의해 제기되는 위험요인

(차) 시험 셋업의 명확한 도면

(카) 수행한 시험, 데이터, 결과, 수행 중 관찰 사항의 기록

(3) FAT 대상

FAT는 정의된 버전의 논리해결기에 대해 수행하여야 한다.

(4) FAT 수행 기준

FAT 계획에 따라 수행하여야 하며 모든 논리가 올바르게 수행됨을 보여야 한다.

(5) 시험 취급 사항

(가) 사용되는 시험 계획의 버전

(나) 시험되는 SIF와 성능 특성

(다) 상세한 시험 절차와 시험 설명

(라) 시험 활동의 시간대별 기록

(마) 사용된 도구, 장치와 인터페이스

(6) 결과 문서화

(가) 시험 사례, 시험 결과, 목적과 시험 기준의 충족 여부를 기술하는 문서를 작성하여야 한다.

(나) 시험 실패 시 실패 사유를 분석하고 적절한 수정 조치를 구현하여야 한다.

(7) 변경 분석

FAT 중 일어난 변경 또는 변화에 대한 안전 분석을 실시하여 다음 사항을 결정하여야 한다.

(가) 각 SIF에 미치는 영향의 범위(Extent)

(나) 정의하고 구현해야 할 시험 및 확인의 범위

8. SIS 설치, 시운전, 입증, 유지보수, 변경 및 해체

8.1 SIS 설치, 시운전 및 입증

8.1.1 목적

(1) SIS SRS와 도면에 따라 SIS를 설치하고 최종 시스템 입증 준비를 위한 시운전을 실시하여야 한다.

(2) 검사와 시험을 통해 설치 및 시운전된 SIS와 그 관련 SIF가 SRS에 기술된 요건을 달성함을 입증하여야 한다.

8.1.2 설치 및 시운전 요건

(1) 설치 및 시운전 계획

(가) 설치와 시운전에 필요한 모든 활동을 정의하여야 하며 다음 사항을 제공하여야 한다.

① 설치 및 시운전 활동

② 설치 및 시운전에 사용할 절차, 수단, 기법

③ 활동 수행 시기

④ 이 활동의 책임을 맡은 사람, 부서, 조직

(2) 설치 및 시운전 계획은 적절한 경우 전체 프로젝트 계획에 통합할 수 있음

(가) SIS 장치 설치

모든 SIS 장치는 설계 및 설치 계획에 따라 적정하게 설치하여야 한다.

(나) SIS 시운전 활동

① 최종 시스템 입증을 위해 계획에 따라 SIS를 시운전하여야 한다.

② 시운전 활동에서 다음 사항을 확인하여야 한다.

㉮ 적절한 접지 연결

㉯ 에너지원의 적절한 연결과 운전 상태

㉰ 수송용 멈추개(Stops)와 충전 물질의 제거

㉱ 물리적 훼손이 없음

㉲ 모든 계기의 적절한 교정과 구성

㉳ 모든 현장장치의 운전

㉴ 논리해결기와 입력/출력의 운전 상태

㉵ 다른 시스템과 주변 장치와의 인터페이스 운전 상태

㉶ 원격 SIS 시스템 간 통신 상태

(다) 시운전 기록

① SIS 시운전 활동의 결과와 설계 단계에서 파악된 목적과 기준 충족 여부를 기술하는 적절한 기록을 생성하여야 한다.

② 고장 발생 시 그 이유를 기록하여야 한다.

(라) 설치와 설계 간 편차의 영향 평가

① 실제 설치가 설계 정보를 따르지 않은 것으로 밝혀진 경우 그 편차를 능숙한 사람이 평가하여 안전에 미치는 영향을 결정하여야 한다.

② 편차가 안전에 영향을 미치지 않으면 설계 정보를 설치 상태로 갱신하고, 부정적인 영향을 미치면 설계 요건을 충족하기 위해 설치를 변경하여야 한다.

8.1.3 입증 요건

(1) SIS 입증 계획

SIS 안전수명주기 내내 SIS 입증 계획을 수립하여 입증에 필요한 모든 활동과 장치를 다음 사항을 포함하여 정의하여야 한다.

(가) 공정에 관련된 모든 운전모드와 장치의 입증

① 설정(Setting)과 조정(Adjustment)을 포함한 사용 준비

② 운전 개시, 자동, 수동, 반자동, 정상상태 운전

③ 재설정, 셧다운, 유지보수

④ SIS 안전수명주기의 이전 단계에서 파악된 다른 운전모드

(나) 입증에 사용할 절차, 수단, 기법과 SIS가 대비하고자 하는 위험사건의 리스크에 공장을 노출시키지 않고 입증 활동을 수행하는 방법

(다) 이 활동들의 수행 시기

(라) 이 활동의 책임을 맡은 사람, 부서, 조직과 입증 활동의 독립성 수준

(마) 입증 시 참조할 기준 정보(예: 원인결과도)

(바) 설치하거나 가용해야 할 장치와 설비

(2) AP 입증 계획

(가) 시운전 시작 전 각 공정 운전모드를 위해 입증할 필요가 있는 AP 함수의 파악

(나) 다음을 포함하는 입증 기술 전략

① 수동 및 자동 기법

② 정적 및 동적 기법

③ 해석적 및 통계적 기법

(다) 기술 전략에 따라 각 SIF가 지정된 안전요건과 지정된 SIL에 부합함을 확인하는 데 사용되는 수단과 절차

(라) 입증 활동을 수행하는 데 필요한 환경

(마) 응용프로그램

(바) 입증 달성의 합격/불합격 기준

(사) 입증 결과(특히 고장)를 평가하기 위한 정책과 절차

(아) 모든 문서의 정확성, 일관성, SIF의 추적가능성

(3) 계기 교정

(가) 측정의 정확도가 입증의 일환으로 요구되는 경우, 이 기능을 위해 사용되는 계기를 응용에 적합한 불확실성 내에서 추적가능한 표준 명세에 대비하여 교정하여야 한다.

(나) 이런 교정이 가능하지 않을 경우 대안의 방법을 사용하고 문서화하여야 한다.

(4) SIS 입증 활동

SIS와 관련 SIF의 입증은 SIS 입증 계획에 따라 다음과 같은 활동을 포함하여 수행하여야 한다.

(가) SIS가 SRS에서 파악한 대로 정상 및 비정상 공정 운전모드 하에서 성능증명 확인

(나) BPCS 및 다른 연결 시스템과의 부정적인 상호작용이 SIS의 적정 운전에 영향을 끼치지 않음을 확인

(다) SIS가 BPCS나 다른 시스템 또는 네트워크와 데이터 과부하와 같은 비정상 조건 하에서도 적절하게 교신할 수 있음을 확인

(라) SIS 설계 문서와 설치 시스템의 일치 확인

(마) SIF가 적법하지 않은 공정 변수값에 대해서도 지정한 대로 수행함을 확인

(바) 적정한 셧다운 순서가 활성화됨을 확인

(사) SIS가 적절한 경보와 운전 표시를 제공함을 확인

(아) SIS에 포함된 계산 기능이 예상된 범위 내의 값뿐만 아니라 한계값 또는 그 밖의 값에 대해서도 올바름을 확인

(자) SIS 리셋 기능이 SRS에서 정의된 대로 작동함을 확인

(차) 우회 기능이 올바르게 작동함을 확인

(카) 운전개시 최우선(Overrides)이 올바르게 작동함을 확인

(타) 수동 셧다운 시스템이 올바르게 운전됨을 확인

(파) 유지보수 절차서에 보증시험 정책이 문서화되어 있음을 확인

(하) 진단 경보기능이 요구대로 작동함을 확인

(거) 유틸리티 중단 시 SIS가 요구대로 작동하고, 유틸리티 회복 시 SIS가 원하는 상태로 복귀함을 확인

(너) SRS에 지정된 EMC 면역성이 달성되었음을 확인

(5) AP 입증사항

(가) 모든 지정된 AP 안전요건이 올바르게 수행되는지 여부

(나) AP가 SIS 결함 조건, 저하된 운전모드, SIS와 BPCS 간 인터페이스의 결함 조건에서 안전요건을 위협하지 않는지 여부

(다) AP가 사용되지 않는(즉, SRS에서 정의되지 않은) 소프트웨어 기능을 실행함으로써 안전요건을 위협하지 않는지 여부

(6) 입증 활동 기록

전체 SIS 입증 활동의 결과를 기록하여 다음 사항을 제공하는 문서를 작성하여야 한다.

(가) 사용한 SIS 입증 계획의 버전

(나) 시험 중인 SIF와 아울러 SIS 입증 계획 중 파악된 요건에 대한 구체적인 참조

(다) 사용한 도구, 장비 및 그 교정 데이터

(라) 각 시험의 결과

(마) 사용된 시험 명세서 버전

(바) 완료된 시험의 수용 기준

(사) 시험되는 SIS 하드웨어, AP, 다른 소프트웨어의 버전

(아) 예상 결과와 실제 결과 간 괴리와 이 괴리의 해결

(자) 괴리 발생 시 시험 계속 또는 변경요구 발의 여부에 관한 분석 및 결정

(7) 예상 결과와 실제 결과 간 괴리 분석

(가) 시험 결과를 예상 결과와 비교하여 확인하여야 함

(나) 양자 간 괴리를 분석하여 입증 작업을 계속할 것인지 또는 변경 요구를 발의하여 개발 수명주기의 초기 단계로 되돌아갈 것인지 여부에 관한 분석 및 결정을 입증 문서의 일부로 제공하여야 한다.

(8) SIS 입증 후 활동

SIS 입증 후 파악된 위험요인의 출현 전에 다음 활동을 수행하여야 한다.

(가) 모든 우회 기능을 정상 위치로 복귀

(나) 모든 공정 차단밸브를 공정 운전개시 요건과 절차에 따라 설정

(다) 모든 시험물질 제거

(라) 모든 시운전 최우선(Overrides)과 강제허용(Force permissives) 제거

8.2 SIS 운전 및 유지보수

8.2.1 목적

각 SIF에 대해 요구된 안전무결성을 유지하는 방식으로 SIS의 운전 및 유지보수를 보장하여야 한다.

8.2.2 요건

(1) 운전 및 유지보수 계획

SIS에 대한 운전 및 유지보수 계획을 수립하여 다음 사항을 제공하여야 한다.

(가) 정상 및 비정상 운전 활동

(나) 검사, 보증시험, 예방 및 고장 유지보수 활동

(다) 운전 및 유지보수에 사용할 절차, 수단, 기법

(라) 진단, 검사 또는 보증시험으로 파악된 결함과 고장에 대한 운전 상 대응

(마) 운전 및 유지보수 절차에의 부합 확인

(바) 이 활동들의 수행 시기

(사) 이 활동의 책임을 맡은 사람, 부서, 조직

(아) SIS 유지보수 계획

(2) 운전 및 유지보수 절차 개발

운전 및 유지보수 절차서를 관련 안전계획에 따라 개발하여 다음 사항을 제공 하여야 한다.

(가) SIS의 설계 시(As designed) 기능안전을 유지하기 위하여 수행해야 할 일상적 방법과 절차

(나) 보증시험의 질과 일관성 , 장치 교체 후 적절한 입증 수행을 보장하기 위하여

사용되는 절차

(다) 유지보수 또는 운전 중 불안전 상태를 예방하고 위험사건의 영향을 감축하기 위해 필요한 수단과 제약조건

(라) 진단장치 시험에 사용되는 방법과 절차

(마) SIS 고장 시 유지해야 할 정보와 SIS에 대한 요구율

(바) 요구율과 SIS 신뢰도 파라미터에 관련된 데이터 수집 절차

(사) SIS에 대한 시험 및 감사 결과를 보여주기 위해 유지해야 할 정보

(아) SIS 내에 결함 또는 고장 발생 시 이행해야 할 유지보수 절차

(3) 운전절차서와 보상 대책

(가) 운전절차서를 마련하여야 한다.

(나) SIS가 우호로 인해 무능화 또는 저하된 기간 중 지속적인 안전을 보장하는 보상대책을 관련 운전 한계와 함께 적용하여야 한다.

(다) 운전자에게 우회 전 및 우회 중 적용할 절차, 우회 제거 전 해야 할 일, 우회 상태의 최대 허용 시간에 관한 정보를 제공하고, 이 정보를 주기적으로 검토하여야 한다.

(4) SIS 우회 중 공정 운전

SIS가 우회 상태에 있을 때 공정 운전 지속은 위험요인 분석을 통해 보상대책이 마련되어 있고 적절한 리스크 감축을 제공한다는 것을 확인하였을 경우에만 허용하고, 그에 따라 운전절차를 개발하여야 한다.

(5) 운전 및 유지보수 진행

운전 및 유지보수는 관련 절차에 따라 진행하여야 한다.

(6) 운전자 훈련

운전자들에게 자신의 분야에서 SIS의 기능 및 운전에 관해 훈련시켜 다음 사항을 이해하도록 보장하여야 한다.

(가) SIS의 작동 방식

(나) SIS가 방호하려는 위험요인

(다) 모든 우회/최우선 스위치를 사용해야 할 상황과 그 사용법

(라) 수동 셧다운 스위치의 운전과 수동 개시 활동 및 이를 활성화시킬 시기

(마) 진단 경보 활성화 시 기대 사항

(바) 진단의 올바른 확인

(7) 우회 기록 및 승인

(가) 모든 우회 상태를 우회 일지에 기록하여야 한다.

(나) 모든 우회는 허가를 받은 후 표시하여야 한다.

(8) 유지보수 인력 훈련

유지보수 인력을 훈련시켜 SIS의 성능을 지속시켜야 한다.

(9) SIS의 예상 거동과 실제 거동 간 괴리 분석

(가) SIS의 예상 거동과 실제 거동 간 괴리를 분석하여 필요시 변경을 가함으로써 안전을 유지하여야 한다.

(나) 다음 사항을 감시(Monitoring)하여야 한다.

① 각 SIF에 대한 요구율

② 시스템에 대한 요구에 뒤따르는 조치

③ 정상운전, 검사, 시험 또는 SIF에 대한 요구 중 SIS의 일부를 이루는 장치의 고장과 고장률

④ 요구의 원인

⑤ 오연동의 원인 및 빈도

⑥ 보상 대책의 일부를 담당하는 장치의 고장

(10) 운전 및 유지보수 절차서 개정

다음과 같은 사유로 필요 시 운전 및 유지보수 절차서 개정이 필요할 수 있다.

(가) 기능 안전 감사

(나) SIS 시험

(다) 정상 또는 비정상 운전과 유지보수 사건에서 얻는 경험

(11) 보증시험 절차서

(가) 진단에 의해 검출되지 않는 위험한 고장을 발견하기 위하여 각 SIF에 대해 보증시험 절차서를 개발하여야 한다.

(나) 이 절차서는 수행해야 할 각 단계를 설명하여야 하며 다음 사항을 포함하여야 한다.

① 각 센서와 최종요소의 올바른 운전

② 올바른 논리 동작

③ 올바른 경보와 표시

(다) 시험해야 할 미검출 고장을 결정하기 위해 다음 방법을 사용할 수 있다.

① 결함수 검토

② FMEA

③ 신뢰도 중심 유지보수

(12) SIS 예비 부품

SIS 예비 부품을 파악하고 준비하여 교체 부품 부족으로 인한 우회기간을 최소화하여야 한다.

(13) 가정의 적합성

운전 및 유지보수 책임자는 H&RA, 할당 및 설계를 검토하여 가정의 적합성을 보장하여야 한다.

8.2.3 보증시험과 검사

(1) 보증시험

(가) 주기적 보증시험

문서화된 절차에 따른 주기적 보증시험을 수행하여 SIS가 SRS에 따라 운전되지 못하도록 방해하는 미검출 결함을 발견하여야 한다.

(나) 시험 대상

센서, 논리해결기 및 최종요소를 포함하는 전체 SIS에 대해 시험하여야 한다.

(다) 보증시험 일정

① 보증시험 일정은 SRS에 따라 수립하여야 한다.

② 운전환경에 설치된 SIS에 대해 7.7 항에 따른 PFDavg 또는 PFH 계산을 통해 SIF 보증시험 빈도를 결정하여야 한다.

(라) 결함 수리

① 보증시험 중 발견된 결함을 안전하고 시의 적절하게 수리하여야 한다.

② 수리 완료 후 보증시험을 반복하여야 한다.

(마) 검증 빈도 재평가

과거 시험 데이터, 공장 경험, 하드웨어 열화(Degradation)를 포함하는 다양한 인자에 의거하여 보증시험의 빈도를 재평가하여야 한다.

(바) AP 변경

① AP 변경 시 변경의 영향을 받는 SIF의 전체 입증 및 보증시험이 필요하다.

② 적절한 검토 및 변경에 대한 부분 시험을 수행하여 이 변경이 갱신된 안전요건에 따라 설계되고 올바르게 구현되었음을 보장하면 이 요건에 대한 예외가

허용된다.

(사) 보증시험 연기

보증시험의 연기를 검토하거나 심각한 지연을 방지하려면 적절한 관리절차를 적용하여야 한다.

(2) 검사

(가) 각 SIS를 주기적으로 육안 검사하여 허가받지 않은 변경 또는 관찰 가능한 악화 (예: 없어진 볼트, 벗겨진 전선, 부서진 도관 등)가 없음을 보장하여야 한다.

(나) 육안 검사는 설비의 기계적 무결성 입증을 위해 필요하며, 보증시험이 발견하지 못한 임박한 고장을 검출할 수 있다.

(3) 보증시험과 검사의 문서화

(가) 요구된 보증시험과 검사가 완료되었음을 증명하는 기록을 유지하여야 한다.

(나) 이 기록은 최소한 다음 정보를 포함하여야 한다.

① 수행된 시험 및 검사의 설명과 사용한 시험 절차의 파악

② 시험과 검사 날짜

③ 시험과 검사를 수행한 사람의 이름

④ 시험된 시스템의 일련 번호 또는 다른 고유 식별자

⑤ 시험과 검사의 결과(발견된 조건과 고장, 남겨진 조건 포함)

8.3 SIS 변경

8.3.1 목적

(1) SIS를 변경하기 전에 이 변경의 적정한 설계, 검토, 승인 및 문서화 보장

(2) SIS에 가한 변경에도 불구하고 요구된 SIS의 안전무결성이 유지됨을 보장

8.3.2 요건

(1) 허가 및 통제 절차

SIS를 변경하기 전에 변경의 허가 및 통제 절차를 마련하여야 한다.

(2) 절차 포함 사항

변경 허가 및 통제 절차는 영향을 받는 위험요인을 파악하고 수행해야 할 작업을 요청하는 명확한 방법을 포함하여야 한다.

(3) 변경 영향 분석

(가) SIS(AP 포함) 변경 수행 전 제안된 변경이 기능안전에 미치는 영향을 결정하기 위한 분석을 수행하여야 한다.

(나) 분석 결과 안전에 영향을 미칠 수 있을 경우 영향을 받는 SIS 수명주기 상의 첫 단계로 되돌아가야 한다.

(4) 변경 및 재입증 계획

변경 및 재입증에 대한 안전계획을 수립하고 그 계획에 따라 수행하여야 한다.

(5) 문서 갱신

변경에 의해 영향을 받는 모든 문서를 갱신하여야 한다.

(6) 변경 활동 개시 시기

변경 활동은 9.2.2.6.1 (9) 항에 따라 FSA를 완료하고 적절한 허가를 받은 후에만 개시하여야 한다.

(7) 변경 정보 유지

SIS의 모든 변경에 대해 다음 정보를 유지하여야 한다.

(가) 변경(Modification) 또는 변화(Change)의 설명

(나) 변화의 이유

(다) 영향을 받는 위험요인과 SIF의 파악

(라) 변경에 요구되는 모든 승인

(마) 변경이 적절히 구현되고 SIS가 요구대로 수행됨을 확인하기 위한 시험

(바) SIS 변경 활동의 상세 사항(예: 변경 일지 기록)

(사) 적절한 구성 이력

(아) 변화가 변경되지 않은 SIS 부분에 부정적인 영향을 미치지 않았음을 확인하기 위한 시험

(8) 변경 수행자

(가) 변경은 적절한 훈련을 받은 유자격자가 수행하여야 한다.

(나) 영향을 받거나 적절한 모든 사람에게 변경을 통보하고 이에 대한 훈련이 필요하다.

8.4 SIS 해체

8.4.1 목적

(1) SIS를 진행 중인 서비스로부터 해제하기 전 적절한 검토 수행 및 필요한 허가 획득

(2) 해체 활동 중 필요한 SIF의 운전 유지

8.4.2 요건

(1) 허가 및 통제 절차

SIS의 일부 또는 전부를 해체하기 전 허가 및 통제 절차를 마련하여야 한다.

(2) 절차 포함 사항

해체 허가 및 통제 절차는 영향을 받는 위험요인을 파악하고 수행해야 할 작업을 요청하는 명확한 방법을 포함하여야 한다.

(3) 해체 영향 분석

(가) 제안된 해체 활동이 기능안전에 미치는 영향에 관한 분석을 수행하여야 한다.

(나) 이 평가에 SIS 안전수명주기에 미치는 영향의 범위를 결정하기에 충분한 H&RA 갱신을 포함하고, 잇따르는 수명주기 단계를 재평가하여야 한다.

(다) 이 평가에서 다음 사항을 고려하여야 한다.

① 해체 활동 수행 중 기능안전

② SIS 해체가 인접한 장치와 설비의 운전에 미치는 영향

(4) 영향 분석 결과의 사용

영향 분석 결과의 재확인 및 재입증을 포함하여 IEC 61511 시리즈의 관련 요건을 재구현하기 위한 안전계획 수립 과정에서 사용하여야 한다.

(5) 해체 활동 개시 시기

해체 활동은 적절한 문서화와 허가 획득 후에 개시하여야 한다.

9. SIS 확인, 관리 및 평가, 수명주기 계획

9.1 SIS 확인

9.1.1 목적

검토, 분석 또는 시험을 통해 SIS의 각 수명주기 단계에서의 출력이 확인 계획에서 파악된 요건을 충족함을 보임.

9.1.2 요건

(1) 확인 계획

(가) SIS 안전수명주기 내내 확인 계획을 수행하여 응용프로그램을 포함한 단계별 필요 활동을 정의하여야 하다.

(나) 확인 계획에서는 다음 사항을 다루어야 한다.

① 확인 활동

② 확인에 사용할 절차, 수단, 기법과 도출된 권장책의 구현 및 해결

③ 확인 활동 시점

④ 확인 활동의 책임을 맡은 사람, 부서, 조직과 독립성 수준

⑤ 확인할 사항의 파악

⑥ 확인 대상이 되는 정보의 파악

⑦ 해당 단계의 요건 대비 출력의 적정성

⑧ 데이터의 정확성

⑨ 부합하지 않는 사항의 처리 방법

⑩ 도구와 자원 분석

⑪ SIS 구현의 완결성과 요건의 추적가능성

⑫ 문서의 가독성과 감사가능성

⑬ 설계의 시험가능성

(2) 확인 시험

시험이 포함된 확인 계획에서 다음 사항을 다루어야 한다.

(가) 응용프로그램, 하드웨어, 현장장치의 통합 전략

(나) 시험 셋업, 유형, 포함시킬 하드웨어, 응용프로그래밍, 프로그래밍 장치의 시험 범위 설명

(다) 시험 사례와 시험 데이터

(라) 수행할 시험 종류

(마) 도구, 하드웨어, 소프트웨어와 필요한 구성을 포함한 시험 환경

(바) 시험 결과를 평가할 시험 기준

(사) 시험 중 실패 시 수정 조치 절차

(아) 물리적 위치

(자) 외부 기능에의 의존성

(차) 적절한 인력

(카) 변경요소관리

(타) 불일치 사항의 처리

(3) 비안전 기능의 확인

안전기능과 통합된 비안전 기능에 의해 간섭이 발생하지 않는지 확인하여야 한다.

(4) 확인 수행

확인 계획에 따라 확인 활동을 수행하여야 한다.

(5) 변경 영향 분석

시험 중 변경요소에 대해 영양을 분석하여 영향을 받는 모든 성분과 필요한 재확인 활동을 결정하여야 한다.

(6) 확인 결과

확인과정의 결과와 아울러 시험의 목적 및 기준이 충족되었는지 여부를 제시하여야 한다.

9.2 SIS 기능안전 관리 및 평가

9.2.1 목적

기능 안전의 목적이 달성되도록 보장하는 데 필요한 관리 활동의 파악

9.2.2 요건

9.2.2.1 일반 사항

기능 안전을 달성하기 위한 정책과 전략을 그 평가 방법과 함께 파악한 후 조직 내에서 소통하여야 한다.

9.2.2.2 조직과 자원

(1) 책임 주체

SIS 안전수명주기의 각 단계를 수행하고 검토할 책임을 지는 사람, 부서, 조직을 파악하고 이들에게 할당된 책무를 알려주어야 한다.

(2) 능숙도(Competence)

(가) SIS 안전수명주기 활동에 참여하는 사람, 부서, 조직은 자신이 책임진 활동을 수행할 수 있도록 능숙하여야 한다.

(나) 능숙도를 고려해야 할 대상 항목은 다음과 같다.

① 응용 분야에 적합한 공학적 지식, 훈련 및 경험

② 사용된 기술에 적합한 공학적 지식, 훈련 및 경험

③ 센서와 최종요소에 적합한 공학적 지식, 훈련 및 경험

④ 안전공학 지식(예: 공정 안전 분석)

⑤ 기능안전에 관한 법령 요건 지식

⑥ SIS 안전수명주기 활동에서 자신의 역할에 맞는 적절한 관리 및 리더십 기량

⑦ 사건의 잠재적 영향 이해

⑧ SIF의 SIL

⑨ 응용 분야와 기술의 참신성과 복잡성

(3) 능숙도 관리

(가) SIS 수명주기에 관여하는 모든 사람의 능숙도 관리를 위한 절차를 마련하여야 한다.

(나) 개인의 수행 활동 대비 능숙도를 주기적으로 평가하여 문서화하고, 한 역할 내에서 담당자 변경 시 평가하여야 한다.

9.2.2.3 리스크 평가와 리스크 관리

6.1의 규정에 따라 위험요인을 파악하고, 리스크를 평가하며, 필요한 리스크 감축을 결정하여야 한다.

9.2.2.4 안전 계획

(1) 수행해야 할 활동과 이 활동의 수행 책임을 맡은 사람, 부서, 조직을 정의하는 안전계획을 수립하여야 한다.

(2) SIS 안전수명주기에서 개인 또는 조직이 수행하는 역할에 상응하는 상세 활동 수준으로 계획을 실행하여야 한다.

(3) 전체 SIS 수명주기에 걸쳐 필요한 만큼 계획을 갱신하여야 한다.

9.2.2.5 구현과 감시

(1) 권장책 이행

다음 활동에서 제안된 SIS 관련 권장책의 신속한 이행 및 만족스러운 해결을 보장하기 위한 절차를 구현하여야 한다.

(가) 위험요인 분석 및 리스크 평가

(나) 확인(Verification) 활동

(다) 입증(Validation) 활동

(라) 기능안전평가(FSA)

(마) 기능안전 감사

(바) 봉쇄상실 사고 후(Post-incident) 및 사고 후(Post-accident) 활동

(2) 공급자 의무

(가) 한 단계 이상의 SIS 안전수명주기에 총괄책임이 있는 조직에 제품 또는 서비스를 제공하는 공급자는 그 조직이 지정한 제품 또는 서비스를 인계하고 품질관리 시스템과 그 적절성을 입증할 수 있는 절차를 마련하여야 한다.

(나) 이 공급자가 제품 또는 서비스에 대해 기능안전에 관한 주장을 하려면 기능안전 관리시스템과 그 적절성을 입증할 수 있는 절차를 마련하여야 한다.

(3) SIS 성능 평가

다음 사항을 위해 SIS의 안전요건 대비 성능을 평가하는 절차를 구현하여야 한다.

(가) 안전을 위협할 수 있는 시스템 고장의 파악 및 방지

(나) SIS의 신뢰도 파라미터가 설계 과정의 가정값과 일치하는지 감시 및 평가

(다) 고장률이 설계과정 중의 가정값보다 클 때 취해야 할 수정 조치의 정의

(라) 실제 운전 중 SIF에 대한 요구율과 SIL 요건 결정을 위한 리스크 평가 과정에서의 가정값의 비교

(4) 기존 SIS

IEC 61511 이전의 코드, 표준, 또는 관행에 따라 설계 및 구성된 기존 SIS에 대해서 그 장치가 안전한 방식으로 설계, 유지보수, 검사, 시험 및 운전되는지 결정하여야 한다.

9.2.2.6 평가, 감사 및 개정

9.2.2.6.1 기능안전평가

(1) FSA 개요

(가) SIS의 각 SIF에 의해 달성되는 기능안전 및 안전무결성에 관한 판단을 내릴 수 있도록 FSA 절차를 정의하고 실행하여야 한다.

(나) 이 절차를 통해 특정 응용 분야에 필요한 기술/응용/운전의 전문지식을 갖춘 FSA팀을 선임하여야 한다.

(2) FSA팀 구성

FSA팀에 프로젝트 설계 또는 SIS의 운전 및 유지보수에 관여하지 않은 능숙한 상위직(senior) 인사를 적어도 1명 포함시켜야 한다.

(3) FSA 계획 시 고려 사항

(가) FSA의 범위

(나) FSA 참여 멤버

(다) FSA팀의 기량, 책임 및 권한

(라) FSA 활동의 결과로서 생성될 정보

(마) FSA에 관여할 다른 안전 당사자

(바) FSA 활동 완료에 필요한 자원

(사) FSA팀의 독립성 수준

(아) 변경 후 FSA 재입증 방법

(4) 평가 대상 수명주기 단계

(가) FSA팀은 현재의 평가 이전의 안전수명주기의 모든 단계 중 과거의 FSA에서 다루지 않았던 단계에서 수행된 작업을 검토하여야 한다.

(나) 과거에 FSA가 수행되었다면 그때의 결론과 권장책을 고려하여야 한다.

(다) FSA 활동을 수행해야 할 SIS 안전수명주기의 단계는 안전계획 과정에서 파악하여야 하며, 일반적으로 다음의 단계(Stages)를 포함하여야 한다.

① H&RA를 통해 필요한 방호계층이 파악되고 SRS가 개발된 후

② SIS 설계 후

③ SIS의 설치, 시운전, 최종 입증이 완료되고 운전 및 유지보수 절차가 개발된 후

④ 운전 및 유지보수에서 경험을 쌓은 후

⑤ 변경 후 SIS 해체 전

(5) FSA 착수 전 확인 사항

FSA팀은 위험요인이 제기되기 전에 기능안전평가를 시도하여 다음 사항을 확인하여야 한다.

(가) H&RA 수행 여부

(나) H&RA에서 제안된 SIS 관련 권장책이 구현 또는 해결 여부

(다) 프로젝트 설계 변경 절차가 마련되어 있고 적절한 구현 여부

(라) 이전의 FSA에서 제안된 권장책 해결 여부

(마) SIS는 SRS에 따라 설계, 시공, 설치되었으며 차이점의 파악 및 해결 여부

(바) SIS와 관련된 안전, 운전, 유지보수 및 비상대응 절차 마련 여부

(사) SIS 입증 계획이 적절하고 입증 활동이 완료되었는지 여부

(아) 근로자 훈련이 완료되었고 SIS에 관한 적절한 정보가 운전 및 유지보수 인력에게 제공되었는지 여부

(자) 추가적인 FSA 구현 계획 또는 전략이 마련되어 있는지 여부

(6) 도구 평가

설계, 개발, 생산 도구가 SIS 안전수명주기 활동에 사용될 때 도구 자체를 평가하여 SIS에 어떠한 부정적 영향도 끼치지 않음을 입증하거나 도구의 출력을 확인(Verification) 절차에 따라 확인(Confirm)하여야 한다.

(7) FSA 결과와 권장책

FSA 결과와 함께 권장책을 도출하여야 한다.

(8) 가용 정보

FSA팀의 요구 시 모든 관련 정보를 제공하여야 한다.

(9) 변경요소에 대한 FSA

제안된 변경에 대해 실시한 영향 분석을 검토하고 변경 작업이 IEC 61511에 맞게 수행되었는지 확인하여야 한다.

(10) 주기적인 FSA 수행

운전 및 유지보수 단계 중 FSA를 주기적으로 수행하여 운전 및 유지보수가 설계 시의 가정에 따라 실시되고, 안전 관리 및 확인에 관한 IEC 61511의 요건이 충족되고 있음을 보장하여야 한다.

9.2.2.6.2 기능안전 감사와 개정

(1) 감사 목적

정보 문서와 기록을 검토하여 기능안전 관리시스템이 마련되어 최신으로 유지 및 이행되고 있는지 결정하고, 간극 발견 시 개선책을 제안한다.

(2) 감사 대상

모든 안전수명주기 활동에서 필요하다고 파악된 모든 절차를 감사하여야 한다.

(3) 감사 주체와 절차

(가) 기능안전 감사는 감사할 SIS의 업무를 담당하지 않은 독립적인 사람이 수행하

여야 한다.

(나) 다음 요건에 맞는 절차를 정의하고 실행하여야 한다.

① 기능안전 감사 활동의 빈도

② SIS 업무를 수행하는 사람, 부서, 조직과 기능안전 감사 활동을 수행하는 사람, 부서, 조직 간의 독립성 정도

③ 활동의 기록 및 이행

(4) 변경요소관리 절차

(가) 동종 간 교체 이외의 SIS 변경을 개시, 문서화, 검토, 구현 및 승인하는 변경관리 절차를 마련하여야 한다.

(나) SIS 요건에 영양을 미치는 변화를 파악하는 변경관리 절차를 마련하여야 한다.

9.2.2.7 SIS 구성관리(Configuration management)

(5) SIS 구성관리 절차

SIS 안전수명주기의 임의 단계 중 SIS의 구성관리 절차를 마련하여야 한다.

(6) SIS 소프트웨어 등의 개정 통제

응용프로그램의 개발 및 실행에 쓰이는 SIS 소프트웨어, 하드웨어 및 절차서를 구성관리 대상으로 삼아 개정 통제 하에 유지하여야 한다.

9.3 안전수명주기 구조와 계획

9.3.1 목적

(1) SIS 안전수명주기 활동의 단계 정의 및 요건 확립

(2) SIS 안전수명주기의 기술적 활동 정의 및 구성

(3) SIS가 안전요건을 충족하도록 만드는 적절한 계획의 수립 보장

9.3.2 요건

(1) SIS 수명주기 정의

(가) IEC 61511 시리즈의 요건을 반영한 SIS와 응용프로그램의 안전수명주기를 안

전계획 과정에서 정의하여야 한다.

(나) 각 단계에서 책임 계층을 파악하여 관련 당사자(예: 공급자, 시스템 통합자, 최종 사용자)에게 전달하여 모든 사람이 각자의 책임을 인지토록 하여야 한다.

(2) 수명주기 각 단계별 정의

SIS와 응용프로그램 안전수명주기의 각 단계를 입력/출력/확인활동 면에서 정의하여야 한다(<표 1>과 <표 2> 참조).

(3) 안전 계획

모든 SIS 안전수명주기 단계에서 다음 사항을 위한 활동/기준/기법/수단/절차/ 책임자를 정의하는 계획을 수립하여야 한다.

(가) 모든 관련된 공정 모드에 대해 SIS 안전요건 달성 보장

(나) SIS의 적정 설치 및 시운전 보장

(다) 설치 후 SIF의 안전무결성 보장

(라) 운전 중 안전무결성 유지(예: 보증시험, 고장 분석)

(마) SIS에 대한 유지보수 활동 중 공정 위험요인 관리

(4) 변경 시 요건

안전수명주기의 어떤 단계에서 그 이전 단계와 관련하여 변경이 필요하면 그 이전 단계와 잇따르는 단계들에 대해 재조사하여 필요 시 변경한 후 재확인하여야 한다.

(5) AP의 방법, 기법, 도구

(가) 응용프로그램의 방법, 기법, 도구는 각 수명주기 단계에서 7.8.6 (2)항에 따라 적용하여야 한다.

(나) 이때 응용프로그램의 규모, 복잡성 정도, 구현할 SIF의 SIL, 설계도구의 표준화 정도, 언어 유형에 따라 방법과 기법을 선정하여야 한다.

(6) 확인

안전계획을 수립한 각 SIS의 안전수명주기 단계는 9.1 항에 따라 확인하고, 10 항에 따라 결과를 제시하여야 한다.

10. 정보 및 문서화 요건

10.1 목적

다음 사항을 위해 필요한 정보의 가용성 및 문서화 보장

(1) 모든 SIS 안전수명주기 단계의 효과적 수행

(2) 확인, 입증 및 FSA 활동의 효과적 수행

10.2 요건

(1) 독자와 정보 목록

IEC 61511 시리즈에서 요구되는 다음 정보를 이 시리즈의 요건을 구현하는 사람들에게 제공하여야 한다.

(가) H&RA 결과

(나) 방호계층 할당

(다) 무결성 요건 결정 시 사용한 가정

(라) SRS

(마) 응용 논리

(바) 설계 문서

(사) 변경 정보 또는 문서

(아) 확인 및 입증 기록

(자) 시운전 및 SIS 입증 절차

(차) SIS 운전 절차

(카) SIS 유지보수 절차

(타) 보증시험 절차

(파) 평가 및 감사 결과

(2) 정보 요건

(가) 시스템 또는 장치의 설치와 사용 설명

(나) 정확하고 최신으로 갱신됨

(다) 이해하기 쉬움

(라) 의도된 목적에 적합함

(마) 접근, 유지, 편집 가능한 형태로 사용가능함

(3) 고유 식별자

문서는 다른 부분을 참조할 수 있도록 고유 식별자를 가져야 한다.

(4) 문서 명칭

문서는 정보 유형을 나타내는 명칭을 가져야 한다.

(5) 추적가능성

문서는 H&RA를 포함하여 이 표준에서 제기되는 기능 및 무결성 요건으로 추적가능 하여야 한다.

(6) 개정 지표

문서는 다른 버전의 정보를 식별할 수 있도록 개정 지표(Revision index)를 가져야 한다.

(7) 문서 구조

문서는 관련 정보를 검색할 수 있도록 구조화되고, 최신 개정판을 식별할 수 있어야 한다.

(8) 문서 관리

모든 관련 문서를 개정, 수정, 검토, 승인하고 적절한 정보 통제 방식에 따라 관리하여야 한다.

(9) 최신 문서 유지

다음 사항에 관련된 최신 문서를 유지하여야 한다.

(가) H&RA 결과와 관련 가정

(나) SIF에 사용된 장치와 그 안전 요건

(다) 기능안전 유지의 책임을 맡은 조직

(라) SIS 기능안전을 달성 및 유지하는 데 필요한 절차

(마) 8.3.2 (7)항에서 정의된 변경 정보

(바) 안전매뉴얼

(사) 설계, 구현, 시험과 입증

[부록 1]

안전계장시스템(SIS)관련 표준 개요

1. ISA S84.01

공정산업을 위한 안전계장시스템 적용

(Application of Safety Instrumented Systems for the Process Industries)

(1) 1996년 최초로 제정되어 공정산업에서 SIS의 설계/운전/유지보수/시험 등 수명주기 활동을 위한 성능 표준을 규정하고, 그 수치적 기준점으로서 안전무결성등급(SIL)을 확립하였으나 SIL3로 한정되며 SIL4 조항은 미규정

(2) 1997년 미국 ANSI 표준으로 채택되고, OSHA가 훌륭한 공학적 관행으로 인정하고 있으나 그 자체가 강제 규정은 아니다.

(3) 2002년 이후, ISA TR84.02 등의 다양한 보충판 및 개정판이 발간되어 왔으나, 기본적으로 IEC 61511을 채택하여 ANSI/ISA 84.00.01-2004로 정립되어 있다.

2. IEC 61508

전기/전자/프로그래밍 가능한 전자 안전관련 시스템의 기능안전

(Functional safety of electrical/electronic/programmable electronic safety-related systems)

(1) 1999년에 제정되어 넓은 산업 분야에서 SIS 구현을 위한 일반적 요건을 다루는 국제 표준으로서 다음 7개 부분으로 구성된다.

(가) Part 1: General requirements

(나) Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

(다) Part 3: Software requirements

(라) Part 4: Definitions and abbreviations

(마) Part 5: Examples of methods for the determination of safety integrity levels

(바) Part 6: Guidelines on the application of parts 2 and 3

(사) Part 7: Overview of techniques and measures

(2) IEC 61508은 ISA S84.01에 비해 다음과 같은 차이점이 있다.

(가) SIL4 조항이 있으며, SIL 증가에 따라 더욱 복잡한 하드웨어 및 소프트웨어 요건을 규정

(나) 비 계장(Non-instrumented) 리스크 감축 설비와 관련된 요건을 지정

(다) ISO 9000시리즈의 품질시스템 또는 그와 동등한 시스템 사용을 요구

(라) "안전 계획(Safety plan)" 사용을 요구(ISA S84.01은 29 CFR 1910.119 규정에 맞는 문서화 요구)

(마) 관리시스템과 관련된 많은 사안을 요구(미국에서 공정안전관리시스템 (PSM)으로 다루고 있음)

(바) ISA S84.01과는 약간 다른 용어 및 약어 사용

3. IEC 61511

공정산업분야를 위한 안전계장시스템 - 기능안전

(Functional safety — Safety instrumented systems for the process industry sector)

(1) 2003년에 제정되어 IEC 61508의 기본체계 내에서 공정산업에 적용 가능한 SIS 요건을 다루는 국제 표준으로서 다음 3개 부분으로 이루어져 있다.

(가) Part 1: Framework, definitions, system, hardware and application programming requirements

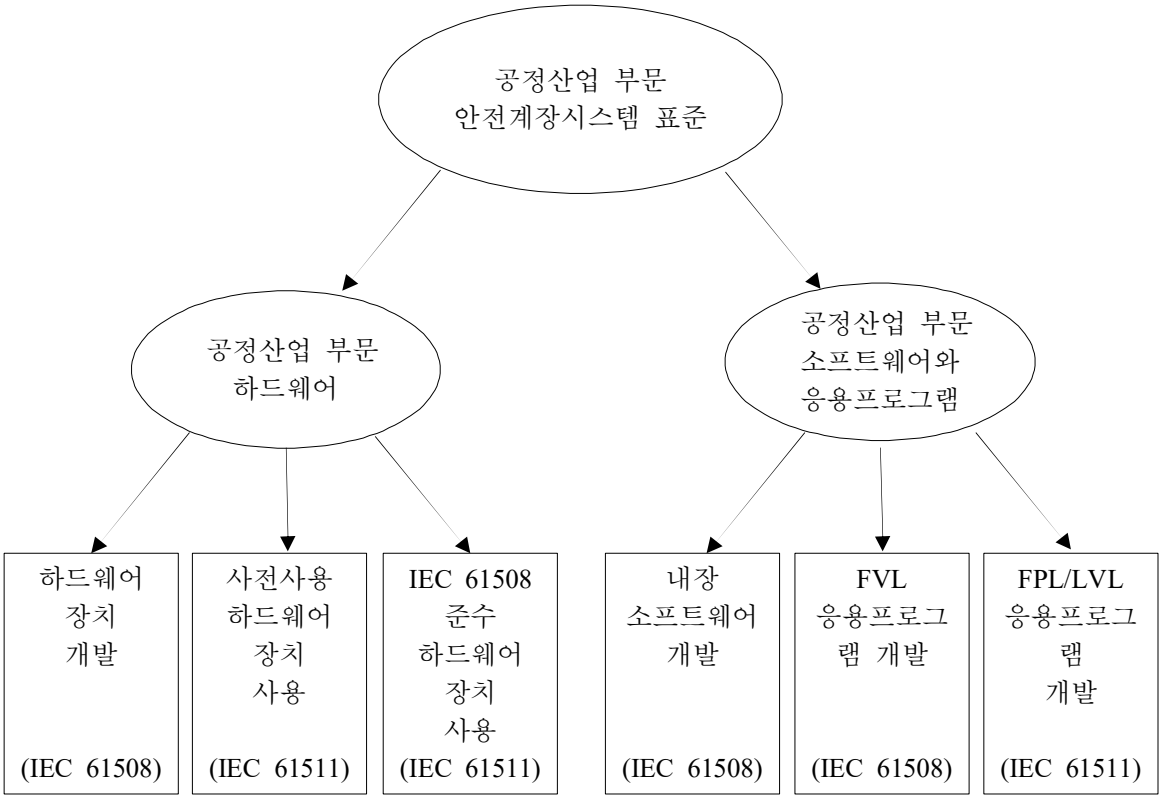
(나) Part 2: Guidelines for the application of IEC 61511-1

(다) Part 3: Guidance for the determination of the required safety integrity levels

(2) 공정산업 부문에서 IEC 61508과 IEC 61511의 관계

(가) 기본적으로 IEC 61508은 SIS 장치의 제조자 또는 공급자에게 적용되는 반면 IEC 61511은 SIS 설계자, 통합자(Integrators) 및 사용자에게 적용되나, IEC 61511에서 지시가 있을 경우 설계자, 통합자, 사용자도 IEC 61508을 사용하여야 한다.

(나) 하드웨어와 소프트웨어 또는 응용프로그램과 관련된 양자 간의 구체적인 차이는 [그림 6]과 같다.



[그림 6] IEC 61511과 IEC 61508의 관계