IEC 61508

Functional safety of electrical/electronic/programmable electronic safety related system

김의섭

목차

- Introduction
- IEC 61508 parts
- 결론

INTRODUCTION

Functional Safety – Driven by Accidents

배경

- **안전기능**은 점점 더 전기, 전자 또는 프로그램 가능한 전자장치 시스템(**E/E/PE**)에 의해 수행되고 있다.
  - 컴퓨터 기반 시스템 (PES) 은 모든 응용 부문에서 안전과 무관한 기능을 수행하는 데 이용되고 있지만, 점차 안전기능에도 이용되고 있는 추세

배경

- 위험측 고장
  - 시스템, 하드웨어 또는 소프트웨어의 잘못된 명세
  - 안전 요구사항 명세에서 누락(예를 들면, 서로 다른 모드들로 운영되는 동안에 관련된 모든 안전기능이 나타나지 않는 고장)
  - 하드웨어 우발 고장 메커니즘
  - 소프트웨어 오류
  - 공통 원인 고장
  - 인적 오류
  - 환경적인 영향(예를 들면, 전자기, 온도, 기계적인 현상들)
  - 공급 시스템 전압 불안정(예를 들면, 공급 손실, 전압 감소, 공급의 재연결)

배경

- 이러한 시스템은 보통 **복잡하고**, 모든 고장 모드를 완전하게 결정하거나 가능한 **모든 행위를 시험하는 것을 현실적으로 불가능**하게 만든다.
  - 시험은 여전히 필수적으로 수행해야 하지만, **안전 성능을 예측 하는 것은 어렵다.**

- 기능안전성 달성을 하기 위해서는 **위험측 고장을 방지**하거나, **고장이 발생할 때 그것을 제어**하는 방식으로 **시스템을 설계**한다는 것이다.

배경

- Middle-to-late 1980s: Work on safety-related systems in the International Electrotechnical Committee, SC 65A WG9 (Software) and WG10 (Systems)
- November 1991: Publication of ‘Software for Computers in the Application of Industrial Safety-related Systems’

  IEC SC 65A WG9 Draft Document
- January 1992: Publication of ‘Functional Safety of Electrical/Electronic/Programmable Electronic Systems; General Aspects: Part 1, General Requirements’

  IEC SC 65A WG10 Draft Document

배경

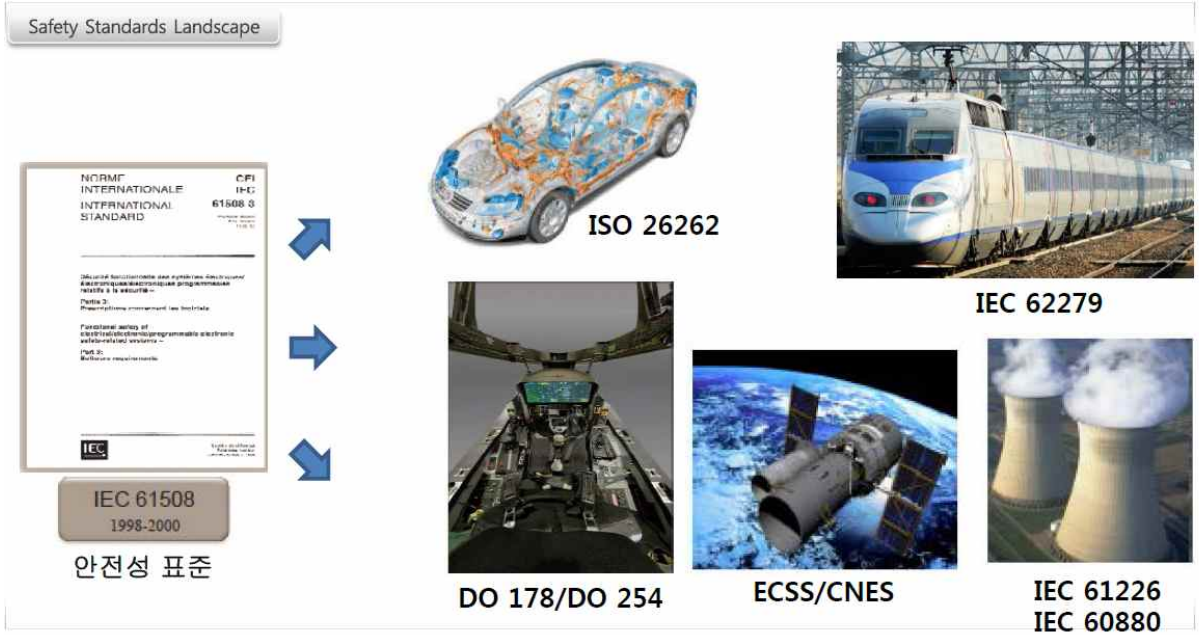
- June 1995: Publication of ‘IEC 1508 — Functional Safety: safety-related systems’ in 7 parts

  Prepared by Working Groups 9 and 10 of SC 65A’
- **December 1997: Publication of 'IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems'**

  Prepared by sub-committee 65A: System aspects
- 1998 - 2000: All seven parts voted to status of standard
- 2010: Publication of Edition 2, after several years of “maintenance”

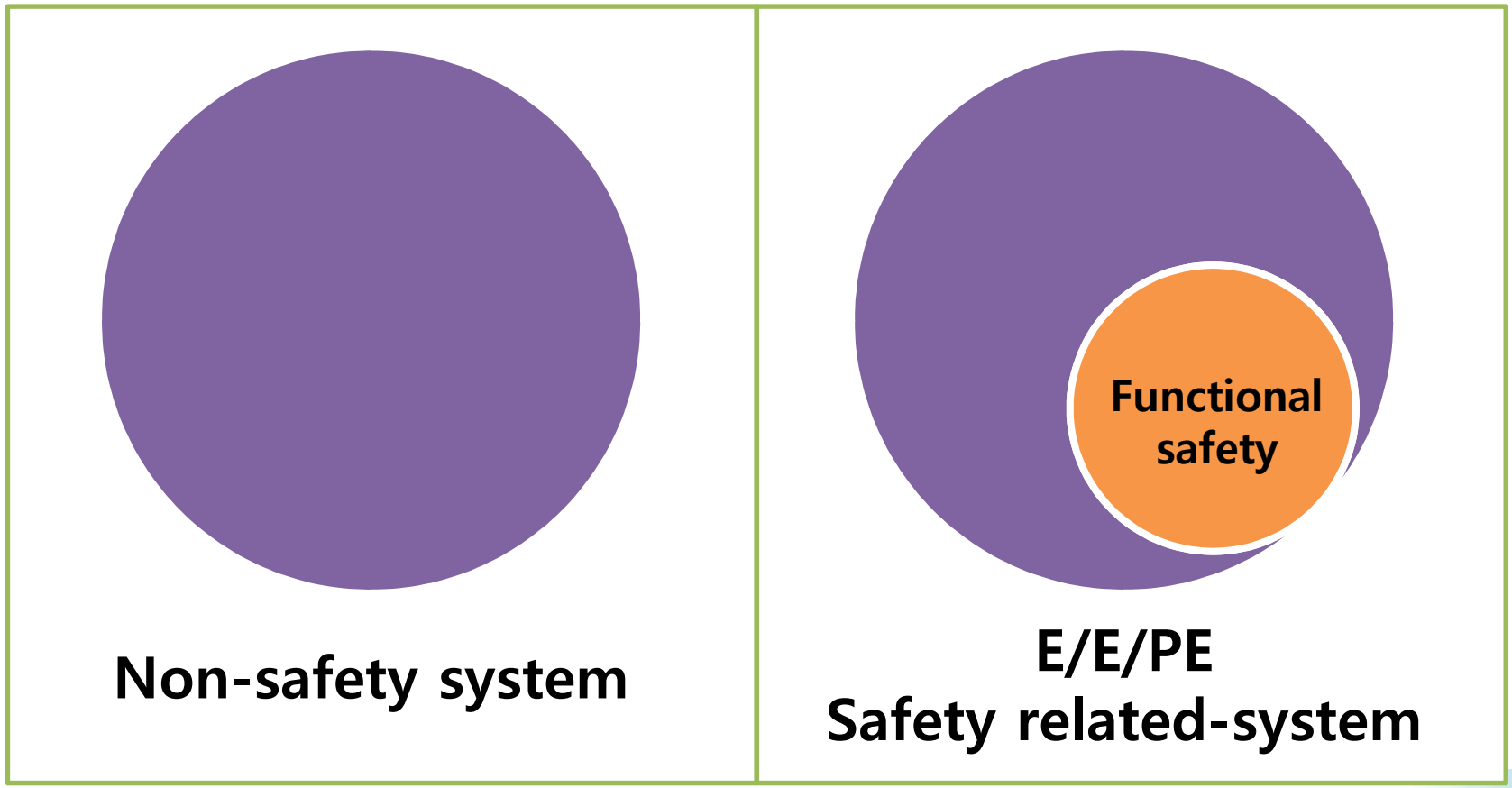
개요

- **IEC 61508**은 산업에 적용되는 규칙의 **국제표준**이다.
- 명칭은 **전기/전자/프로그램 가능한 전자 안전 관리 시스템의 기능 안전** 이다.
- **IEC 61508**은 모든 종류의 산업에 적용 가능한 기본적인 기능 안전 표준이 될 의도로 작성되었다.



개요

- IEC 61508 : **Functional safety** of electrical/electronic/ programmable electronic **safety related-system**



범위

- **E/E/PE** 안전관련 시스템

- EX)
  - 위해한 화학 장치 공장에서 응급 가동 중단 시스템
  - 크레인 안전 하중 지시계(Clane safe load indicator)
  - 철도 신호 시스템
  - 기계 가드 연동 및 비상정지 시스템
  - 속도 제한을 위한 보호용 가변 속도 모터 드라이브
  - 의료용 방사선 기계 노출량 제어 및 연동을 실시하는 시스템
  - 동적 포지셔닝(해양시설 접근 시 선박 움직임 제어)
  - 항공 비행 표면 제어의 플라이 바이 와이어 작동
  - 자동차 표시등, 브레이크 잠김 방지 및 엔진 관리 시스템
  - 네트워크 활성화 장치 설비의 원격 모니터링, 작동 또는 프로그래밍
  - 안전에 영향을 미치는 잘못된 결과가 있는 경우 정보기반 의사결정 지원 도구
  - 원자력발전소 제어 시스템

Functional Safety

- Safety
  - This is **freedom from unacceptable risk** of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

- Functional Safety
  - is **part of the overall safety** that depends on a system or equipment operating correctly in response to its inputs.

- 예를 들어 Over-themperatur protection device의 경우
  - 온도 sensor를 사용해서 모터가 과열되기 전에 감속시키기는 보호장치가 functional safety이다.
- 하지만
  - 고온을 버티기 위해 어떤 특별한 절연체를 쓰는 것은 functional safety가 아니다.

- Functional safety
  - 위험원을 다루는 하나의 방법일 뿐이고, 설계를 통해 고유의 안전을 확보하는 것과 같이, **위험원을 제거하거나 감소시키는 방법**이 가장 중요한 것이다.

Functional safety 을 달성하기 위해..

- 1. Safety function requirement (기능이 무엇을 수행한다.)
  - 위협원 검출
  - **Hazard analysis**
- 2. Safety integrity requirement (안전기능이 만족스럽게 수행될 가능성)
  - Risk assessment
  - **Safety integrity levels (SILs)**
  - 높은 안전무결성수준일 수록 위험측 고장 가능성이 낮아진다.
- 3. **Safety lifecycle**

SIL

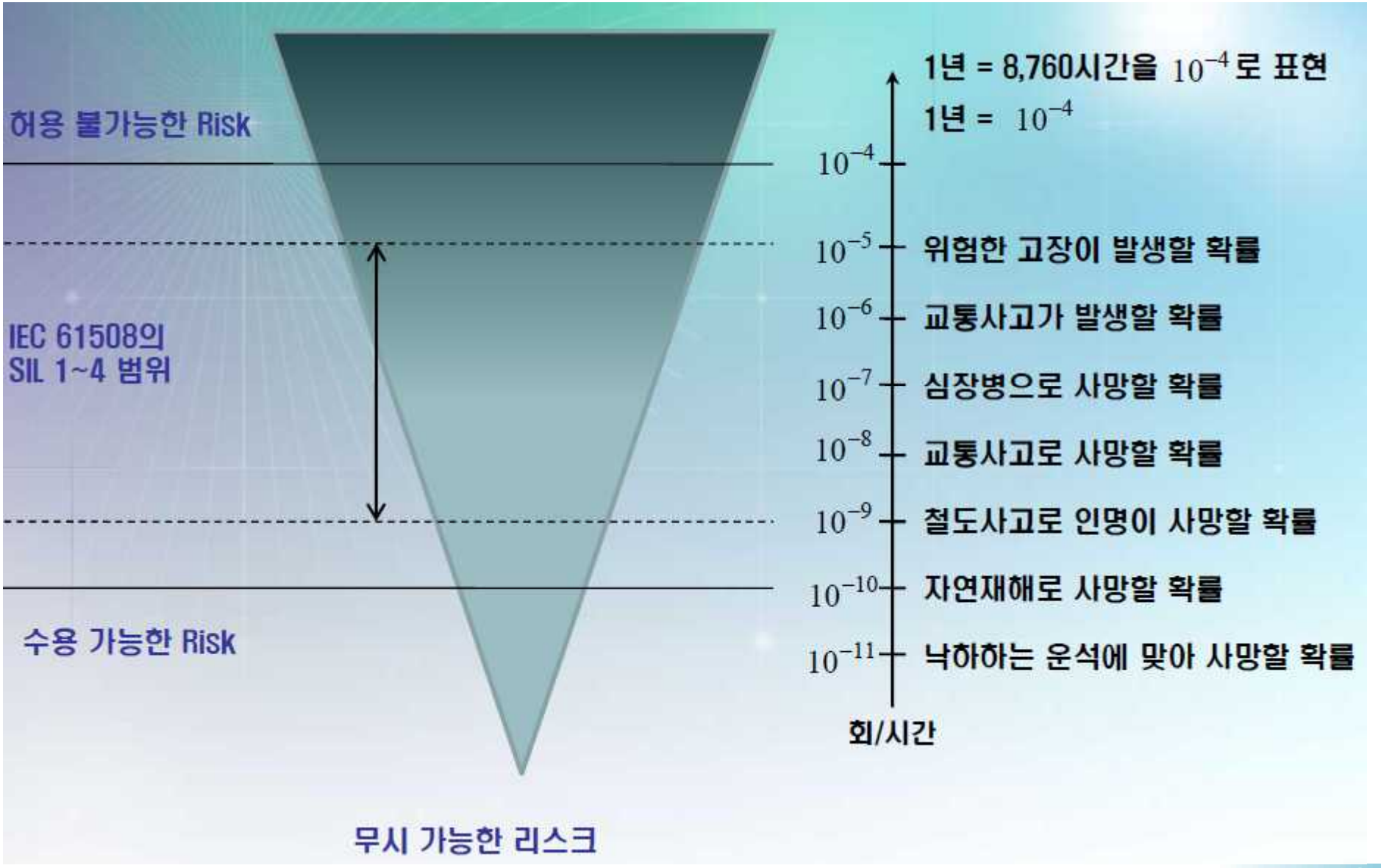
- **Safety integrity levels (SILs)**
  - 주어진 모든 조건하에 있는 안전관련 시스템이 주어진 시간 내에 요구되는 안전기능을 만족스럽게 수행할 수 있는 확률로 정의된다

Safety-Integrity Level (SIL)	High demand rate (dangerous failures/hr)	Low demand rate (Probability of failure on demand)
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

High demand rate : 안전관련 기능에 대한 사용이 계속적으로 발생시 적용(예: 센서류)

Low demand rate : 안전관련 기능에 대한 사용 빈도수가 대략 년 1회 미만 발생시 적용(예: 에어백)

SIL


허용 불가능한 Risk
IEC 61508의
SIL 1~4 범위
수용 가능한 Risk
무시 가능한 리스크
1년 = 8,760시간을 10^{-4}로 표현
1년 = 10^{-4}
10^{-4}
10^{-5} 위험한 고장이 발생할 확률
10^{-6} 교통사고가 발생할 확률
10^{-7} 심장병으로 사망할 확률
10^{-8} 교통사고로 사망할 확률
10^{-9} 철도사고로 인명이 사망할 확률
10^{-10} 자연재해로 사망할 확률
10^{-11} 낙하하는 운석에 맞아 사망할 확률
회/시간

SIL

HOME > 뉴스 > e비즈*솔루션 > SI

포스코ICT, 스크린도어 SIL 레벨4 등급 인증

2013년 02월 07일 17:45:58 / 이상일 기자 2401@ddaily.co.kr

[디지털데일리 이상일기자] 포스코ICT(사장 허남석)가 개발한 철도시스템의 안정성과 신뢰성이 국제적인 수준에 이르렀다는 인증을 받아 해외 시장 진출이 더욱 가속화될 전망이다.

포스코ICT는 7일, 국내 최초로 지하철 스크린도어(PSD) 제어부에 대해 SIL 레벨4 등급 인증을 받았다고 밝혔다. 스크린도어는 지하철 승강장 연단에 고정벽과 자동문을 설치해 승강장과 철도 선로를 차단하는 시스템으로 크게 제어부(Control System)와 도어부(Motorized Door)로 분류된다.

이번에 포스코ICT가 인증을 받은 SIL(Safety Integrity Level)은 철도를 비롯해 원자력발전소, 의학기기 등과 같은 산업장비의 전자·전기·신호 분야의 안전성과 신뢰성을 정량적으로 측정해 등급을 매기는 것으로 레벨4가 최고 등급이다.

지난 2010년부터 브라질 상파울로 지하철 2,3,4호선에 자사의 PSD 시스템을 공급하고 관련 시스템을 구축하는 사업을 진행하고 있는 포스코ICT는 브라질 시장 진출 초기 단계부터 SIL 3등급 수준의 제품을 개발하는 등 한발 앞선 준비를 해왔다고 설명했다.

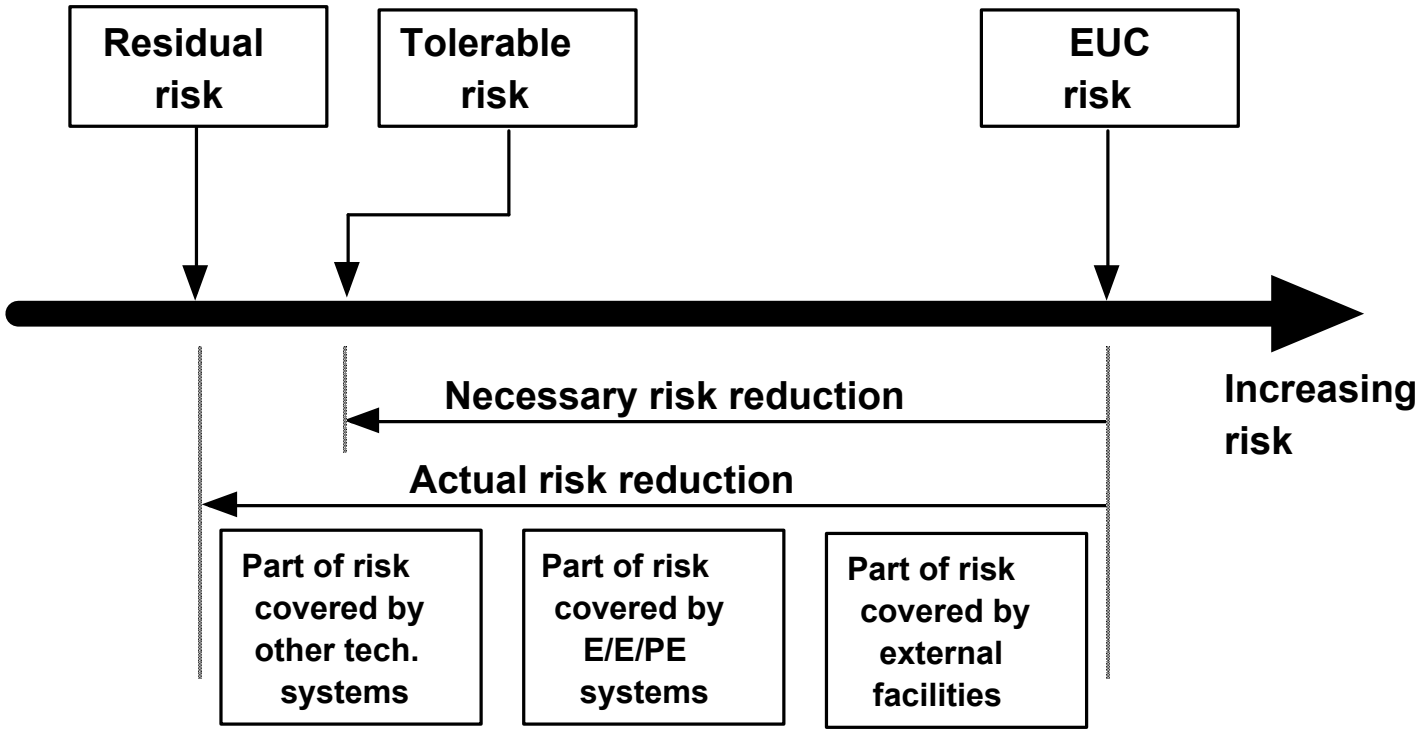
미국이나 유럽에서는 철도를 비롯한 관련 산업분야 장비에 대해 SIL 인증을 강력하게 요구하고, 비교적 저성장 시장인 아시아권에서도 인증획득을 요구하는 상황이기 때문에 SIL 인증이 이제 해외 시장 진출을 위한 핵심적인 자격으로 인식되고 있다.

이번 인증 획득을 통해 포스코ICT는 국제 규격을 적용한 시스템 개발 및 검증 역량을 확보하고, 해외 철도사업에서도 보다 유리한 입지를 점할 수 있게 될 전망이다.

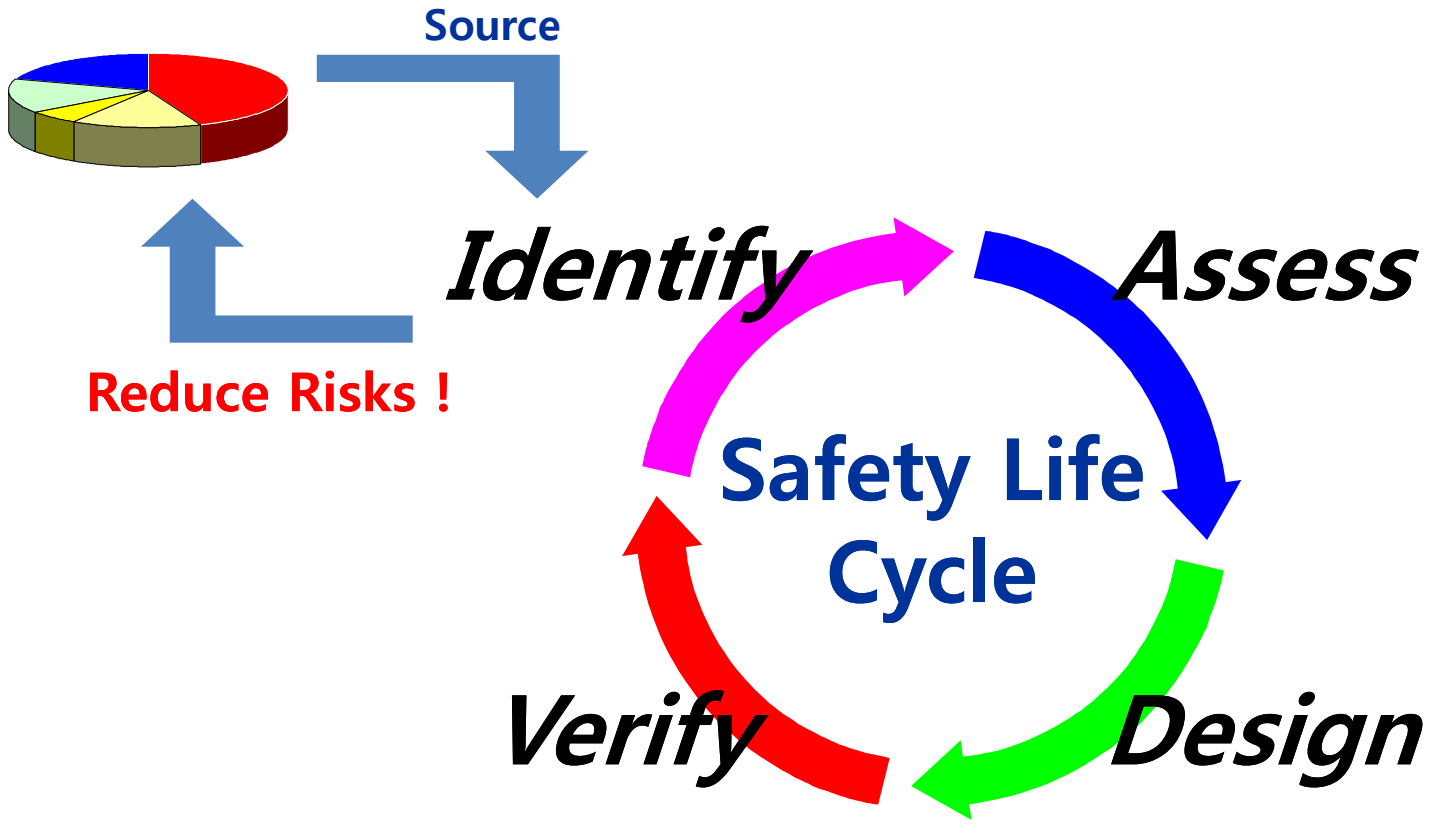
포스코ICT 관계자는 "철도 산업에서 안정성을 검증하는 기준인 SIL 인증 획득이 전 세계적으로 강력하게 요구되고 있으며, 국내에서도 SIL 인증에 대한 관심이 높아지고 있는 상황"이라며 "이번 인증 획득을 통해 입증된 시스템의 안정성 및 신뢰성을 기반으로 해외 철도시장 공략에 박차를 가할 계획" 이라고 말했다.

<이상일 기자>2401@ddaily.co.kr

Risk reduction



Safety lifecycle



Safety lifecycle

Understand the functional goals and design

⇓

Identify the hazards

⇓

Analyse the hazards

⇓

Determine and assess the risks posed by the hazards

⇓

Specify the risk reduction measures and their SILs

⇓

Define the required safety functions (and their SILs)

⇓

Carry out safety validation

⇓

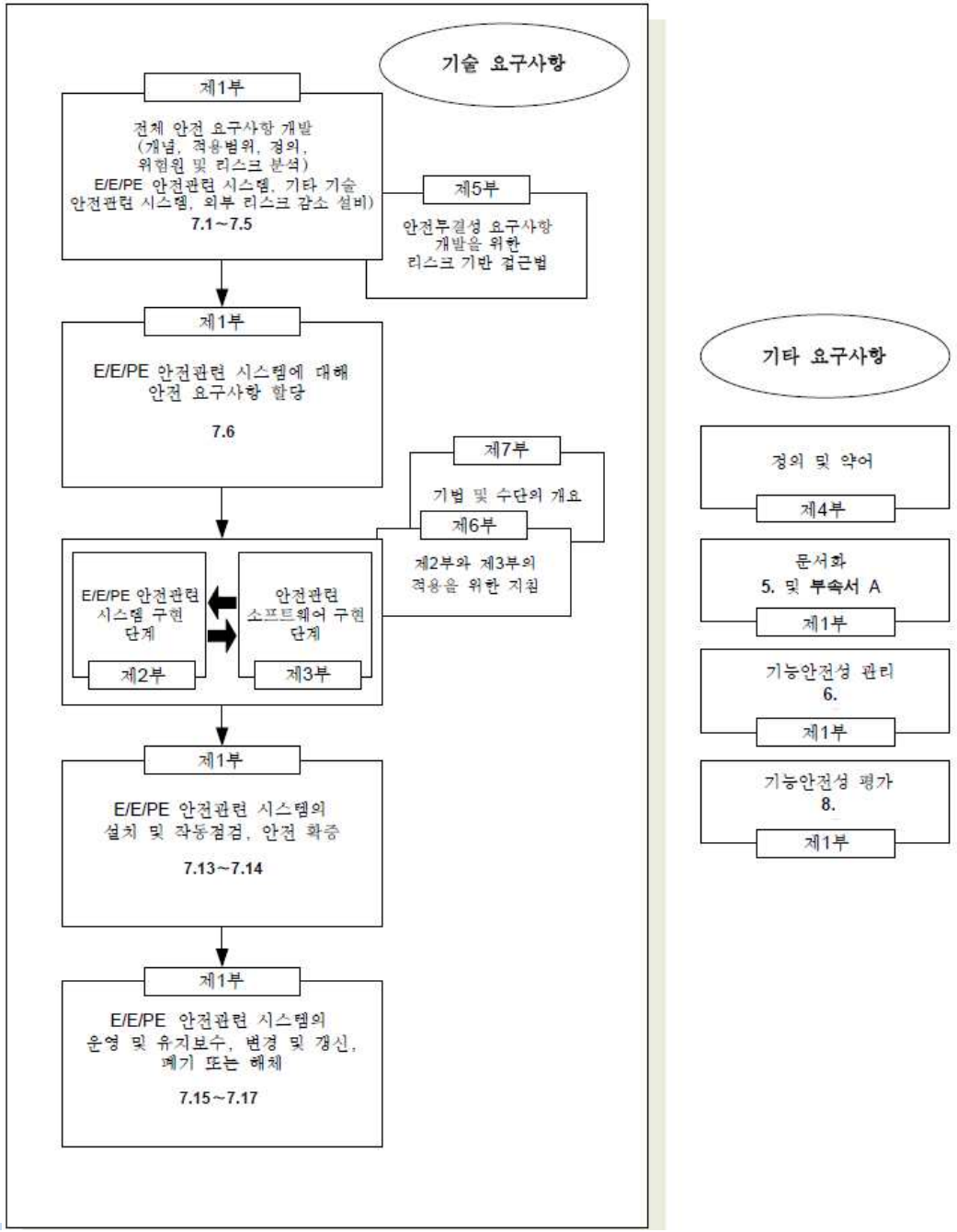
Operate, maintain, change, decommission, dispose safely

구성

- IEC 61508 : Functional safety of electrical/electronic/ programmable electronic safety related-system
  - 7 part, 400 page

  - IEC 61508-1 : *General requirements*
  - IEC 61508-2 : *Requirements for electrical/electronic/programmable electronic safety-related systems*
  - IEC 61508-3 : *Software requirements*
  - IEC 61508-4 : *Definitions and abbreviations*
  - IEC 61508-5 : *Examples of methods for the determination of safety integrity levels*
  - IEC 61508-6 : *Guidelines on the application of IEC 61508-2 and IEC 61508-3*
  - IEC 61508-7 : *Overview of techniques and measures*

IEC 61508 시리즈의 전체 프레임워크



목적

- 안전성 및 경제적인 성과 모두 개선하기 위한 E/E/PE 기술의 잠재성을 발현한다.
- **기술적인 개발이 전체 안전 프레임워크 내에서 이루어지도록 한다.**
- 미래에 대한 충분한 유연성을 가지며 기술적으로 견고한 시스템 기반 접근방법을 제공한다.
- **안전관련 시스템에 요구되는 성능을 결정하기 위해 리스크 기반 접근방법을 제공한다.**
- 산업에 직접적으로 사용될 수 있고, 또한 분야별 표준(예를 들면, 기계, 장치 화학공장, 의료 또는 철도)이나 제품 표준(전력 구동 시스템)을 개발하는 데 도움이 될 수 있는 **일반론에 기초한 표준을 제공한다**.
- 컴퓨터 기반 기술을 사용할 때, 사용자 및 규정자(regurator)가 신뢰를 얻기 위한 수단을 제공한다.
  - IEC 61508은 E/E/PE 안전관련 시스템에 의해 달성된 기능안전성을 **권한이 없는 사람이 피해를 입히고/입히거나, 그렇지 않고 반대로 피해를 입는 것**을 방지하기 위해 필요할 수 있는 주의사항은 **다루지 않는다.**

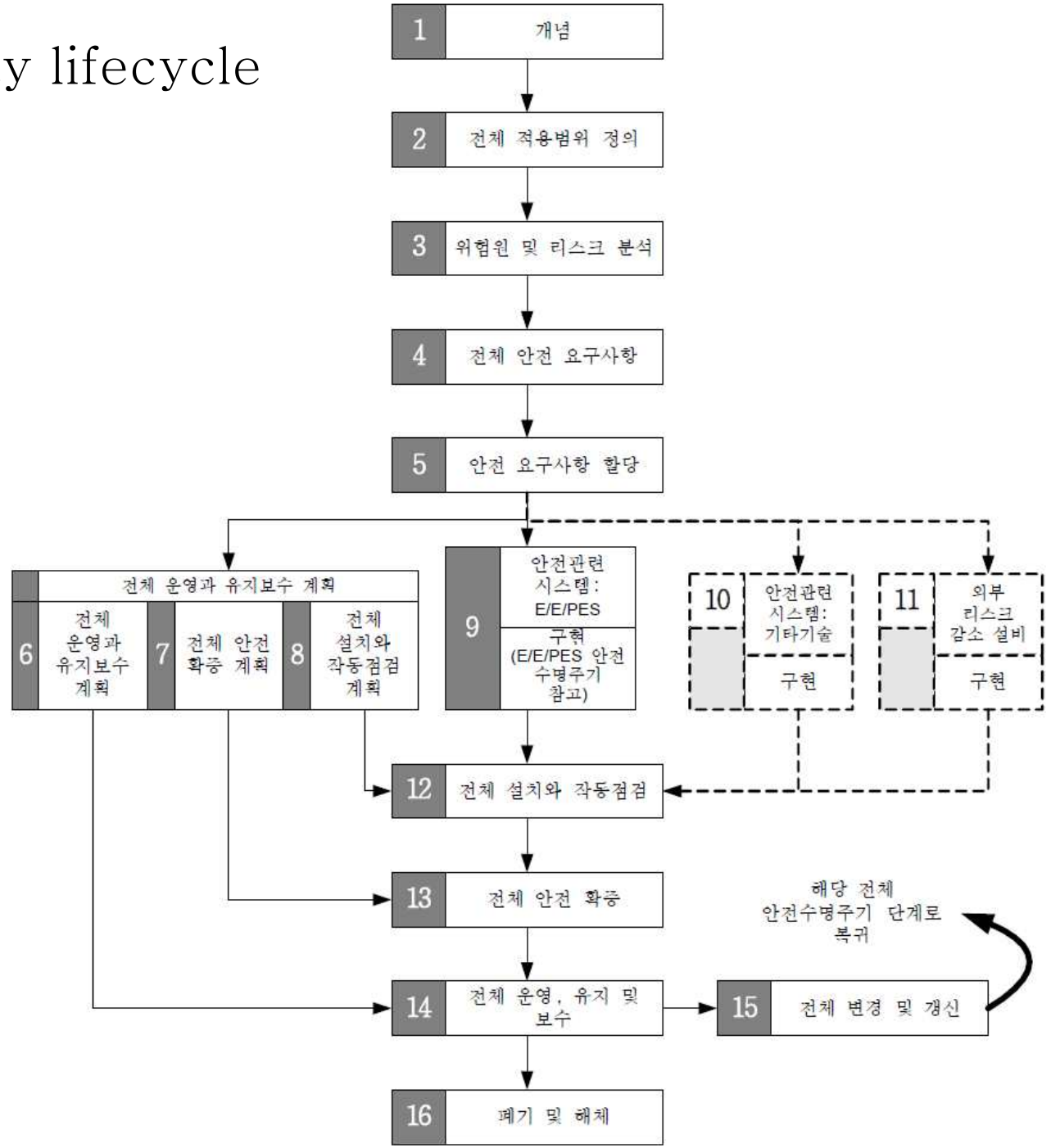
키워드

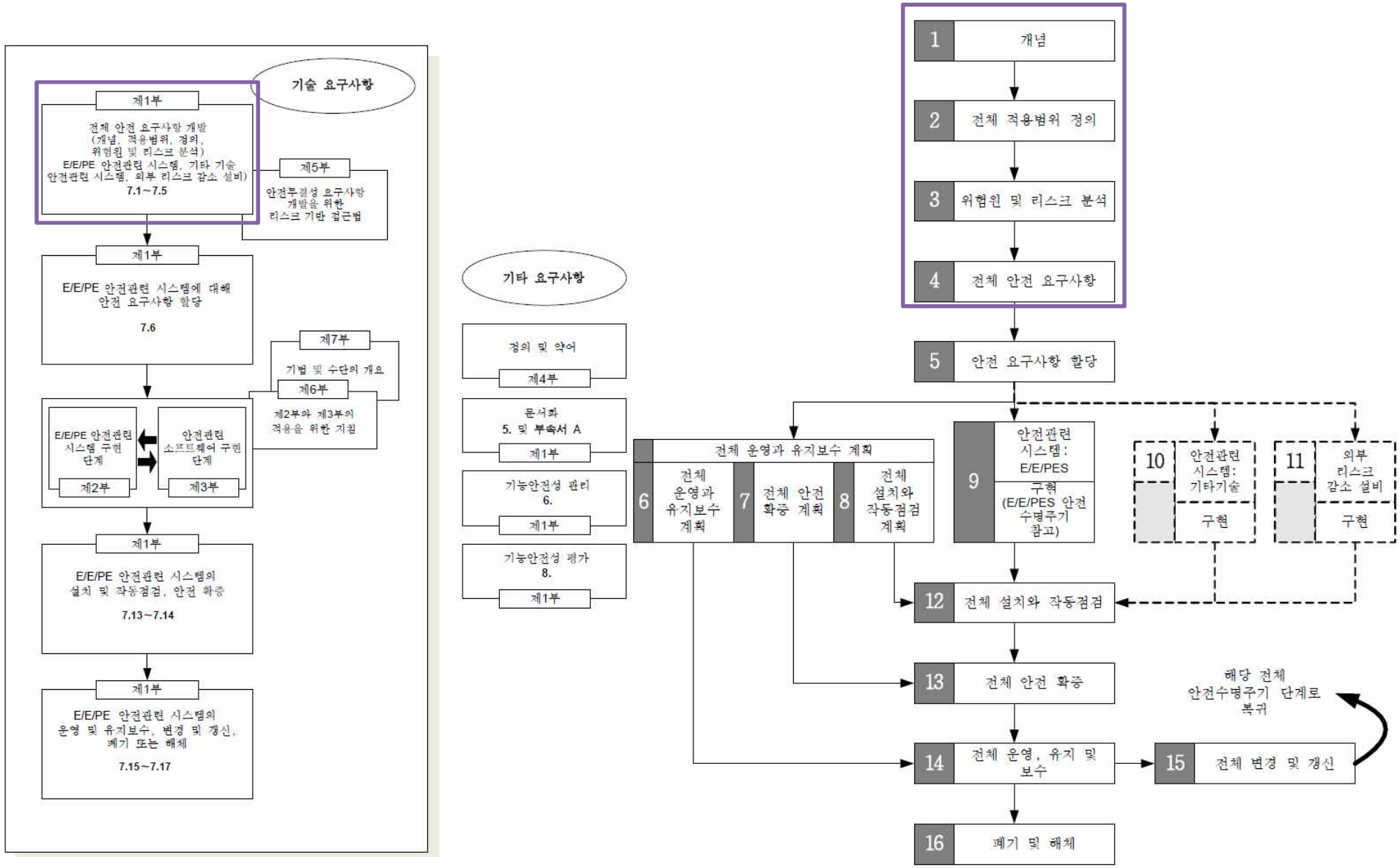
- Safety
- Safety function
- Electrical/electronic/programmable electronic (E/E/PE)
- Safety lifecycle
- Safety integrity level (SIL)
- EUC (Equipment under control)

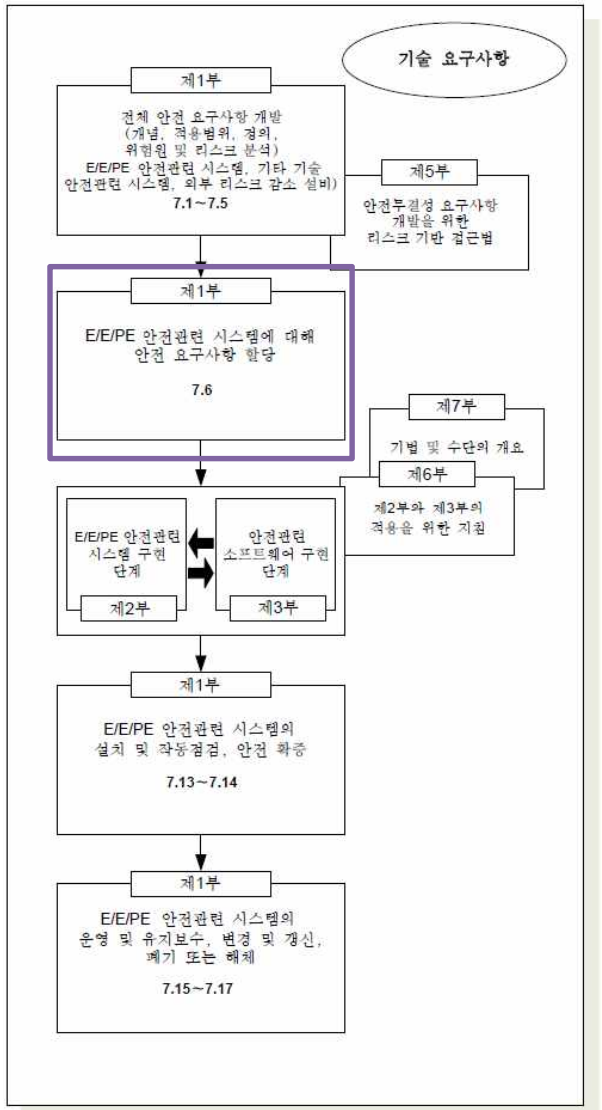
IEC 61508

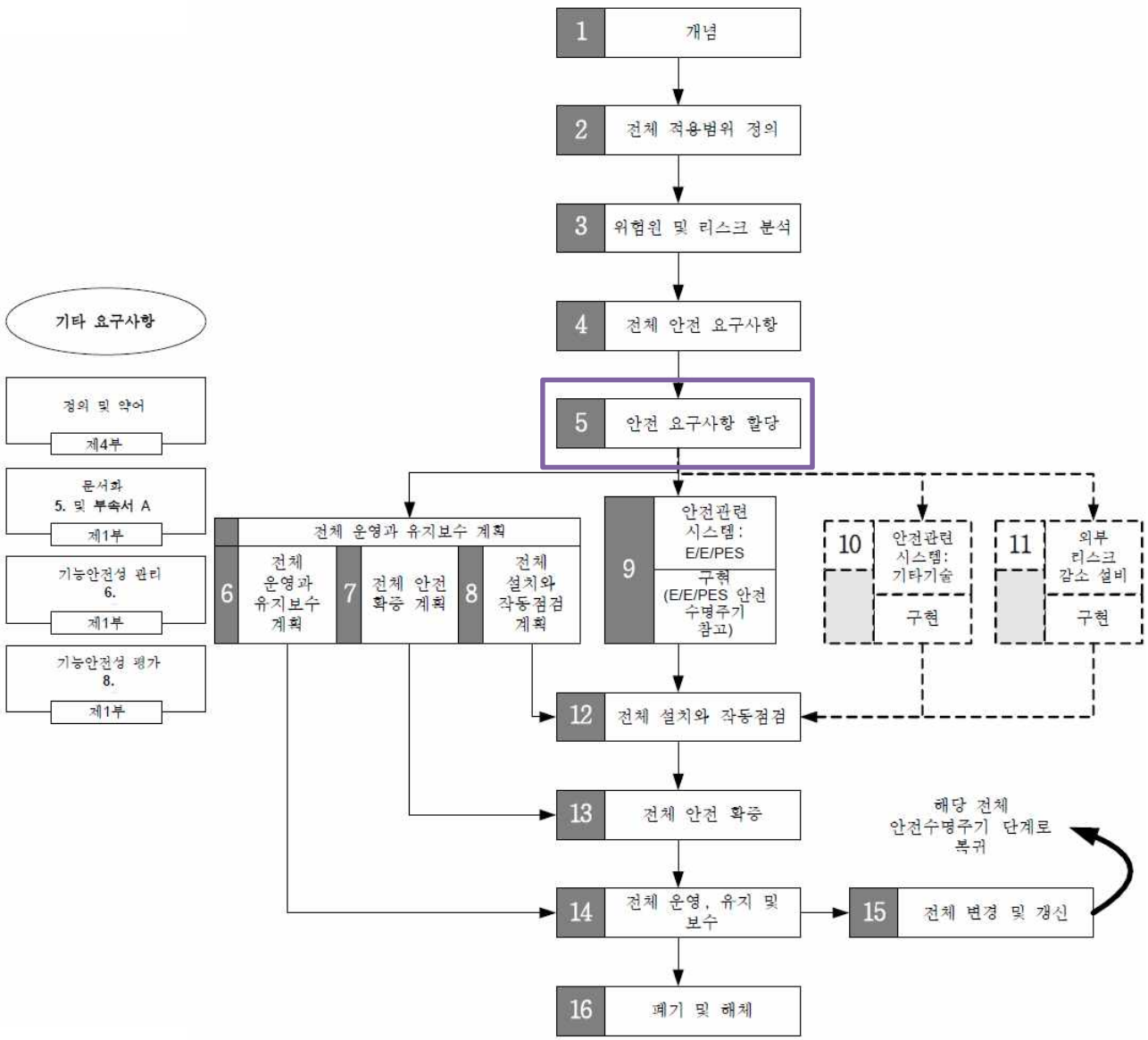
PARTS

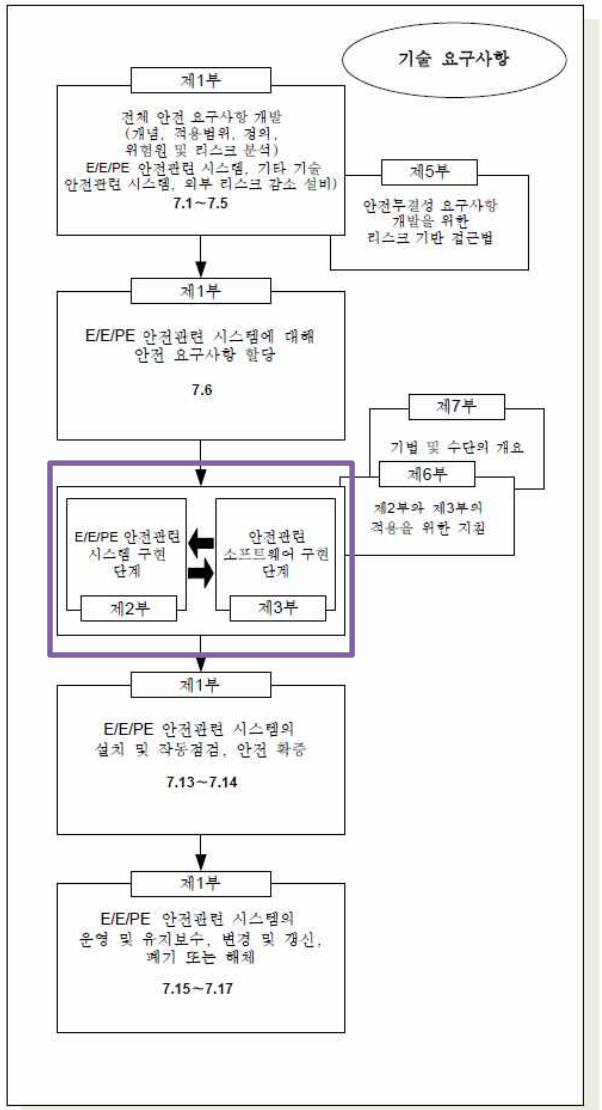
Safety lifecycle

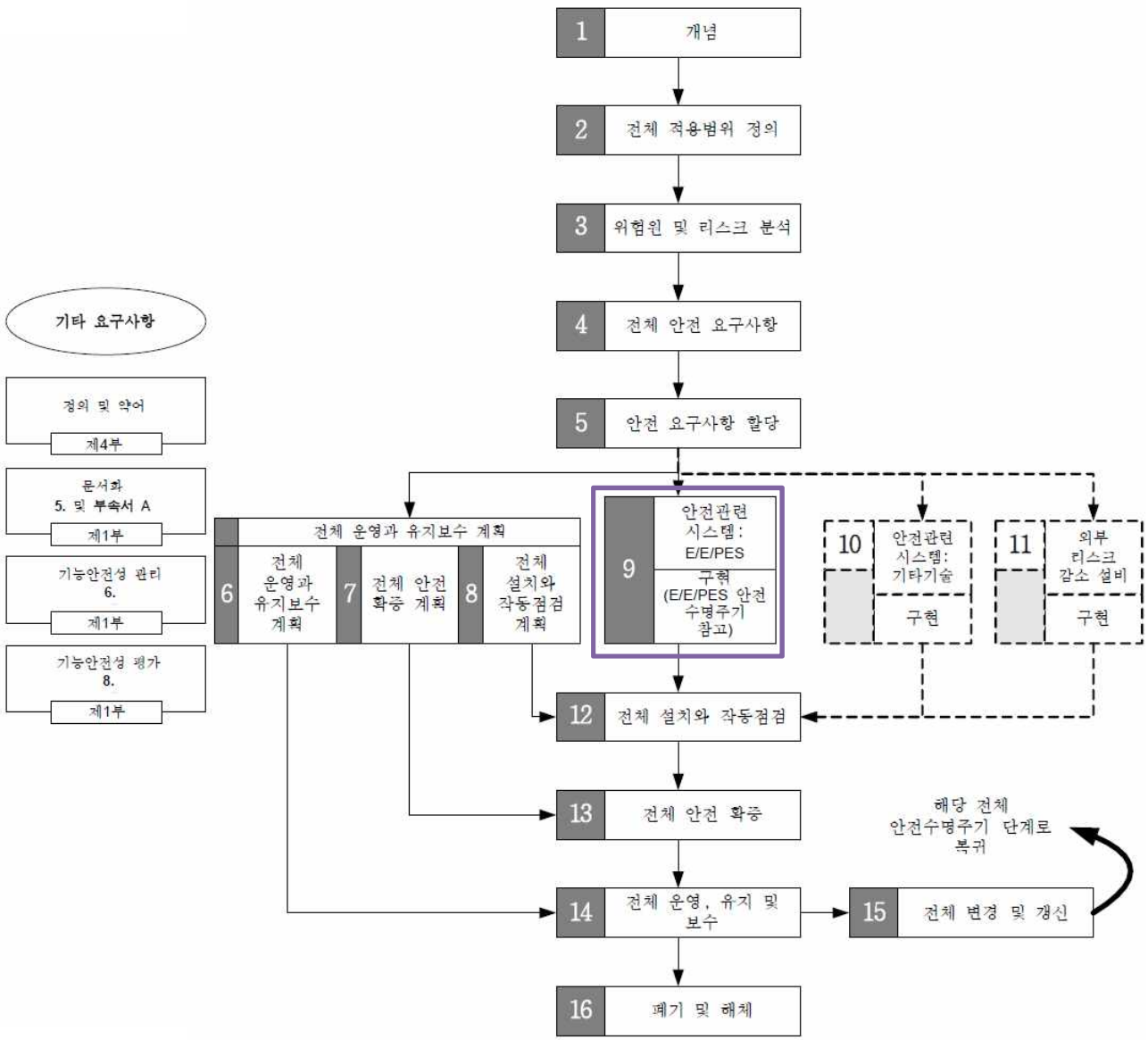


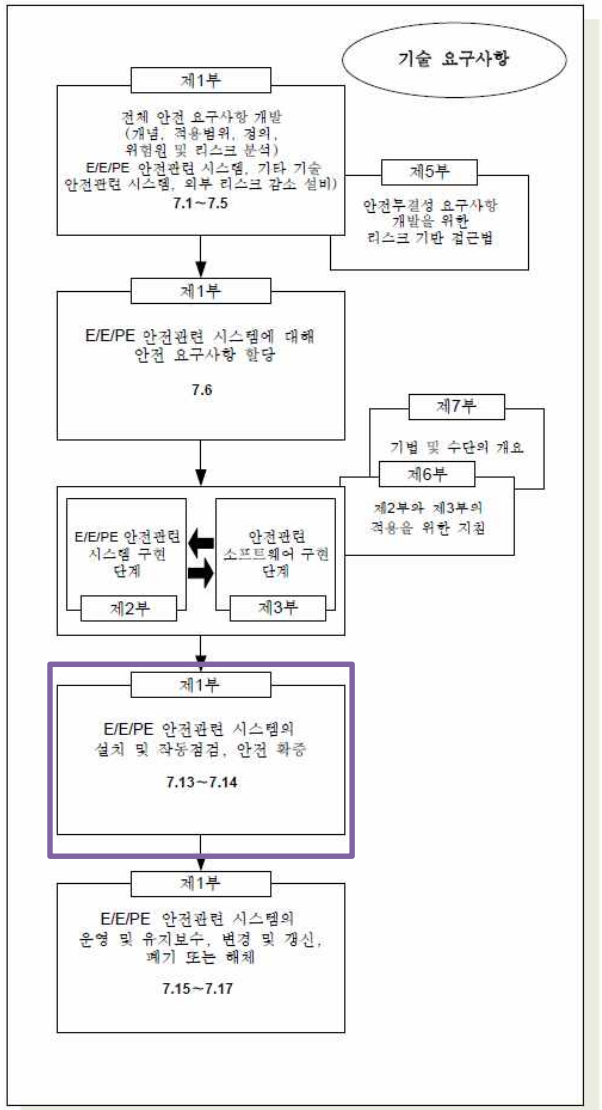

기술 요구사항
제1부
전체 안전 요구사항 개발
(개념, 적용범위, 정의,
위험원 및 리스크 분석)
E/E/PE 안전관련 시스템, 기타 기술
안전관련 시스템, 외부 리스크 감소 설비)
7.1~7.5
제5부
안전무결성 요구사항
개발을 위한
리스크 기반 접근법
제1부
E/E/PE 안전관련 시스템에 대해
안전 요구사항 할당
7.6
제7부
기법 및 수단의 개요
제6부
제2부와 제3부의
적용을 위한 지침
E/E/PE 안전관련
시스템 구현
단계
제2부
안전관련
소프트웨어 구현
단계
제3부
제1부
E/E/PE 안전관련 시스템의
설치 및 작동점검, 안전 확증
7.13~7.14
제1부
E/E/PE 안전관련 시스템의
운영 및 유지보수, 변경 및 갱신,
폐기 또는 해체
7.15~7.17
기타 요구사항
정의 및 약어
제4부
문서화
5. 및 부속서 A
제1부
기능안전성 관리
6.
제1부
기능안전성 평가
8.
제1부
1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술 구현
11 외부 리스크 감소 설비 구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체
안전수명주기 단계로
복귀
16 폐기 및 해체

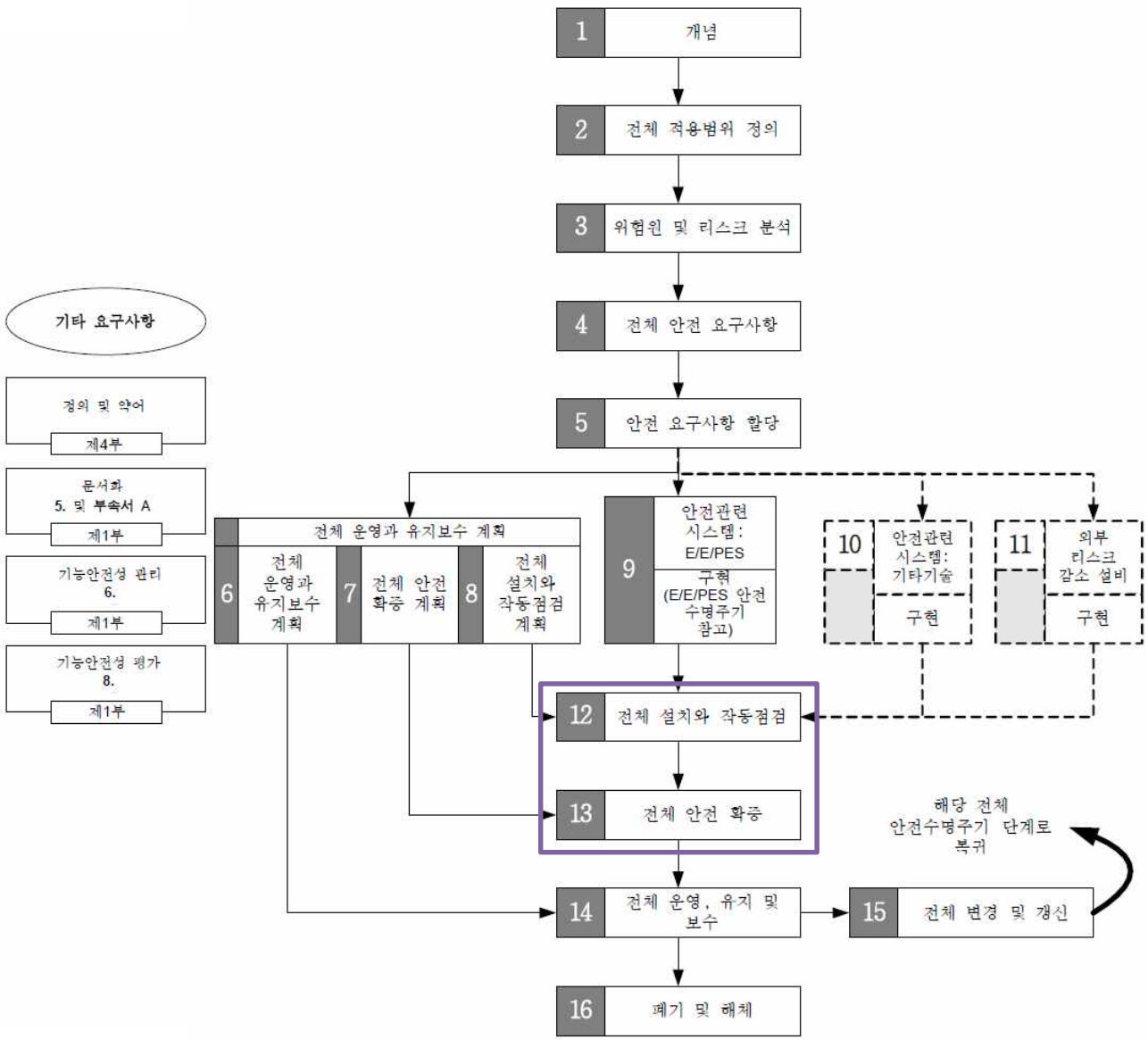

기술 요구사항
제1부
전체 안전 요구사항 개발
(개념, 적용범위, 정의,
위험원 및 리스크 분석)
E/E/PE 안전관련 시스템, 기타 기술
안전관련 시스템, 외부 리스크 감소 설비)
7.1~7.5
제5부
안전무결성 요구사항
개발을 위한
리스크 기반 접근법
제1부
E/E/PE 안전관련 시스템에 대해
안전 요구사항 할당
7.6
제7부
기법 및 수단의 개요
제6부
제2부와 제3부의
적용을 위한 지침
E/E/PE 안전관련
시스템 구현
단계
제2부
안전관련
소프트웨어 구현
단계
제3부
제1부
E/E/PE 안전관련 시스템의
설치 및 작동점검, 안전 확증
7.13~7.14
제1부
E/E/PE 안전관련 시스템의
운영 및 유지보수, 변경 및 갱신,
폐기 또는 해체
7.15~7.17

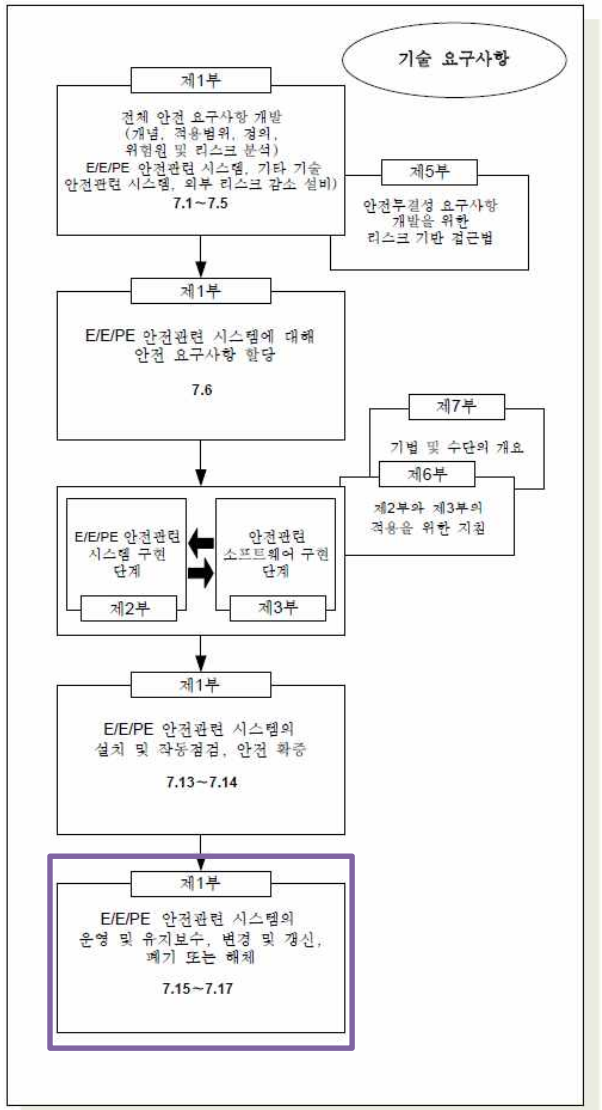

기타 요구사항
정의 및 약어
제4부
문서화
5. 및 부속서 A
제1부
기능안전성 관리
6.
제1부
기능안전성 평가
8.
제1부
1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술 구현
11 외부 리스크 감소 설비 구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체

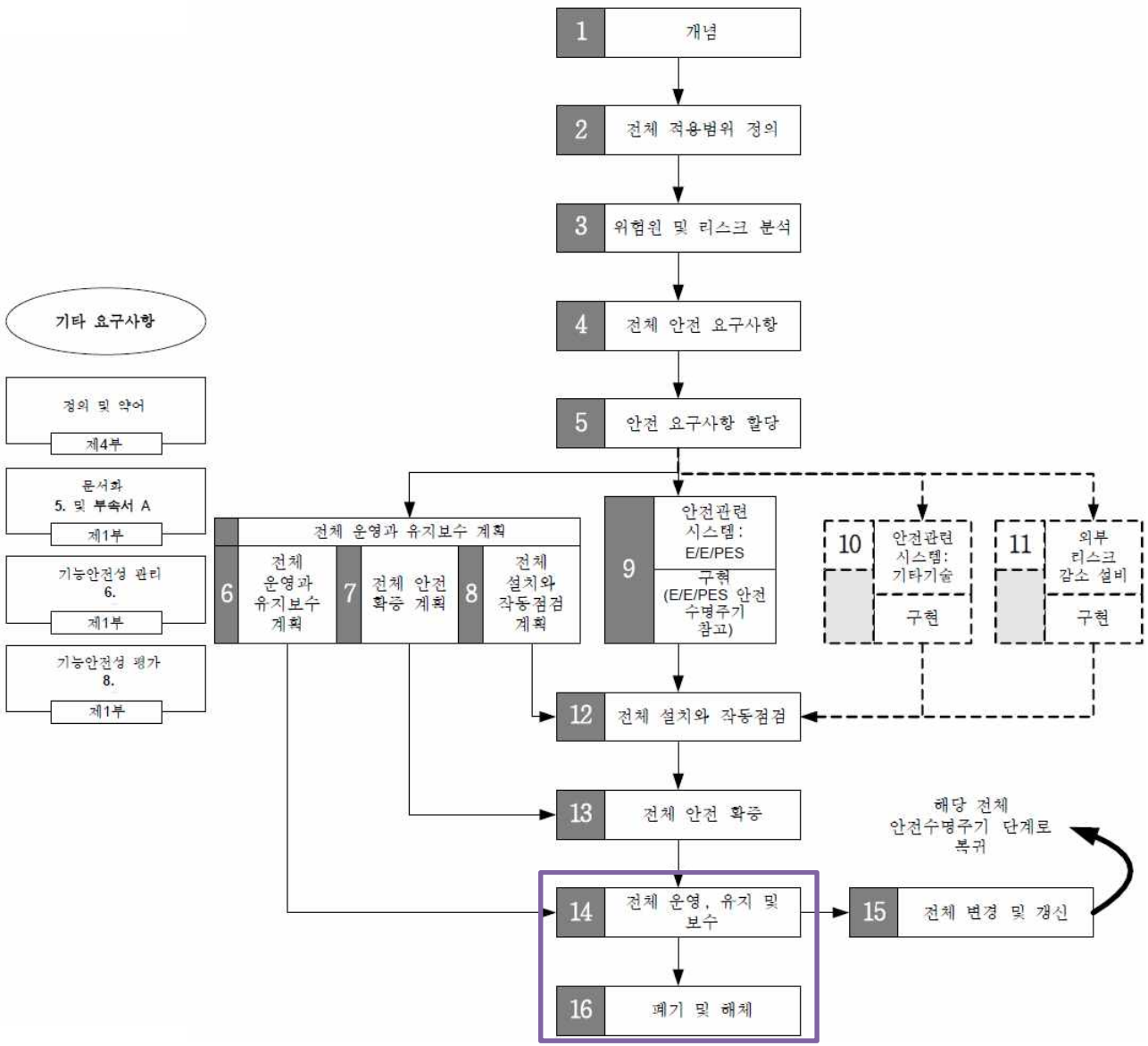

기술 요구사항
제1부
전체 안전 요구사항 개발
(개념, 적용범위, 정의,
위험원 및 리스크 분석)
E/E/PE 안전관련 시스템, 기타 기술
안전관련 시스템, 외부 리스크 감소 설비)
7.1~7.5
제5부
안전무결성 요구사항
개발을 위한
리스크 기반 접근법
제1부
E/E/PE 안전관련 시스템에 대해
안전 요구사항 할당
7.6
제7부
기법 및 수단의 개요
제6부
제2부와 제3부의
적용을 위한 지침
E/E/PE 안전관련
시스템 구현
단계
제2부
안전관련
소프트웨어 구현
단계
제3부
제1부
E/E/PE 안전관련 시스템의
설치 및 작동점검, 안전 확증
7.13~7.14
제1부
E/E/PE 안전관련 시스템의
운영 및 유지보수, 변경 및 갱신,
폐기 또는 해체
7.15~7.17

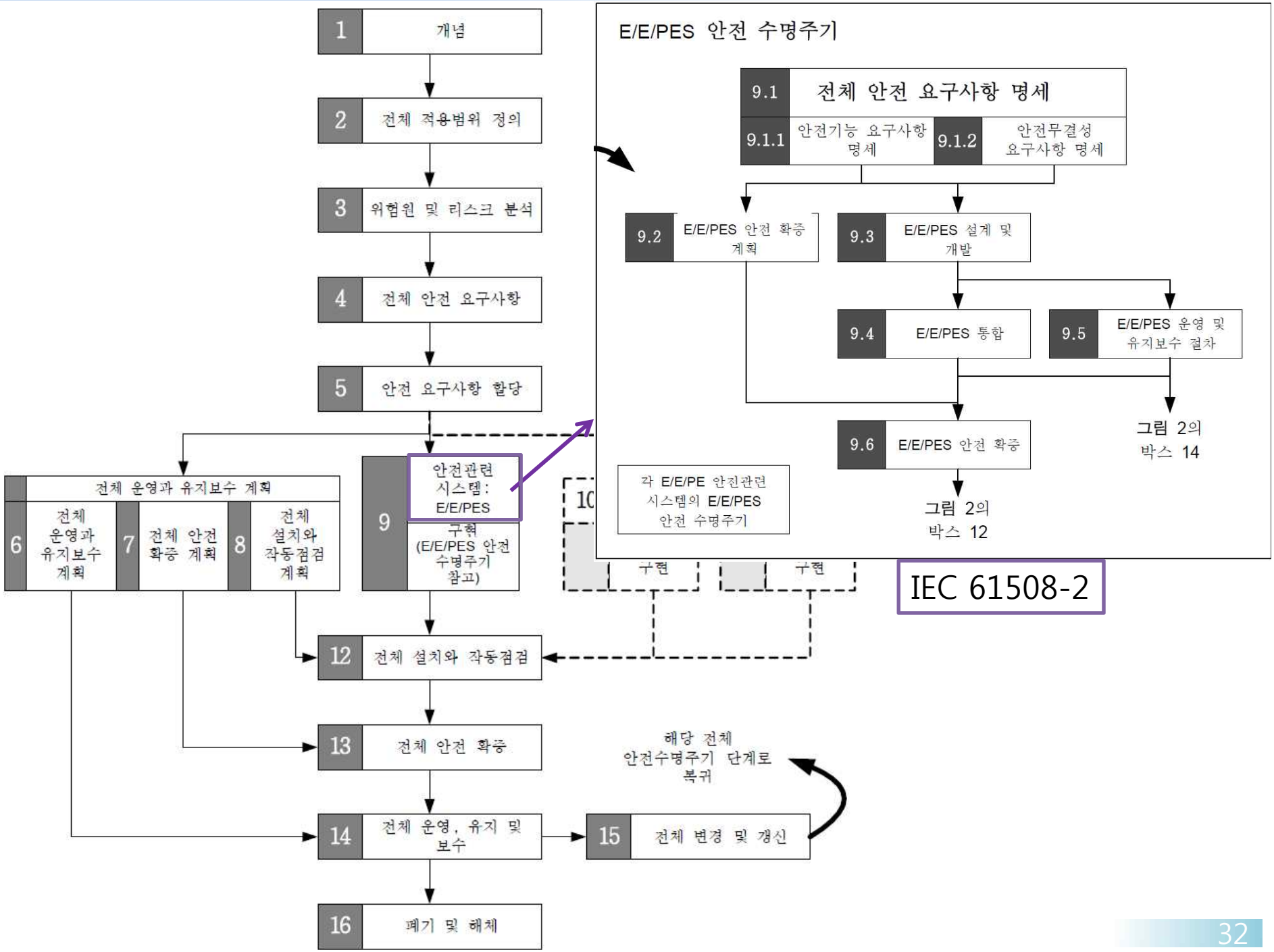

기타 요구사항
정의 및 약어
제4부
문서화
5. 및 부속서 A
제1부
기능안전성 관리
6.
제1부
기능안전성 평가
8.
제1부
1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술 구현
11 외부 리스크 감소 설비 구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체

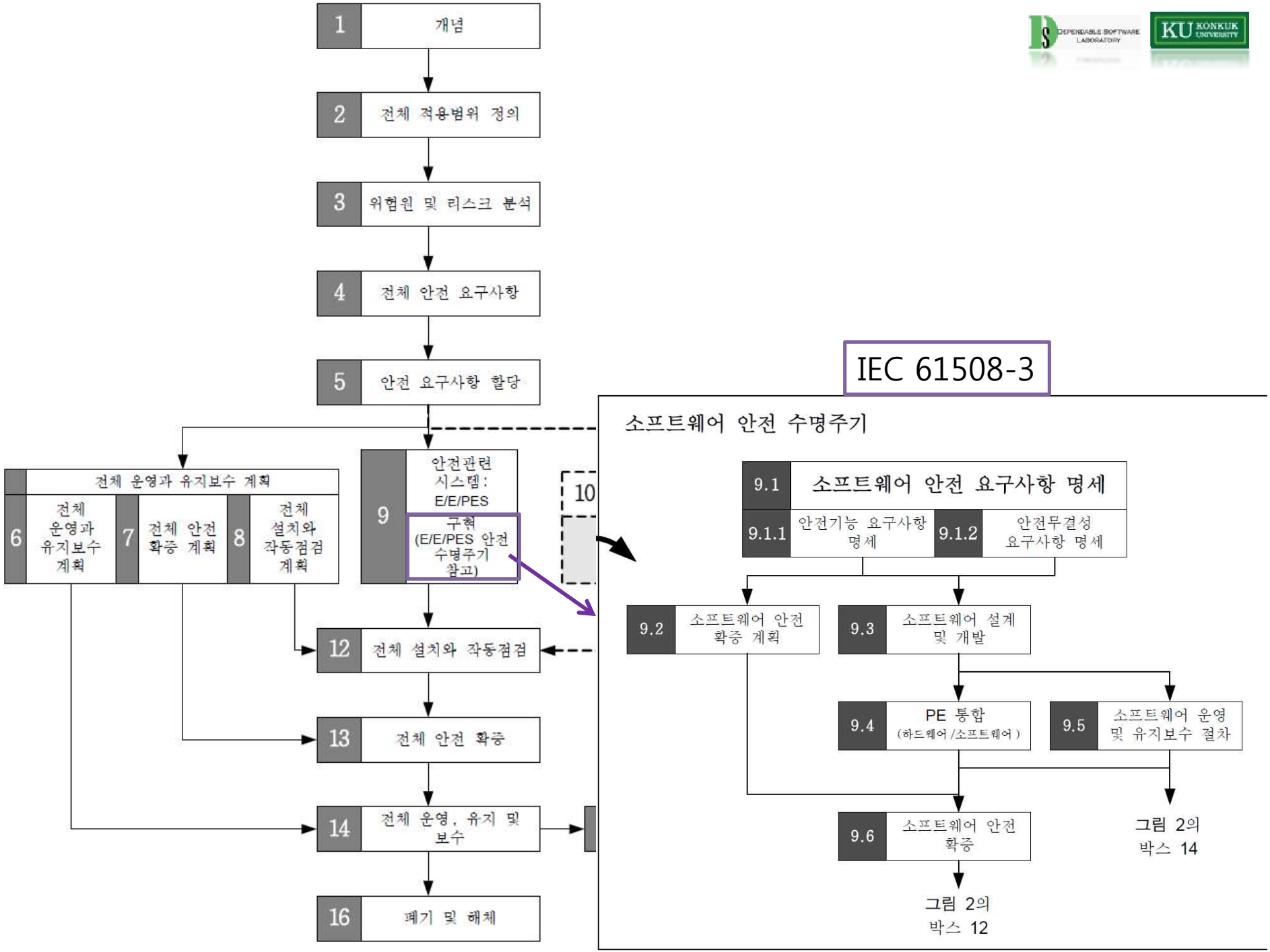

기술 요구사항
제1부
전체 안전 요구사항 개발
(개념, 적용범위, 정의,
위험원 및 리스크 분석)
E/E/PE 안전관련 시스템, 기타 기술
안전관련 시스템, 외부 리스크 감소 설비)
7.1~7.5
제5부
안전무결성 요구사항
개발을 위한
리스크 기반 접근법
제1부
E/E/PE 안전관련 시스템에 대해
안전 요구사항 할당
7.6
제7부
기법 및 수단의 개요
제6부
제2부와 제3부의
적용을 위한 지침
E/E/PE 안전관련
시스템 구현
단계
제2부
안전관련
소프트웨어 구현
단계
제3부
제1부
E/E/PE 안전관련 시스템의
설치 및 작동점검, 안전 확증
7.13~7.14
제1부
E/E/PE 안전관련 시스템의
운영 및 유지보수, 변경 및 갱신,
폐기 또는 해체
7.15~7.17


기타 요구사항
정의 및 약어
제4부
문서화
5. 및 부속서 A
제1부
기능안전성 관리
6.
제1부
기능안전성 평가
8.
제1부
1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술 구현
11 외부 리스크 감소 설비 구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체


기술 요구사항
제1부
전체 안전 요구사항 개발
(개념, 적용범위, 정의,
위험원 및 리스크 분석)
E/E/PE 안전관련 시스템, 기타 기술
안전관련 시스템, 외부 리스크 감소 설비)
7.1~7.5
제5부
안전무결성 요구사항
개발을 위한
리스크 기반 접근법
제1부
E/E/PE 안전관련 시스템에 대해
안전 요구사항 할당
7.6
제7부
기법 및 수단의 개요
제6부
제2부와 제3부의
적용을 위한 지침
E/E/PE 안전관련
시스템 구현
단계
제2부
안전관련
소프트웨어 구현
단계
제3부
제1부
E/E/PE 안전관련 시스템의
설치 및 작동점검, 안전 확증
7.13~7.14
제1부
E/E/PE 안전관련 시스템의
운영 및 유지보수, 변경 및 갱신,
폐기 또는 해체
7.15~7.17

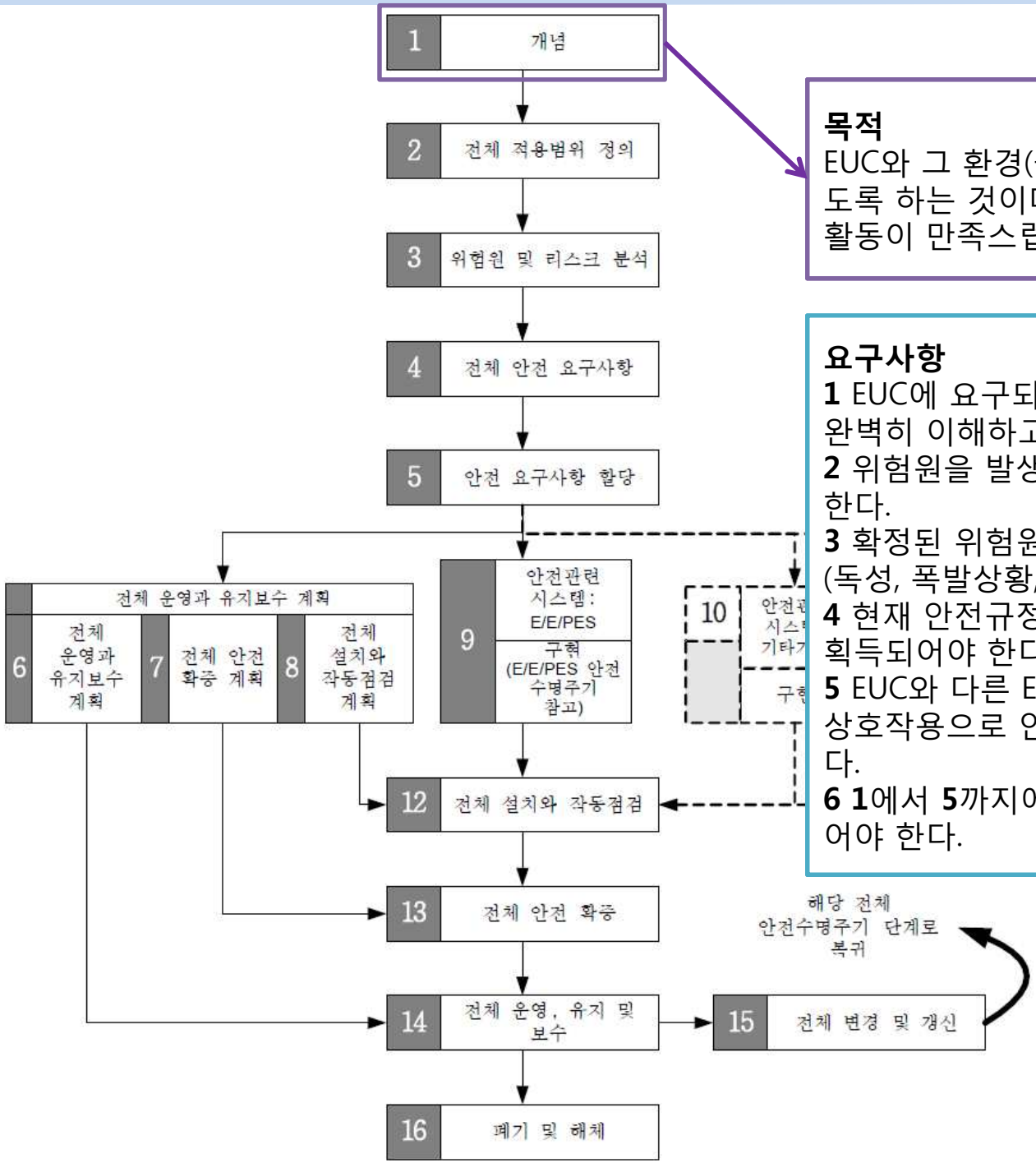

기타 요구사항
정의 및 약어
제4부
문서화
5. 및 부속서 A
제1부
기능안전성 관리
6.
제1부
기능안전성 평가
8.
제1부
1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술 구현
11 외부 리스크 감소 설비 구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 구현
구현
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
16 폐기 및 해체
해당 전체 안전수명주기 단계로 복귀
각 E/E/PE 안전관련 시스템의 E/E/PES 안전 수명주기
E/E/PES 안전 수명주기
9.1 전체 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 E/E/PES 안전 확증 계획
9.3 E/E/PES 설계 및 개발
9.4 E/E/PES 통합
9.5 E/E/PES 운영 및 유지보수 절차
9.6 E/E/PES 안전 확증
그림 2의 박스 14
그림 2의 박스 12
IEC 61508-2


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
16 폐기 및 해체
IEC 61508-3
소프트웨어 안전 수명주기
9.1 소프트웨어 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 소프트웨어 안전 확증 계획
9.3 소프트웨어 설계 및 개발
9.4 PE 통합 (하드웨어/소프트웨어)
9.5 소프트웨어 운영 및 유지보수 절차
9.6 소프트웨어 안전 확증
그림 2의 박스 14
그림 2의 박스 12

Safety lifecycle

- 목적과 요구사항으로 구성

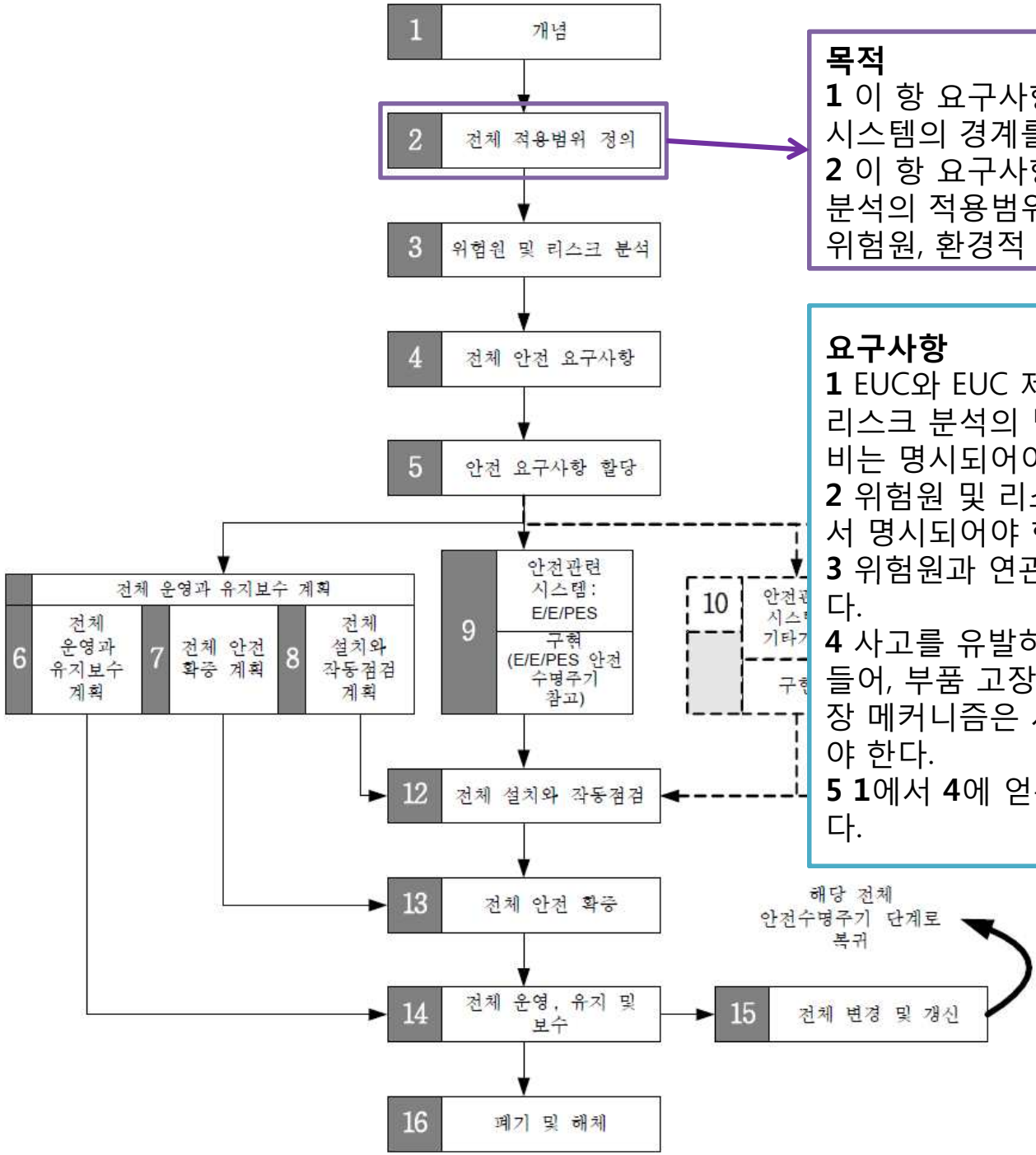


목적

EUC와 그 환경(물리적, 법적 등)을 충분히 이해하도록 하는 것이며, 그럼으로써 기타 안전수명주기 활동이 만족스럽게 실시될 수 있도록 하는 것이다.

요구사항

1 EUC에 요구되는 통제기능, 물리적 환경에 대해 완벽히 이해하고 있어야 한다.
2 위험원을 발생시킬 수 있는 원인이 결정되어야 한다.
3 확정된 위험원에 관한 정보가 획득되어야 한다 (독성, 폭발상황, 부식성, 반응성, 인화성 등).
4 현재 안전규정(국가적 및 국제적)에 관한 정보가 획득되어야 한다.
5 EUC와 다른 EUC들(설치되었거나 설치될)과의 상호작용으로 인한 위험원이 고려되어야 한다.
6 **1**에서 **5**까지에서 얻은 결과와 정보는 문서화되어야 한다.



목적

1 이 항 요구사항의 첫째 목적은 EUC와 EUC 제어 시스템의 경계를 결정하는 것이다.

2 이 항 요구사항의 둘째 목적은 위험원 및 리스크 분석의 적용범위를 명시하는 것이다(예 : 프로세스 위험원, 환경적 위험원 등).

요구사항

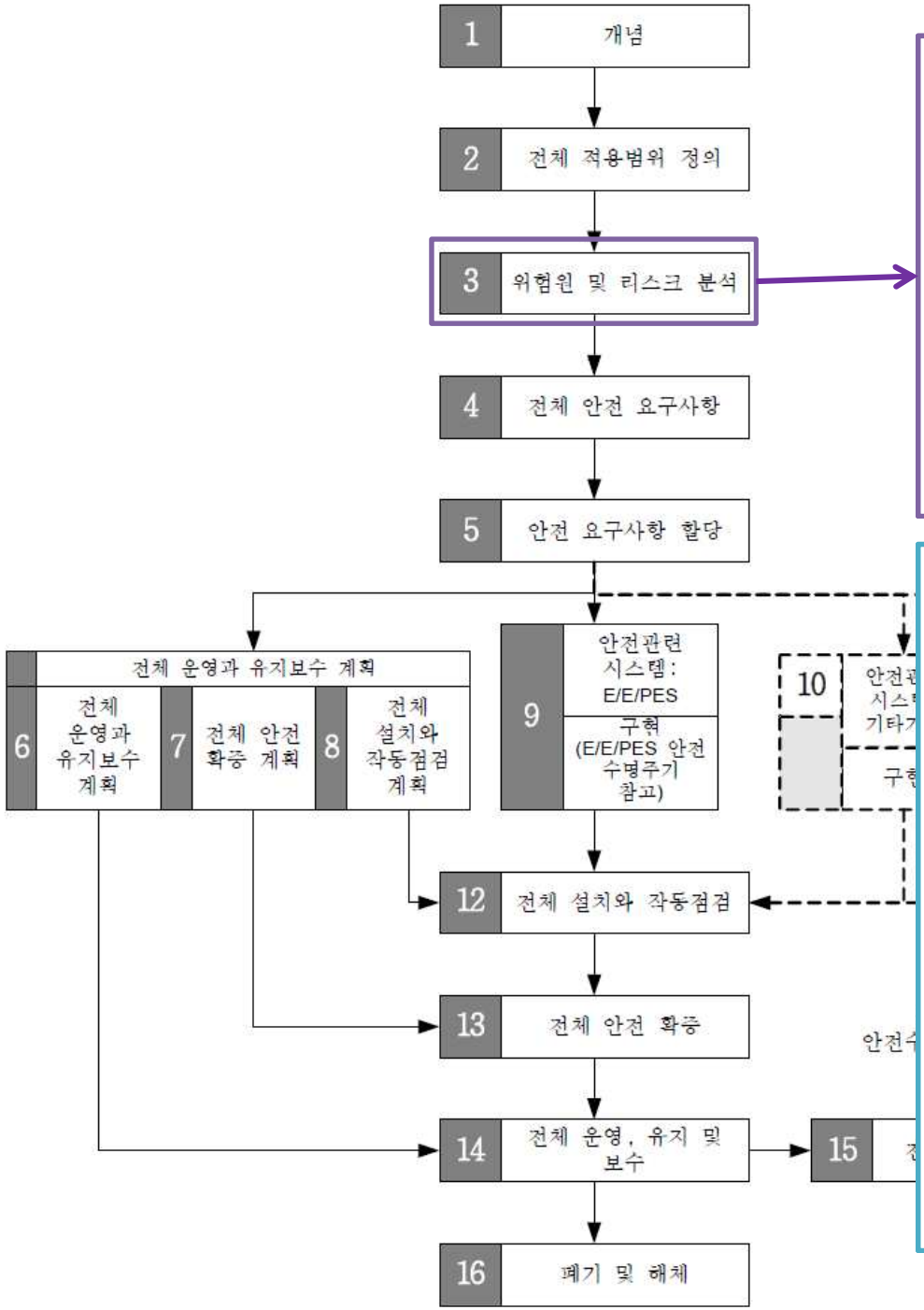
1 EUC와 EUC 제어 시스템을 포함하여, 위험원 및 리스크 분석의 범위에 포함되어야 하는물리적 장비는 명시되어야 한다.

2 위험원 및 리스크 분석은 외부적 경우를 고려해서 명시되어야 한다.

3 위험원과 연관된 세부 시스템이 명시되어야 한다.

4 사고를 유발하는 경우의 유형을 고려하여(예를 들어, 부품 고장, 절차 결함, 인적 오류, 종속적 고장 메커니즘은 사고를 발생시키는 원인) 명시하여야 한다.

5 **1**에서 **4**에 얻은 결과와 정보는 문서화되어야 한다.



목적

1 이 항 요구사항 첫째 목적은 모든 합리적으로 예측 가능한 상황(결함 상황 및 오용 포함)에서의 EUC와 EUC 제어 시스템(운영상의 모든 상태에서)의 위험원과 위해 사건을 결정하는 것이다.

2 이 항 요구사항 둘째 목적은 **1**에서 확정된 위해 사건으로 이르게 하는 사건 순서를결정하는 것이다.

3 이 항 요구사항의 셋째 목적은 **1**에서 확정된 위해 사건과 연관된 EUC 리스크를 결정하는 것이다.

요구사항

1 위험원 및 리스크 분석은 전체 적용범위 정의 단계로부터 얻은 정보를 고려하여수행되어야 한다. 전체, E/E/PES 또는 소프트웨어 안전수명주기 단계에서 취해져야 한다고 결정된 사항들이, 후속단계에서 변경됨으로 인해서 그 전 단계에서 취해져야 한다고 결정된 사항의 기본이 변경되는 경우는, 추가적인 위험원 및 리스크 분석이 수행되어야 한다.

2 위험원 제거를 고려하여야 한다.

3 EUC와 EUC 제어 시스템의 위험원 및 위해 사건을 합리적으로 예측 가능한 모든 상황(결함 상황 및 합리적으로 예측 가능한 오용 포함)하에서 결정되어야 한다. 이와 관련된 인적 요인 문제도 포함되어야 하며 EUC의 운영 방식 중 비정상적이거나 흔치 않은 방식에 대해 특히 주의를 기울여야 한다.

4 **3**에서 확정된 위해 사건을 초래하는 사건 순서가 결정되어야 한다.

5 **3**에서 명시된 상황에 대해 위해 사건 발생 가능성이 평가되어야 한다.

6 **3**에서 확정된 위해 사건과 연관된 잠재 결과를 결정하여야 한다.

7 EUC의 리스크는 확정된 위해 사건마다 평가 및 측정되어야 한다.

8 **1~7**의 요구사항을 정량적 또는 정성적인 위험원 및 리스크 분석 기법을 응용함으로써 만족시킬 수 있다

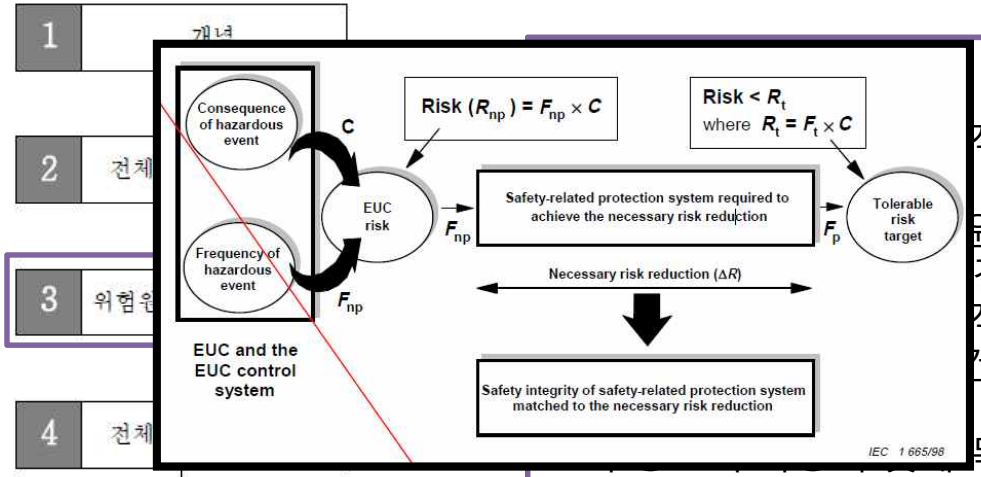
9 기법의 적절성 및 기법이 적용될 필요가 있는 범위는 다음과 같은 요인을 고려하여 적용되
어야 한다.

10 위험원 및 리스크 분석은 다음 사항을 고려하여야 한다.

11 위험원 및 리스크 분석을 구성하는 정보와 결과는 문서화 되어야 한다.

12 위험원 및 리스크 분석을 구성하는 정보와 결과는 전체 안전수명주기, 즉 위험원 및 리스크분석 단계에서 폐기 및 처리 단계까지의 기간 동안 EUC와 EUC 제어 시스템에 대하여 보관되어야한다.

정성적 방법



적은 모든 합리적으로 예
및 오용 포함)에서의
운영상의 모든 상태에서)
결정하는 것이다.
적은 **1**에서 확정된 위해
건 순서를결정하는 것이

목적은 **1**에서 확정된 위
해 사건과 연관된 EUC 리스크를 결정하는 것이다.

1 개념

2 전체

3 위험원

4 전체

5 안전 요구사항 할당

전체 운영과 유지보수 계획

6 전체 운영과 유지보수 계획

7 전체 안전 확증 계획

8 전체 설치와 작동검검 계획

9

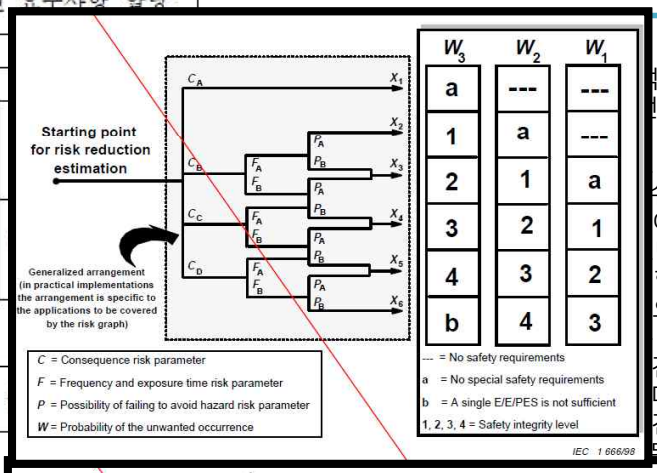
12 전체

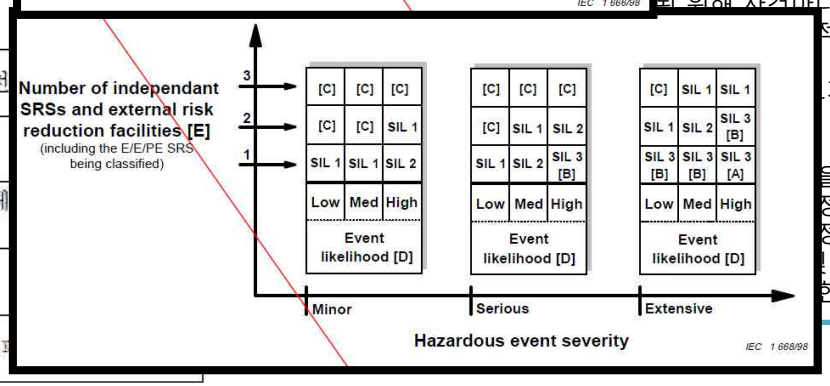
13 전

14 전체

16

정량적 방법
리스크 그래프
심각도 매트릭스

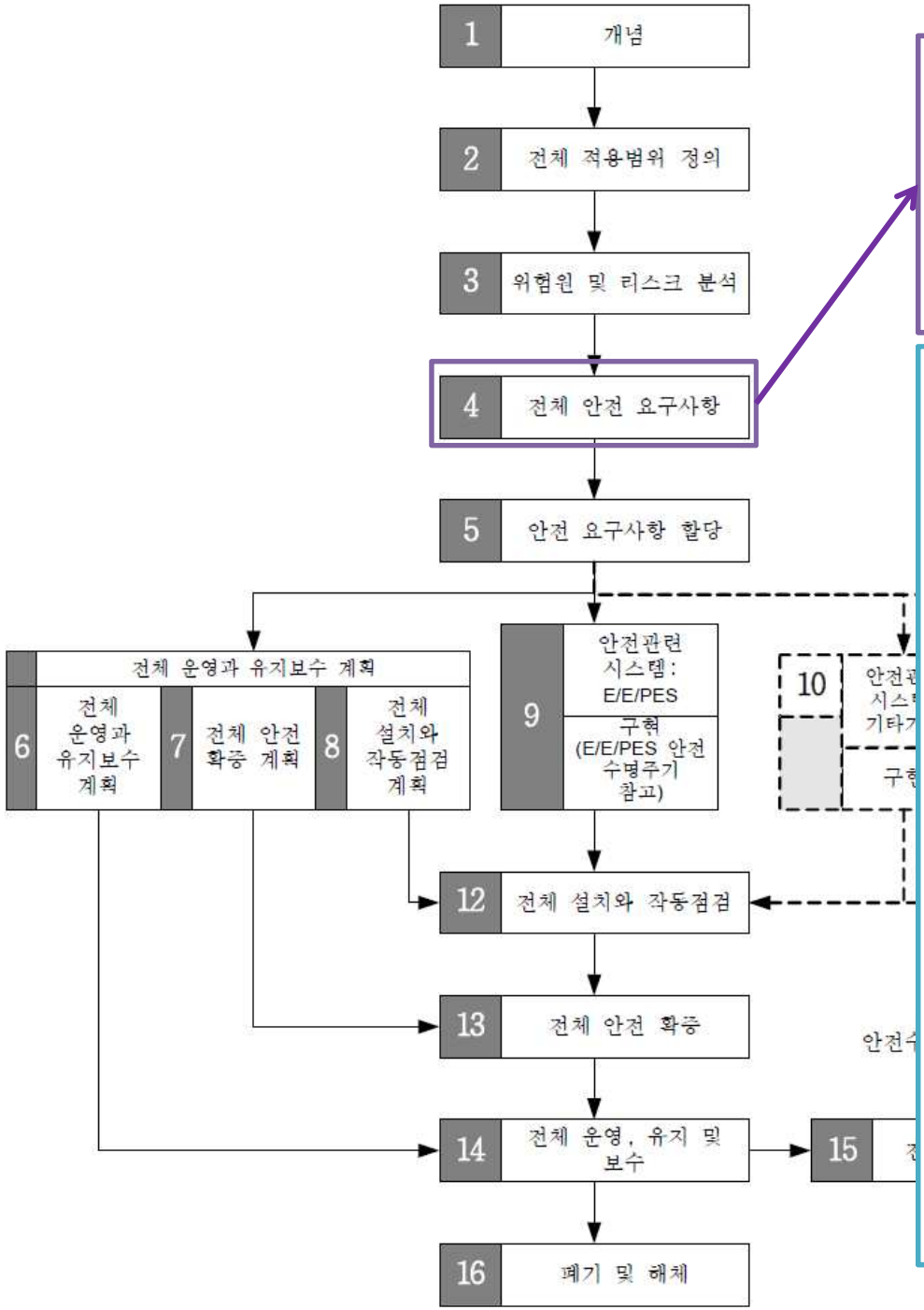




은 전체 적용범위 정의 단계로부터 얻은 정보를 고려
체, E/E/PES 또는 소프트웨어 안전수명주기 단계에서
사항들이, 후속단계에서 변경됨으로 인해서 그 전 단
결정된 사항의 기본이 변경되는 경우는, 추가적인 위
수행되어야 한다.
여야 한다.
템의 위험원 및 위해 사건을 합리적으로 예측 가능한
합리적으로 예측 가능한 오용 포함)하에서 결정되어야
요인 문제도 포함되어야 하며 EUC의 운영 방식 중 비
방식에 대해 특히 주의를 기울여야 한다.
건을 초래하는 사건 순서가 결정되어야 한다.
대해 위해 사건 발생 가능성이 평가되어야 한다.
건과 연관된 잠재 결과를 결정하여야 한다.
되 위해 사건마다 평가 및 측정되어야 한다.
적인 위험원 및 리스크 분석 기법을 응

가 있는 범위는 다음과 같은 요인을 고

을 고려하여야 한다.
정보와 결과는 문서화 되어야 한다.
정보와 결과는 전체 안전수명주기, 즉
처리 단계까지의 기간 동안 EUC와
한다.



목적

이 항 요구사항의 목적은 E/E/PE 안전관련 시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 대하여, 안전기능 요구사항 및 안전무결성 요구사항의 측면에서 전체 안전 요구사항에 대한 명세서를 개발하는 것이다. 그럼으로써 필요한 기능 안전성을 달성하는 것이다.

요구사항

1 결정된 각 위험원에 대해 요구되는 기능안전성을 확보하기 위해서 필요한 안전기능들이 명시되어야 한다. 이를 위해 전체 안전기능 요구사항에 대한 명세를 구성하여야 한다.

2 결정된 각 위해 사건에 대하여 필요한 리스크 감소가 결정 되어야 한다. 필요한 리스크 감소는 정량적 그리고/또는 정성적 방법으로 결정되어도 된다.

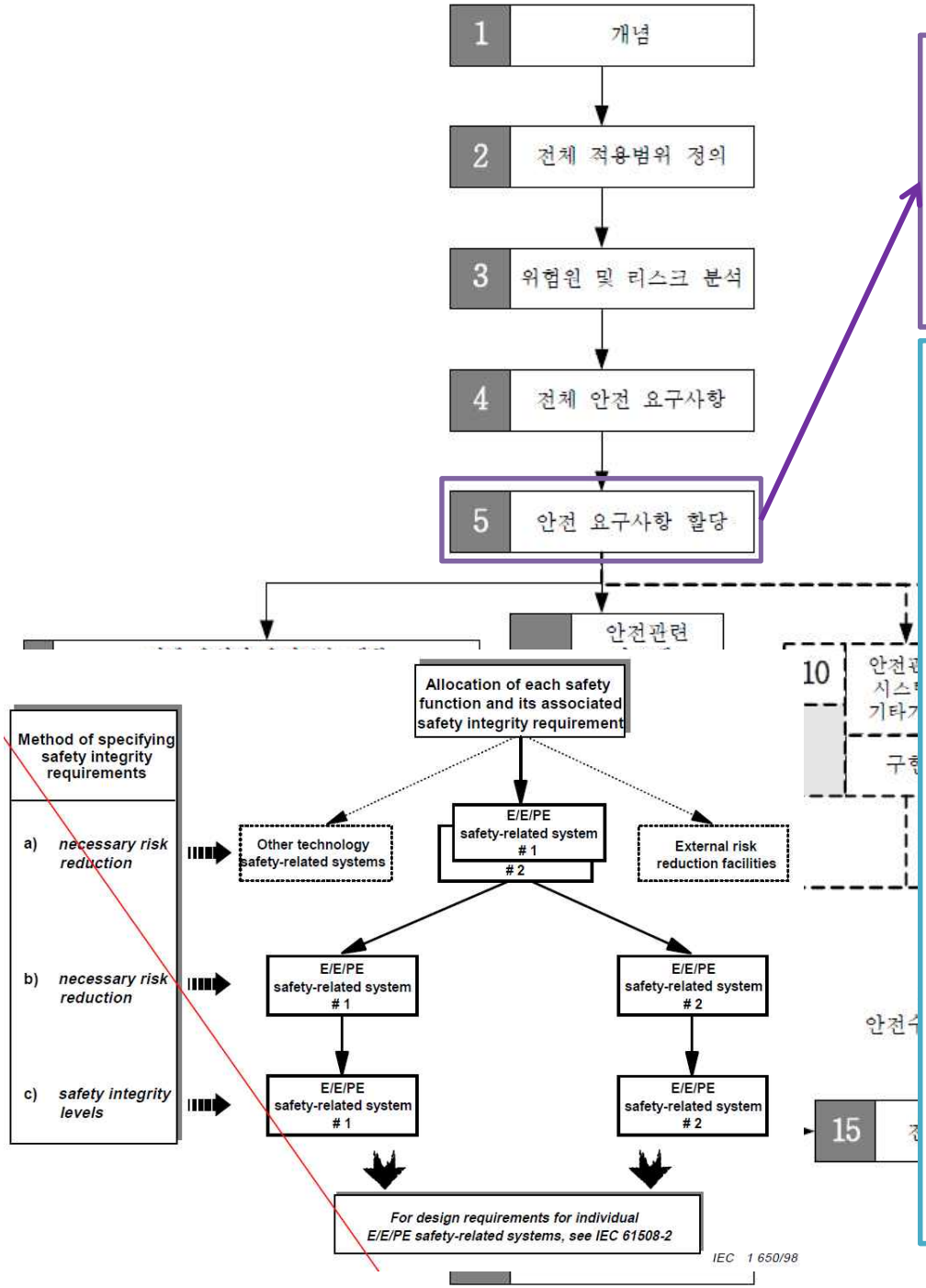
3 어떠한 응용분야의 국제표준이 존재하고, 거기에 필요한 리스크 감소를 직접적으로 결정하
는 적절한 방법이 포함되어 있는 경우에는 그러한 표준서들을 이 항의 요구사항을 충족하기 위해 사
용되어도 된다.

4 EUC 제어시스템의 고장으로 하나 이상의 E/E/PE나 기타 기술적 안전관련 시스템과/또는외부 리스크 감소 설비가 필요한 경우, 그리고 EUC 제어 시스템을 안전관련 시스템으로 지정하지 않는 경우, 다음의 요구사항이 적용되어야 한다.

5 **4**의 a)에서 d)까지의 요구사항에 해당되지 않는다면, EUC 제어 시스템을 안전관련 시스템으로 보아야 한다. EUC 제어시스템에 할당되는 안전무결성수준은 표 2와 표 3에 명시된 목표고장 기준에 따라서 EUC 제어시스템의 고장률에 근거하여야 한다. 그러한 경우, 할당된 안전무결성수준에 해당되는 이 표준의 요구사항을 EUC 제어시스템에 적용하여야 한다.

6 필요한 리스크 감소 측면에서, 안전무결성 요구사항이 각 안전기능에 대해 명시되어야 한다. 이를 통해, 전체 안전무결성 요구사항에 대한 명세가 구성되어야 한다.

7 안전기능을 위한 명세와 안전무결성 요구사항을 위한 명세은 함께 전체 안전 요구사항을 위한 명세를 구성하여야 한다.



목적

1 이 항 요구사항의 첫째 목적은 지정된 E/E/PE 안전관련 시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 전체 안전요구사항(안전기능 요구사항과 안전무결성 요구사항 모두)에대한 명세를 포함하여 안전기능을 할당하기 위한 것이다.

2 이 항 요구사항의 둘째 목적은 각 안전기능에 대해 안전무결성수준을 할당하는 것이다.

요구사항

1 필요한 기능안전성을 달성하기 위해 이용되는 안전관련 시스템을 명시하여야 한다. 필요한 리스크 감소는 다음에 의해 달성되어도 된다.

2 지정된 E/E/PE 안전관련 시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 대해 안전기능을 할당할 때, 전체 안전수명주기의 모든 단계에서 이용할 수 있는 기술과 자원이 고려되어야 한다.

3 각 안전기능을 ***5***에 따라 개발된 관련 안전무결성 요구사항과 함께 지정된 E/E/PE 안전관련 시스템에 할당하여 해당 안전기능에 필요한 리스크 감소가 달성될 수 있도록 한다. 이때, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 의해 달성되는 리스크 감소에 대해서도 고려해야 한다. 이런 할당과정은 반복이 많으며, 필요한 리스크 감소가 달성되기 어렵다고 판단되면, 구조가 변경되어야 하며 할당을 반복하여야 한다.

4 **3**에 나타난 할당은 모든 안전기능이 할당되며 각 안전기능에 대해 안전무결성 요구사항이 충족되도록(**10**에서 명시된 최우선 요구사항에 따라) 행해져야 한다.

5 각각의 안전기능에 대한 안전무결성 요구사항은 각 목표 안전무결성 파라미터가 다음 둘 중 어떠한 것에 적합한지 구분되어야 한다.

6 안전무결성 요구사항 할당은 확률을 조합하는 적절한 기법을 이용하여 수행되어야 한다.

7 할당은 공통 원인 고장의 확률을 고려하여 진행하여야 한다. E/E/PE 안전관련 시스템, 기타기술 안전관련 시스템, 외부 리스크 감소 설비가 할당에 대해 서로 독립적으로 취급되기 위해서는, 다음과 같아야 한다.

8 **7**의 모든 요구사항이 충족될 수 없다면, 안전무결성 할당을 위해서 E/E/PE 안전관련시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비를 독립적인 것으로 다루면 안 된다. 이들의 관계가 충분히 독립적(안전무결성 관점에서)이라는 것을 입증하는 분석이 시행되는 한 예외가된다.

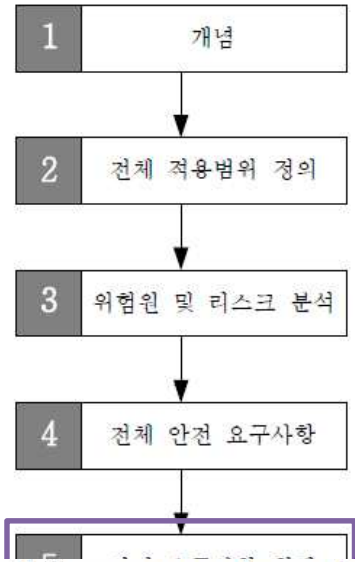
9 할당이 충분히 진행되면, (E/E/PE 안전관련 시스템(들)에 대해 할당된 각 안전기능에 대한)안전무결성 요구사항을 표 2와 표 3에 따른 안전무결성수준으로 명시하여야 한다. 그리고 안전무결성 요구사항을 측정하여 목표 안전무결성 파라미터가 다음의 어느 것인지를 나타내야 한다.

10 서로 다른 안전무결성수준을 가지는 안전기능들을 구현한 E/E/PE 안전관련 시스템은, 그안전기능들 간의 구현 독립성이 충분하다는 것을 보여줄 수 없다면, 이렇게 구현 독립성이 불충분한안전관련 하드웨어와 소프트웨어의 각 부분(Part)들은 가장 높은 안전무결성수준을 가지는 안전기능에 속하는 것으로 취급하여야 한다. 그러므로 상대적으로 가장 높은 안전무결성수준에 적용 가능한 요구사항들이 모든 부분에 적용하여야 한다.

11 안전무결성수준 4인 E/E/PE 안전관련 시스템 단독으로 구성된 구조라면, 아래 a) 또는 b)와c) 중 한쪽 기준을 충족하는 경우에만 허용되어야 한다.

12 단일한 E/E/PE 안전관련 시스템에 대해 할당되는 목표 안전무결성 고장 기준은 표 2와 표3에서 명시된 것보다 낮으면 안 된다. 다시 말해 안전관련 시스템의 운영은 다음을 고려해야 한다.

13 항 **1**~**12**에서 얻은 안전요구사항 할당에 관한 정보와 결과는 기타 가정 및 검증 근거와 함께 문서화되어야 한다.



목적

1 이 항 요구사항의 첫째 목적은 지정된 E/E/PE 안전관련 시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 전체 안전요구사항(안전기능 요구사항과 안전무결성 요구사항 모두)에대한 명세를 포함하여 안전기능을 할당하기 위한 것이다.

2 이 항 요구사항의 둘째 목적은 각 안전기능에 대해 안전무결성수준을 할당하는 것이다.

Table 2 – Safety integrity levels: target failure measures for a safety function operating in low demand mode of operation

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

Table 3 – Safety integrity levels: target failure measures for a safety function operating in high demand or continuous mode of operation

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

요구사항

1 필요한 기능안전성을 달성하기 위해 이용되는 안전관련 시스템을 명시하여야 한다. 필요한 리스크 감소는 다음에 의해 달성되어도 된다.

2 지정된 E/E/PE 안전관련 시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 대해 안전기능을 할당할 때, 전체 안전수명주기의 모든 단계에서 이용할 수 있는 기술과 자원이 고려되어야 한다.

3 각 안전기능을 ***5***에 따라 개발된 관련 안전무결성 요구사항과 함께 지정된 E/E/PE 안전관련 시스템에 할당하여 해당 안전기능에 필요한 리스크 감소가 달성될 수 있도록 한다. 이때, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비에 의해 달성되는 리스크 감소에 대해서도 고려해야 한다. 이런 할당과정은 반복이 많으며, 필요한 리스크 감소가 달성되기 어렵다고 판단되면, 구조가 변경되어야 하며 할당을 반복하여야 한다.

4 **3**에 나타난 할당은 모든 안전기능이 할당되며 각 안전기능에 대해 안전무결성 요구사항이 충족되도록(**10**에서 명시된 최우선 요구사항에 따라) 행해져야 한다.

5 각각의 안전기능에 대한 안전무결성 요구사항은 각 목표 안전무결성 파라미터가 다음 둘 중 어떠한 것에 적합한지 구분되어야 한다.

6 안전무결성 요구사항 할당은 확률을 조합하는 적절한 기법을 이용하여 수행되어야 한다.

7 할당은 공통 원인 고장의 확률을 고려하여 진행하여야 한다. E/E/PE 안전관련 시스템, 기타기술 안전관련 시스템, 외부 리스크 감소 설비가 할당에 대해 서로 독립적으로 취급되기 위해서는, 다음과 같아야 한다.

8 **7**의 모든 요구사항이 충족될 수 없다면, 안전무결성 할당을 위해서 E/E/PE 안전관련시스템, 기타 기술 안전관련 시스템, 외부 리스크 감소 설비를 독립적인 것으로 다루면 안 된다. 이들의 관계가 충분히 독립적(안전무결성 관점에서)이라는 것을 입증하는 분석이 시행되는 한 예외가된다.

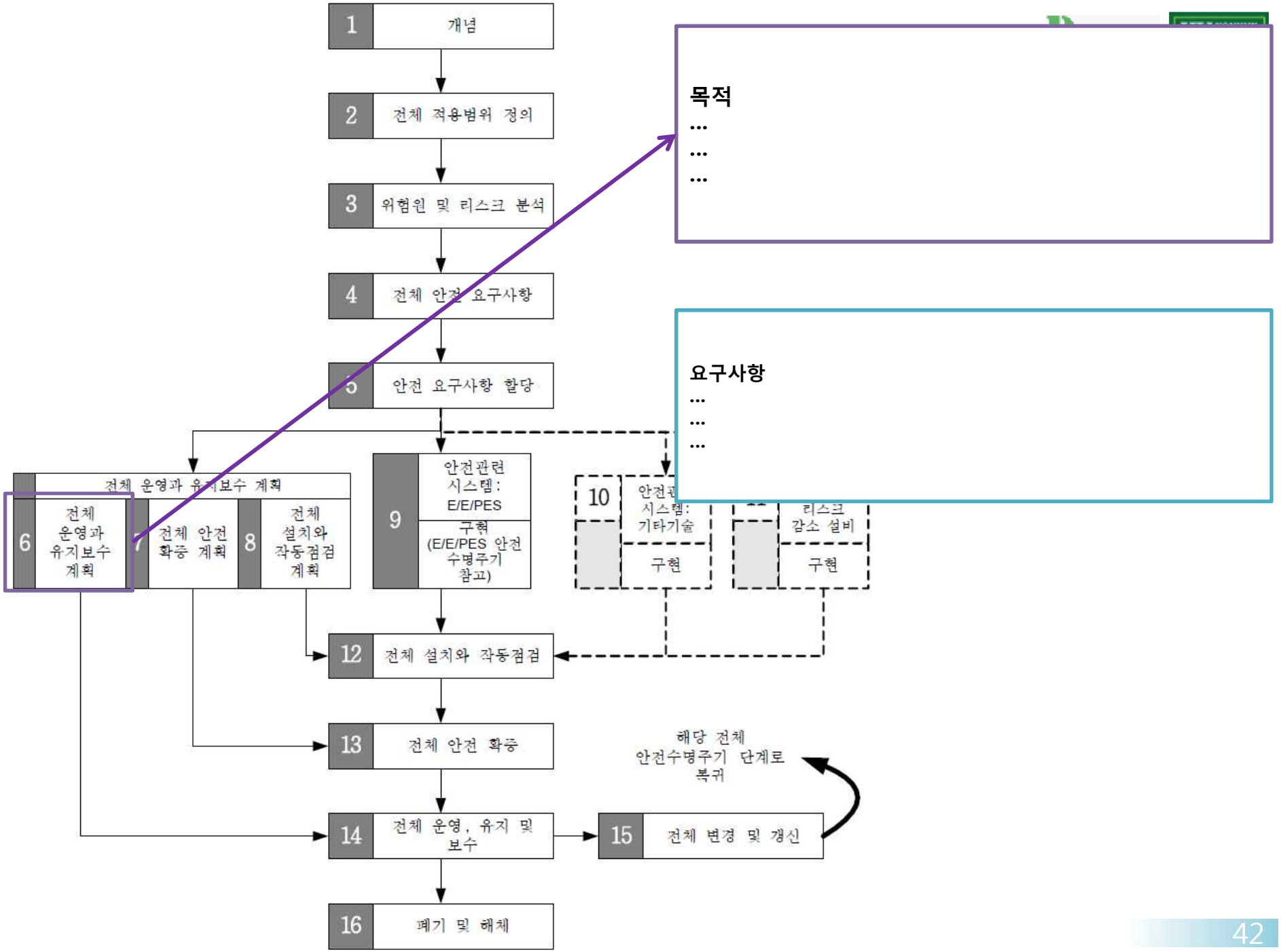
9 할당이 충분히 진행되면, (E/E/PE 안전관련 시스템(들)에 대해 할당된 각 안전기능에 대한)안전무결성 요구사항을 표 2와 표 3에 따른 안전무결성수준으로 명시하여야 한다. 그리고 안전무결성 요구사항을 측정하여 목표 안전무결성 파라미터가 다음의 어느 것인지를 나타내야 한다.

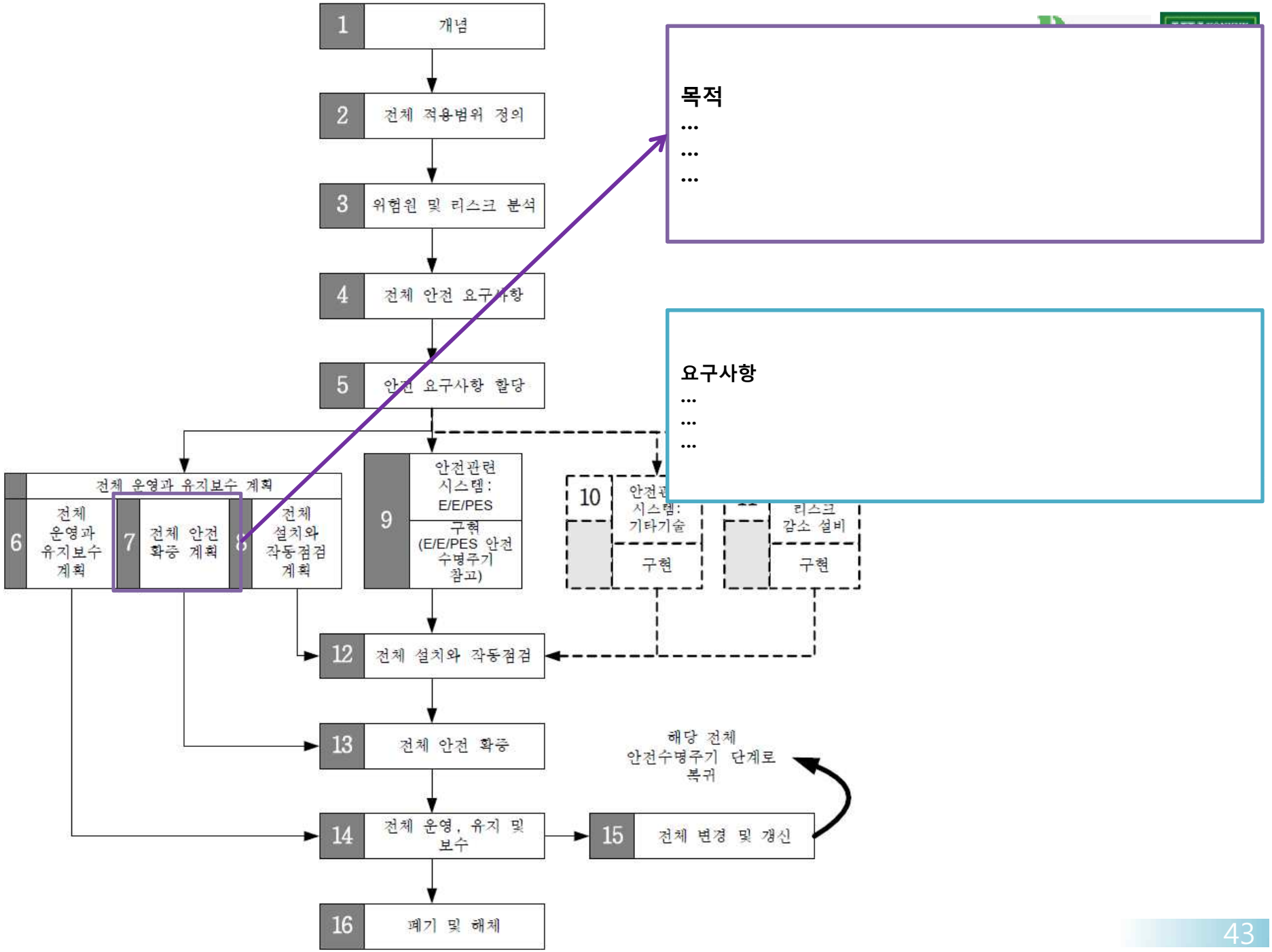
10 서로 다른 안전무결성수준을 가지는 안전기능들을 구현한 E/E/PE 안전관련 시스템은, 그안전기능들 간의 구현 독립성이 충분하다는 것을 보여줄 수 없다면, 이렇게 구현 독립성이 불충분한안전관련 하드웨어와 소프트웨어의 각 부분(Part)들은 가장 높은 안전무결성수준을 가지는 안전기능에 속하는 것으로 취급하여야 한다. 그러므로 상대적으로 가장 높은 안전무결성수준에 적용 가능한 요구사항들이 모든 부분에 적용하여야 한다.

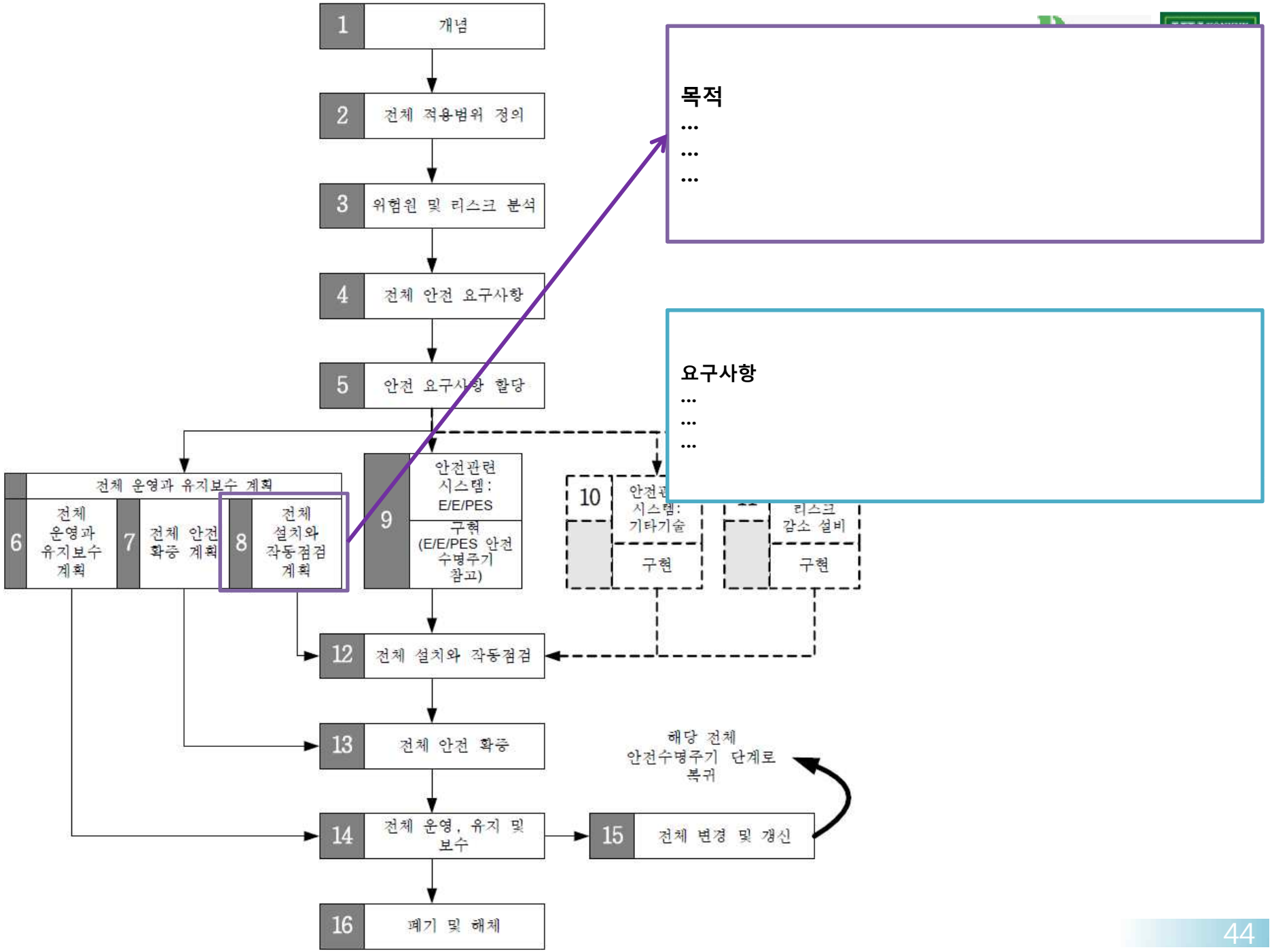
11 안전무결성수준 4인 E/E/PE 안전관련 시스템 단독으로 구성된 구조라면, 아래 a) 또는 b)와c) 중 한쪽 기준을 충족하는 경우에만 허용되어야 한다.

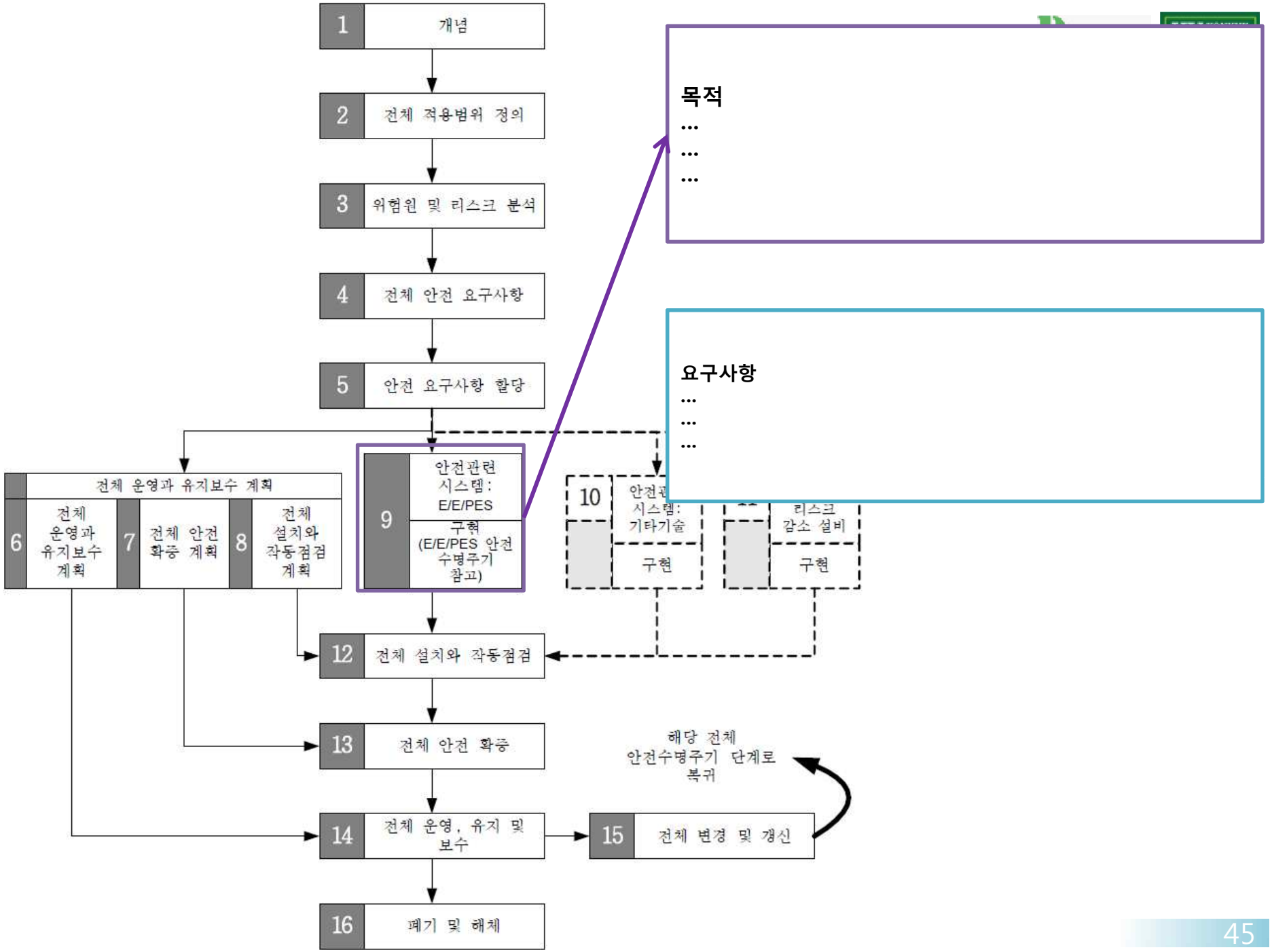
12 단일한 E/E/PE 안전관련 시스템에 대해 할당되는 목표 안전무결성 고장 기준은 표 2와 표3에서 명시된 것보다 낮으면 안 된다. 다시 말해 안전관련 시스템의 운영은 다음을 고려해야 한다.

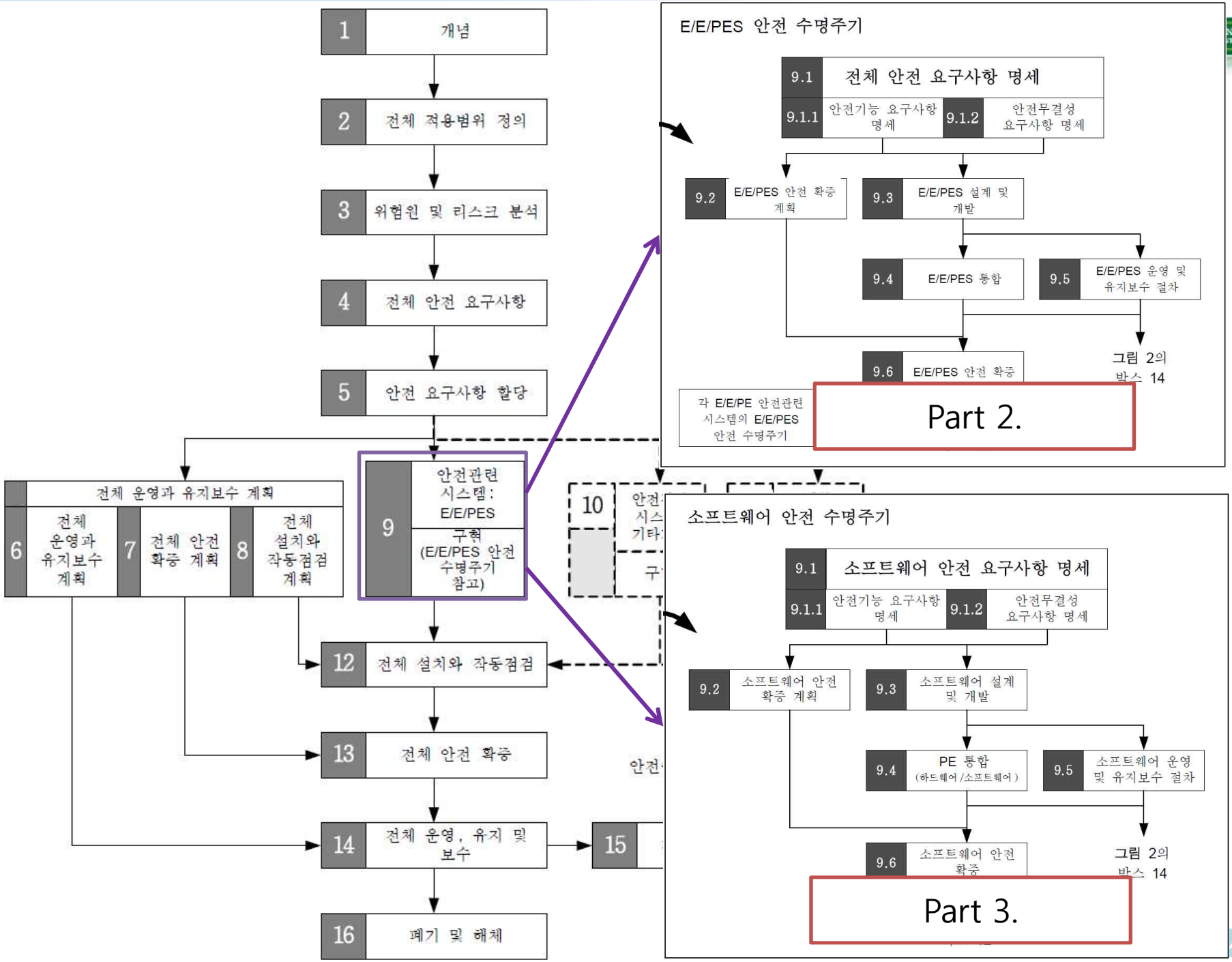
13 항 **1**~**12**에서 얻은 안전요구사항 할당에 관한 정보와 결과는 기타 가정 및 검증 근거와 함께 문서화되어야 한다.

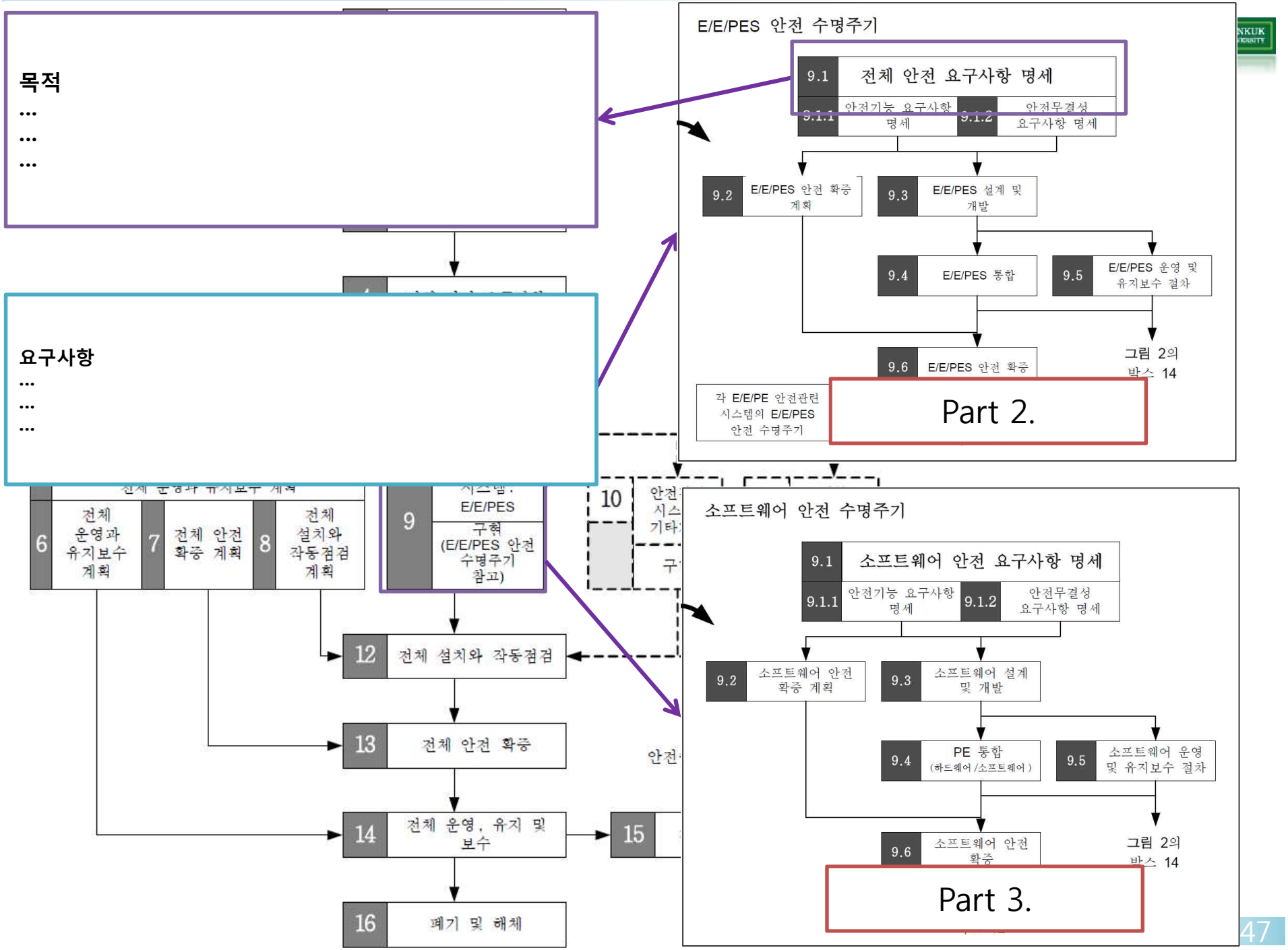

1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES
구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술
구현
리스크 감소 설비
구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체
목적
…
…
…
요구사항
…
…
…


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES
구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술
구현
리스크 감소 설비
구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체
목적
…
…
…
요구사항
…
…
…


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
목적
…
…
…
요구사항
…
…
…
전체 운영과 유지보수 계획
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동점검 계획
9 안전관련 시스템: E/E/PES
구현 (E/E/PES 안전 수명주기 참고)
10 안전관련 시스템: 기타기술
구현
리스크 감소 설비
구현
12 전체 설치와 작동점검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 안전관련 시스템: E/E/PES
구현 (E/E/PES 안전 수명주기 참고)
10 안전관 시스템: 기타기술
구현
리스크 감소 설비
구현
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15 전체 변경 및 갱신
해당 전체 안전수명주기 단계로 복귀
16 폐기 및 해체
목적
…
…
…
요구사항
…
…
…


1 개념
2 전체 적용범위 정의
3 위험원 및 리스크 분석
4 전체 안전 요구사항
5 안전 요구사항 할당
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 안전관련 시스템: E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10 안전 시스템 기타
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15
16 폐기 및 해체
E/E/PES 안전 수명주기
9.1 전체 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 E/E/PES 안전 확증 계획
9.3 E/E/PES 설계 및 개발
9.4 E/E/PES 통합
9.5 E/E/PES 운영 및 유지보수 절차
9.6 E/E/PES 안전 확증
그림 2의 박스 14
각 E/E/PE 안전관련 시스템의 E/E/PES 안전 수명주기
Part 2.
소프트웨어 안전 수명주기
9.1 소프트웨어 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 소프트웨어 안전 확증 계획
9.3 소프트웨어 설계 및 개발
9.4 PE 통합 (하드웨어 /소프트웨어)
9.5 소프트웨어 운영 및 유지보수 절차
9.6 소프트웨어 안전 확증
그림 2의 박스 14
Part 3.


목적
…
…
…
요구사항
…
…
…
E/E/PES 안전 수명주기
9.1 전체 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 E/E/PES 안전 확증 계획
9.3 E/E/PES 설계 및 개발
9.4 E/E/PES 통합
9.5 E/E/PES 운영 및 유지보수 절차
9.6 E/E/PES 안전 확증
그림 2의 박스 14
각 E/E/PE 안전관련 시스템의 E/E/PES 안전 수명주기
Part 2.
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15
16 폐기 및 해체
소프트웨어 안전 수명주기
9.1 소프트웨어 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 소프트웨어 안전 확증 계획
9.3 소프트웨어 설계 및 개발
9.4 PE 통합 (하드웨어 /소프트웨어)
9.5 소프트웨어 운영 및 유지보수 절차
9.6 소프트웨어 안전 확증
그림 2의 박스 14
Part 3.

목적

…

…

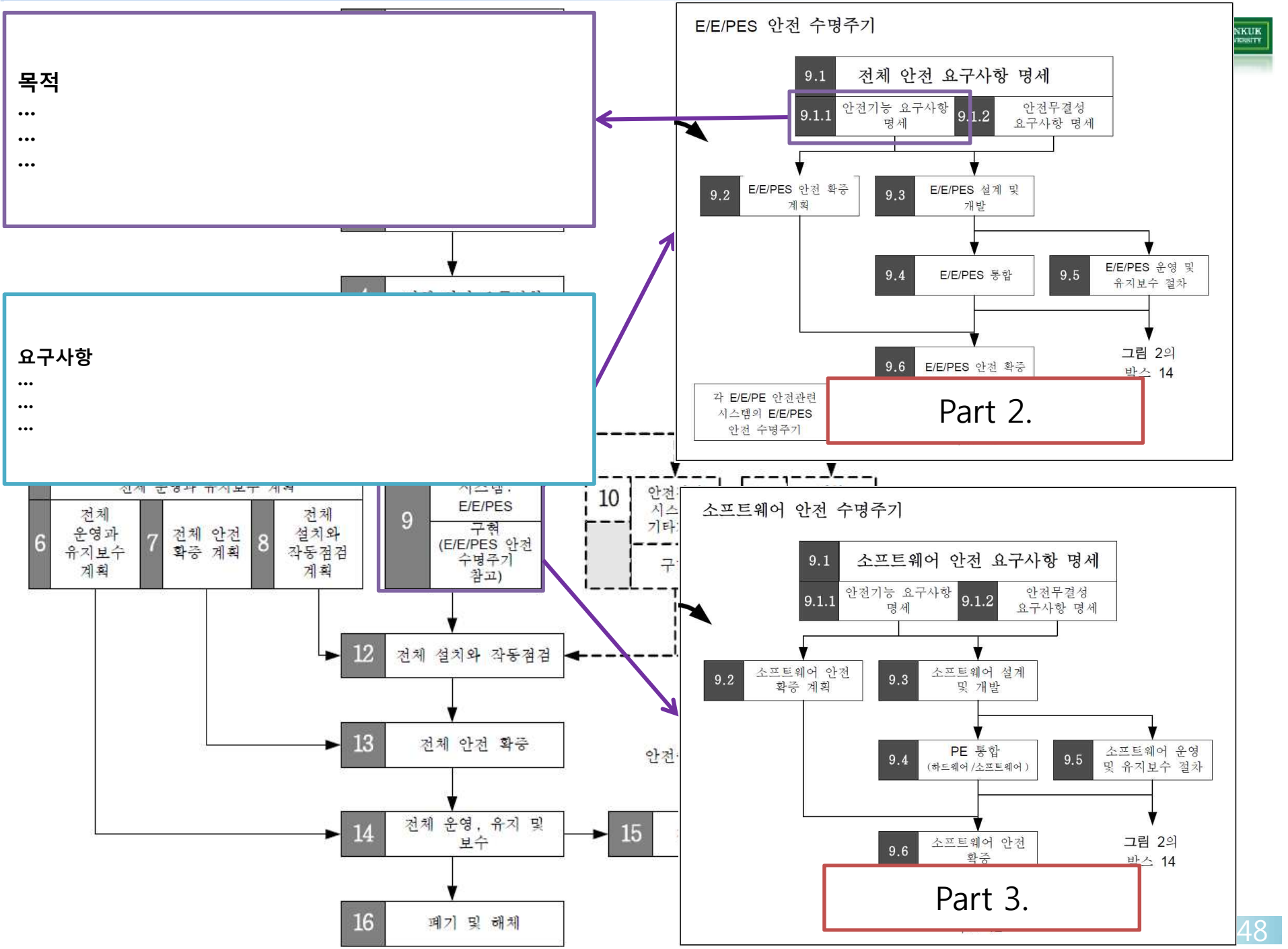
…

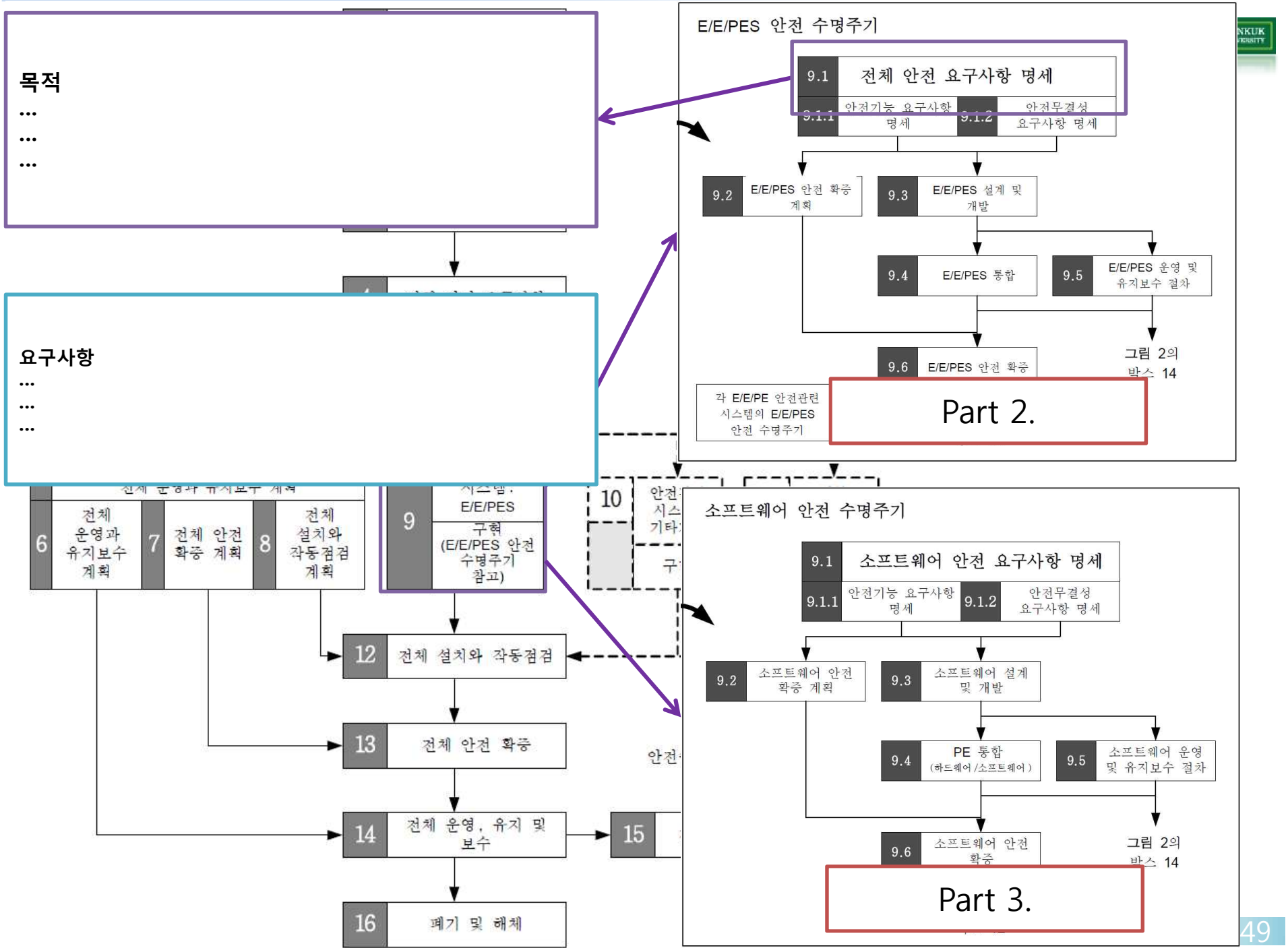
요구사항

…

…

…


E/E/PES 안전 수명주기
9.1 전체 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 E/E/PES 안전 확증 계획
9.3 E/E/PES 설계 및 개발
9.4 E/E/PES 통합
9.5 E/E/PES 운영 및 유지보수 절차
9.6 E/E/PES 안전 확증
그림 2의 박스 14
각 E/E/PE 안전관련 시스템의 E/E/PES 안전 수명주기
Part 2.
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15
16 폐기 및 해체
소프트웨어 안전 수명주기
9.1 소프트웨어 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 소프트웨어 안전 확증 계획
9.3 소프트웨어 설계 및 개발
9.4 PE 통합 (하드웨어 /소프트웨어)
9.5 소프트웨어 운영 및 유지보수 절차
9.6 소프트웨어 안전 확증
그림 2의 박스 14
Part 3.


목적
…
…
…
요구사항
…
…
…
E/E/PES 안전 수명주기
9.1 전체 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 E/E/PES 안전 확증 계획
9.3 E/E/PES 설계 및 개발
9.4 E/E/PES 통합
9.5 E/E/PES 운영 및 유지보수 절차
9.6 E/E/PES 안전 확증
그림 2의 박스 14
각 E/E/PE 안전관련 시스템의 E/E/PES 안전 수명주기
Part 2.
6 전체 운영과 유지보수 계획
7 전체 안전 확증 계획
8 전체 설치와 작동검검 계획
9 E/E/PES 구현 (E/E/PES 안전 수명주기 참고)
10
12 전체 설치와 작동검검
13 전체 안전 확증
14 전체 운영, 유지 및 보수
15
16 폐기 및 해체
소프트웨어 안전 수명주기
9.1 소프트웨어 안전 요구사항 명세
9.1.1 안전기능 요구사항 명세
9.1.2 안전무결성 요구사항 명세
9.2 소프트웨어 안전 확증 계획
9.3 소프트웨어 설계 및 개발
9.4 PE 통합 (하드웨어 /소프트웨어)
9.5 소프트웨어 운영 및 유지보수 절차
9.6 소프트웨어 안전 확증
그림 2의 박스 14
Part 3.

결론

IEC 61508은

- E/E/PE 안전관련 시스템의 **안전무결성 요구사항을 결정**하기 위하여 **리스크 기반 접근법**을 사용하고 이것을 어떻게 사용될 수 있는지에 대해 많은 예시를 다룬다.

- E/E/PE 안전관련 시스템에 의해 기능안전성이 달성되었음을 보증하는 데 필요한 활동들의 기술적인 프레임워크로서 전체 **안전 수명수기 모델**을 사용한다.

- 최초 개념부터, 위험원 분석 및 리스크 평가, 안전 요구사항 개발, 명세, 설계 및 구현, 운영 및 유지보수 그리고 변경을 통해, 최종적인 해체 및/또는 폐기까지 모든 안전 수명주기 활동을 다룬다.

IEC 61508은

- **시스템 측면**(하드웨어 및 소프트웨어로 이루어진, 안전기능들을 수행하는 모든 서브 시스템들을 포함)과 **고장 메커니즘**들(우발 하드웨어 및 시스템적인 고장)을 다룬다.

- **고장을 막기 위한**(결함 도입을 방지하기 위한) 요구사항과 **고장을 제어하기 위한**(결함 발생시에도안전을 보증하기 위한) 요구사항 둘 다 다룬다.

- 요구된 안전무결성을 달성하기 위해 필요로 하는 **기법 및 수단**을 명시한다.

Advantages of IEC 61508

- **International basic safety standard**, which describes the state-of-the-art of safety engineering in all aspects.
- The application of this standard is of great advantage, especially concerning the development of complex systems, reduces planning and development risks.
- The application of the **life-cycle model** reduces delays during development and product launch and reduces the danger, to be confronted with unpleasant surprises during the development phase.

Advantages of IEC 61508

- Product- and application independent, however risk-dependent requirements; so a comparable safety level for the protection of comparable risks is achieved
- The probability for the occurrence of faults is considered; so the measures for fault detection and control can be adjusted accordingly.
- Requires the consideration of complete safety functions.
- Is a basic standard for the development of safety-related products, which are applied within the application area of the sector standard IEC 61511, EN 50156, IEC 62061, etc.

Weakness of IEC 61508

- Large effort for documentation, which in case of development of low complex products is disadvantageous and causes considerable time delay.

- Comprehensive standard and not easy to read and to understand for a layman.