[2023 KEPIC-Week]

디지털 상용품 검증을 위한 IEC 61508 활용 가능성 평가

2023. 9. 7

한국수력원자력㈜

Contents

1. 배경 및 현황

❖ 배경

- 전 산업계의 디지털화가 진행됨에 따라 원자력발전소 설비도 디지털 부품 수가 급격하게 증가하고 있는 추세
- 그러나, 일반규격품 제작사의 기술자료(S/W코드, V&V) 제공 및 실사 기피로 CGID 수행에 대한 현실적인 애로사항 및 자재 조달에 난항
- (해외)미국 NRC는 IEC 61508 SIL인증※ 활용한 원자력 디지털기기 CGID에 대한 NEI Report TR 17-06을 승인('22.10)

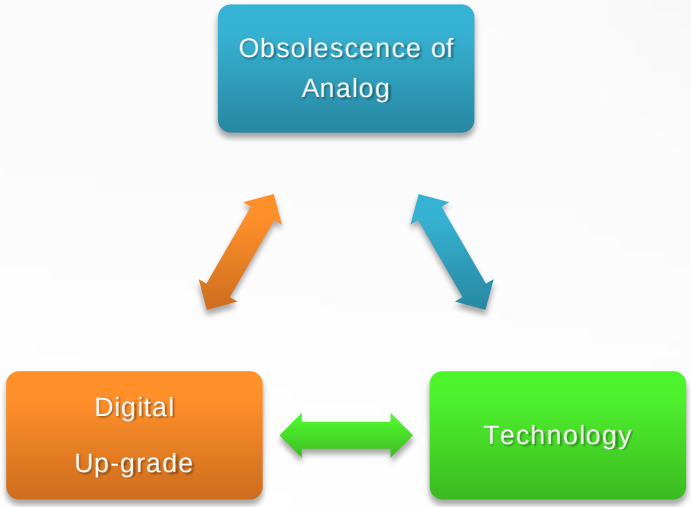
> ※ IEC 61508: 전기/전자/프로그램을 포함하는 시스템에 대한 기능 안전
> - 1998년 제정되어 자동차, 의료, 철도, 조선 등에 적용 중
> - SIL(Safety Integrity Level): 안전무결성 수준에 대한 제3자 검증 제도

- (국내)규제기관 주도 하에 상용 디지털기기 CGID 규제 지침 제정 준비

1. 배경 및 현황

❖ 디지털 변화의 흐름

- Analog 기술의 진부화
- 생산중단 품목의 증가
- Supply Chain의 변화
- 처리속도, 정비편의성의 장점
- Digital Upgrade 필요성
- 기술 경쟁력 확보



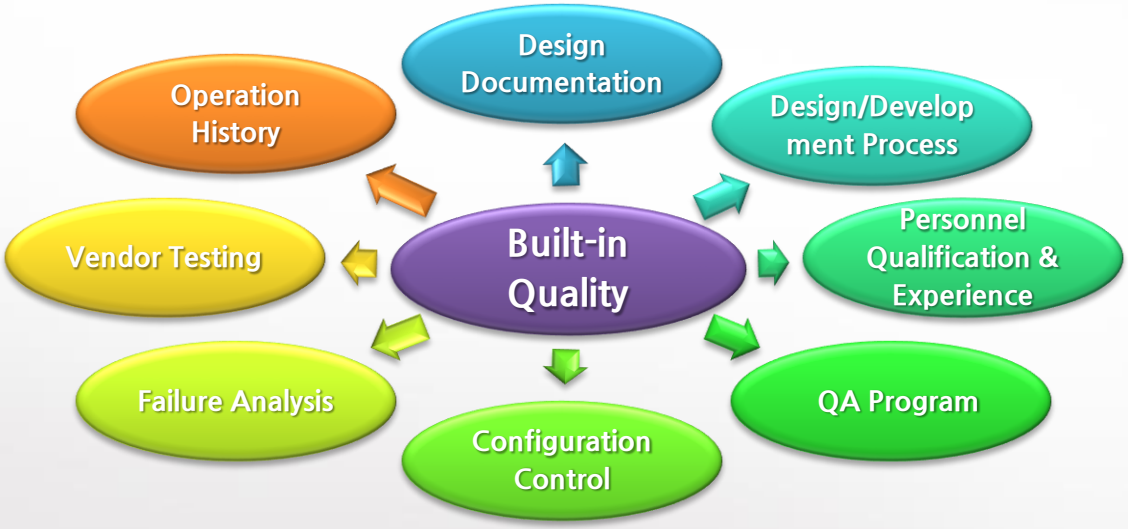
- 단위 품목(PCB, 제어기, 기록계) 교체부터
  제어/감시 계통 전체에 대한 업그레이드, 신규 디지털 기기로의 변화

1. 배경 및 현황

❖ 現 디지털기기 CGID 문제점

- EPRI TR-106439 (1996년) 이후 추가적인 가이드의 부재
- EPRI TR-106439 에 따르면, 디지털기기는 기존 H/W의 식별 및 성능 특성에 추가로 Dependability※ 특성 확인이 필수적이며
  CGID Process Method 2(Survey), 4(History)를 통해 가능함

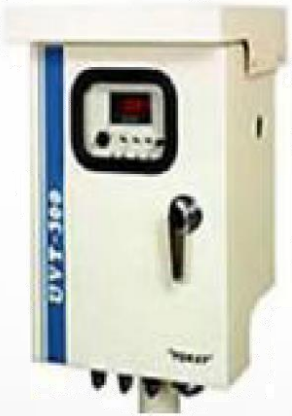
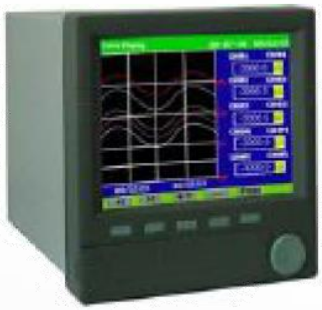
※ Dependability: Built-in Quality, Reliability, Safety, Maintainability, Problem Reporting, Configuration Control 등을 포함하는 개념



2. 가동원전 디지털기기

❖ 디지털기기 설치 현황

- 2000년대 운전을 시작한 발전소의 경우 안전관련 설비에 호기당 약 700개 이상의 디지털 부품을 포함하고 있음
- 디지털 부품의 범위: 프로그래밍 가능한 소프트웨어, 변경 가능한 상수, 수정 가능한 데이터베이스를 내장한 Programmable Device

			
Indicator	Chemical Analyzer	Recorder	Relay

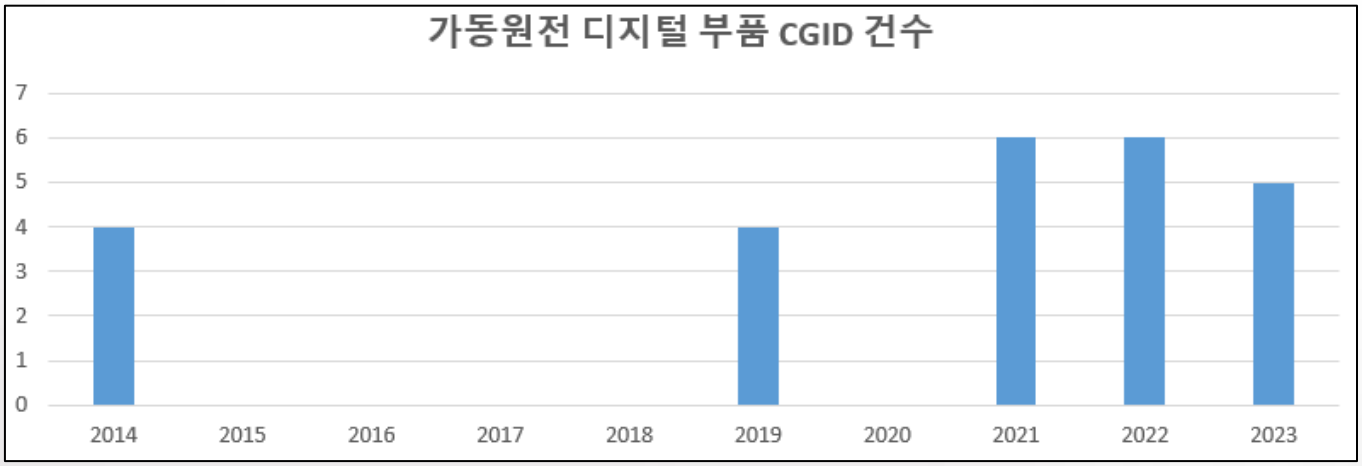
디지털부품이 포함된 기기들 (예시)

2. 가동원전 디지털기기

❖ 상용 디지털 부품 CGID

➢ 2014년 중앙연구원에서 미국 제작사 2곳 Method 2 Survey 통해 CGID를 수행한 이후 일부 기기공급자들도 수행한 이력을 확인

년도	건수	품목	제작사	검증기관
2014	4	Relay, Controller	G社 등	CRI
2019	4	Relay	G社	H社
2021	6	Relay	G社	H社
2022	6	Relay	G社	H社
2023	5(상반기)	Controller 등	W社 등	H社, Y社



3. IEC 61508 SIL Certification

❖ IEC 61508

Application Field & Standard

AUTOMOTIVE.
ISO 26262

RAILWAY APPLICATION.
EN 50126, 50128,EN 50129
IEC 62278, IEC 62279, IEC 62425

MACHINERY.
ISO 13849. IEC 62061 : Safety of machinery

PROCESS INDUSTRY.
IEC 61511 : Functional safety – Safety instrumented systems for the process industry

NUCLEAR.
IEC61513, **IEC60880**

MEDICAL.
IEC 62304 : Medical device software
IEC 60601 : Medical Electrical Equipment

OTHERS.
IEC60730, IEC66336 ..

Mother standard of functional safety standards

3. IEC 61508 SIL Certification

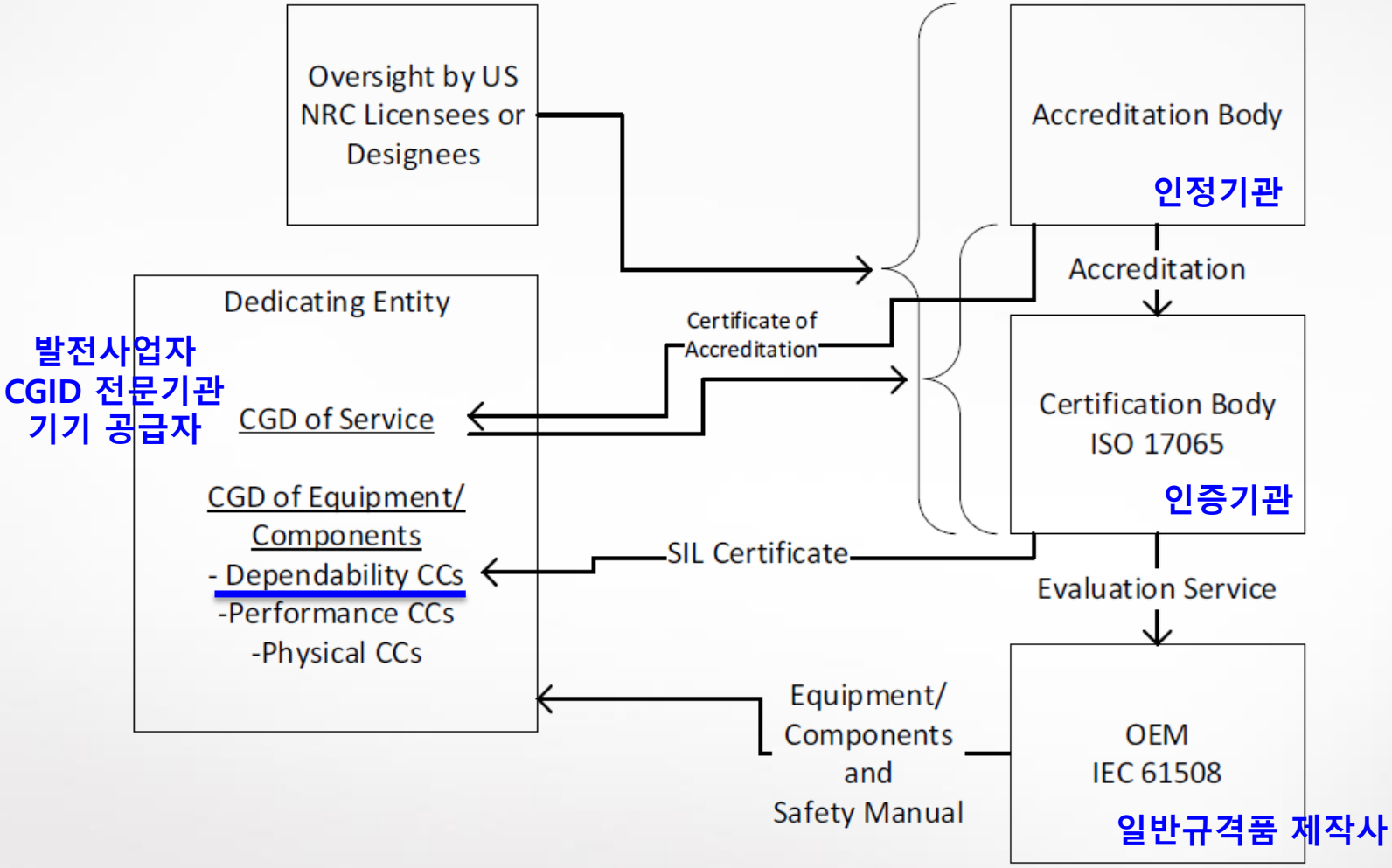
❖ Safety Integrity Level

- **S**afety **I**ntegrity **L**evel (SIL) 안전무결성수준
  - ANSI/ISAS84 01과(ANSI: 미국표준협회) IEC 61508(IEC국제전기표준기구)에서 사용되는 기준
- 4 level scale – SIL1, SIL2, SIL3, SIL4 숫자가 높을 수록 높은 무결성이 구현되어야 하므로 잠재적 위험도가 높은 시스템에 할당
  - 높은 잠재 risk를 갖는 시스템 → 높은 SIL (e.g. SIL3, SIL4) / 낮은 잠재 risk를 갖는 시스템 → 낮은 SIL (e.g. SIL1, SIL 2)
- 안전분석/위험도평가 (Hazard Analysis and Risk Assessment)를 통하여 SIL과 Safety Function이 결정됨
- 안전기능과 안전기능(Safety Function)을 구현하기 위한 안전 요구사항(Safety Requirement)에 할당
- 일반적으로 발전소, 플랜트, 대량수송(열차제어시스템) 등의 제어계통은 SIL3 이상이 요구됨 (safety critical systems)

10,000~100,000 years / 10e-8 ~10e-9 hours 위험측 고장이 발생 (사고)	SIL 4
1000~10,000 years / 10e-7 ~10e-8 hours 위험측 고장이 발생 (사고)	SIL 3
100~1000 years / 10e-6 ~10e-7 hours 위험측 고장이 발생 (사고)	SIL2
1~100 years / 10e-5 ~10e-6 hours 위험측 고장이 발생 (사고)	SIL1

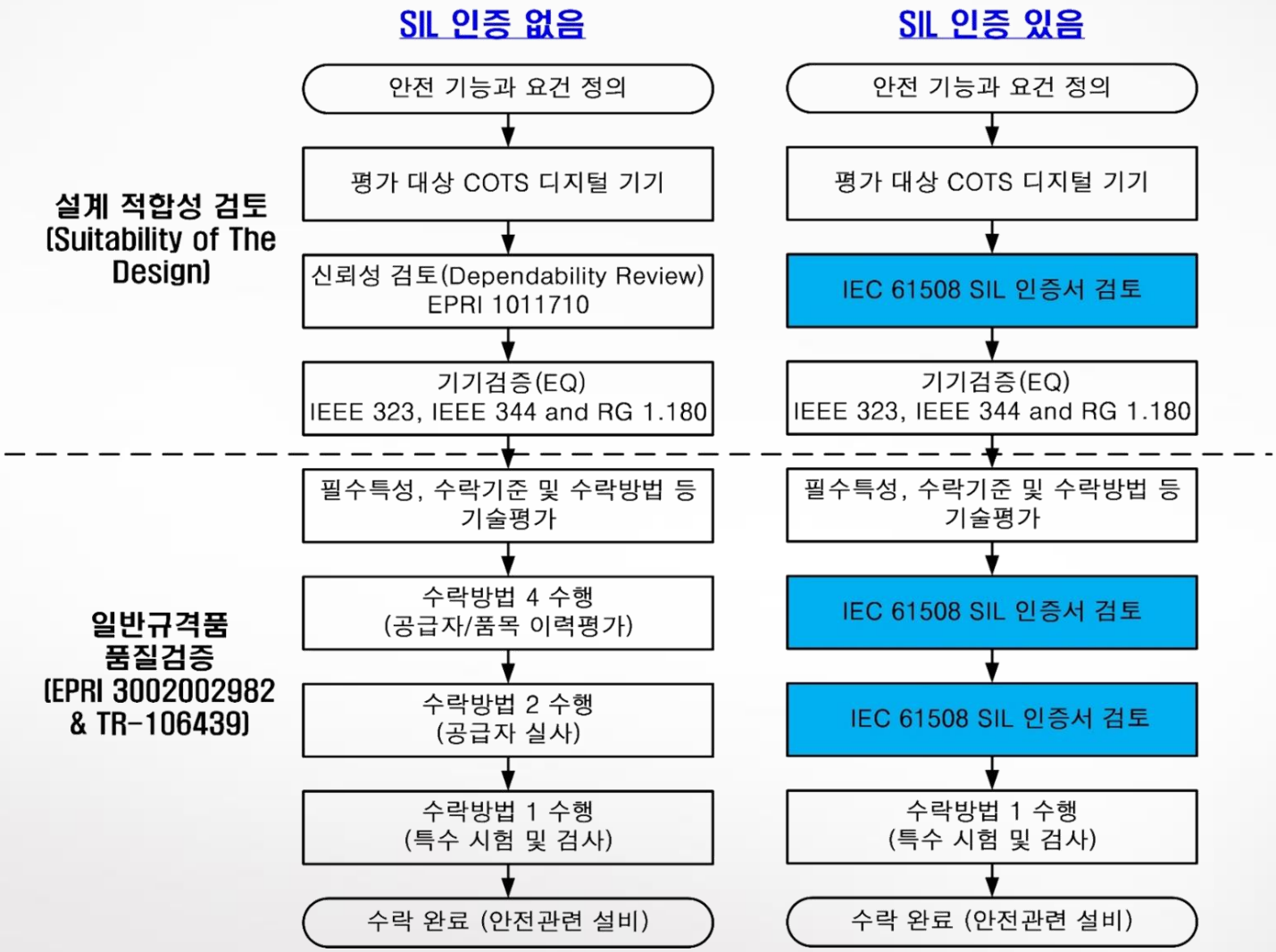
4. NEI TR 17-06

❖ IEC 61508 SIL 인증을 활용한 CGID 프로세스 제안



4. NEI TR 17-06

❖ IEC 61508 SIL 인증을 활용한 CGID 프로세스 제안



5. 시사점

❖ 기대 효과

- ➢ 사업자(원자력공급자) 입장: EPRI TR-106439 기반 CGID Method 2 Survey에 의존할 수 밖에 없었던 상황에서 선택지가 추가되므로 긍정적
- ➢ 일반규격품 공급자 입장: 단일 SIL 인증제품으로 원자력을 포함한 여러 산업계에 매출을 기대할 수 있으므로 긍정적
- ➢ 국내 원자력산업계 SIL 인증 선제적 대응으로 해외 원전 수출 기여

❖ 추가 고려사항

- ➢ 일반규격품 공급자들이 시간, 비용을 추가하여 SIL 인증 제품 개발로 선회할 유인이 필요 (원자력발전소 부품 수는 소량이고 매출 비중 낮음)
- ➢ 실효성 있는 절차를 위해서는 SIL 수준 및 인증 범위 등 합리적인 결정 필요

감사합니다.