고압전동기 보호계전기
SIL Level 3 인증

Your Permanent Partner!

전력에너지 종합 솔루션을 선도하는
지속가능한 최고의 파트너

2023. 9. 7.

와이피피㈜

목차

Ⅰ. 과제 개요

Ⅰ. 과제 개요

과제명

- 중요 고압전동기 고장보호용 스마트계전기 개발
  - 품질등급 A

개발기간

- 2020.09.01 ~ 2024.08.31 (총 48개월)

기능 및 일반성능

- 보호기능
  - 과전류(51), 순시과전류(50), 지락(50G), 과부하(49) 보호 등
- Data 수집기능
  - Waveform Recording, Event Logging, Trend Logging
- 사용환경
  - 전원 DC125V 또는 AC120V
  - 사용온도범위 : -20 ~ 60℃

신뢰성

- **S/W V&V (IEEE1012) + SIL3 (IEC61508)**

Ⅱ. IEC61508 vs. IEEE1012

Ⅱ. IEC61508 vs. IEEE 1012

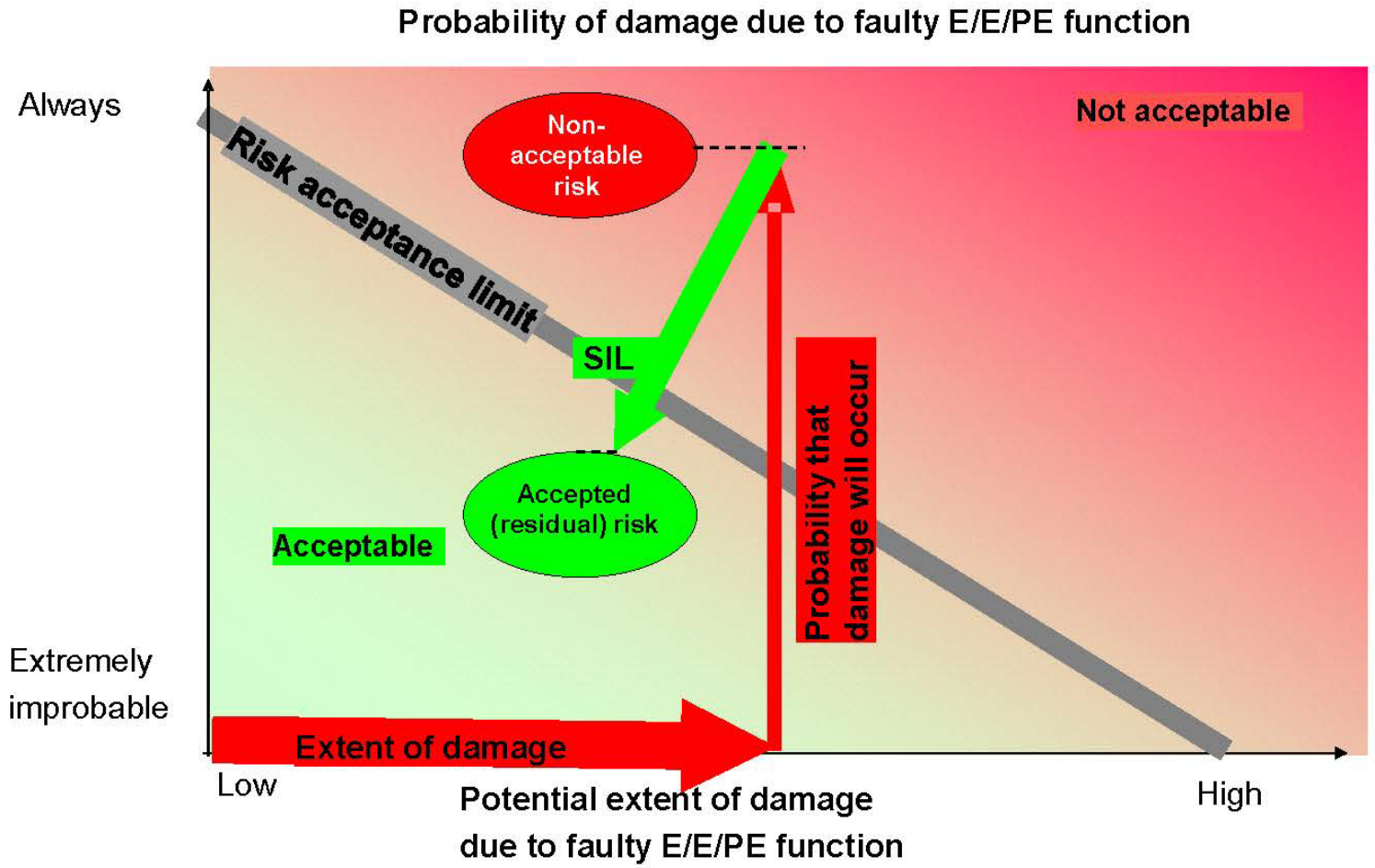
- **Functional Safety 규격**

IEC 61508
General

- ISO 26262 — Automotive
- IEC 62279 — Rail
- IEC 61511 — Process Industries
- IEC 61513 — Power Plants
- IEC 62061 — Machinery

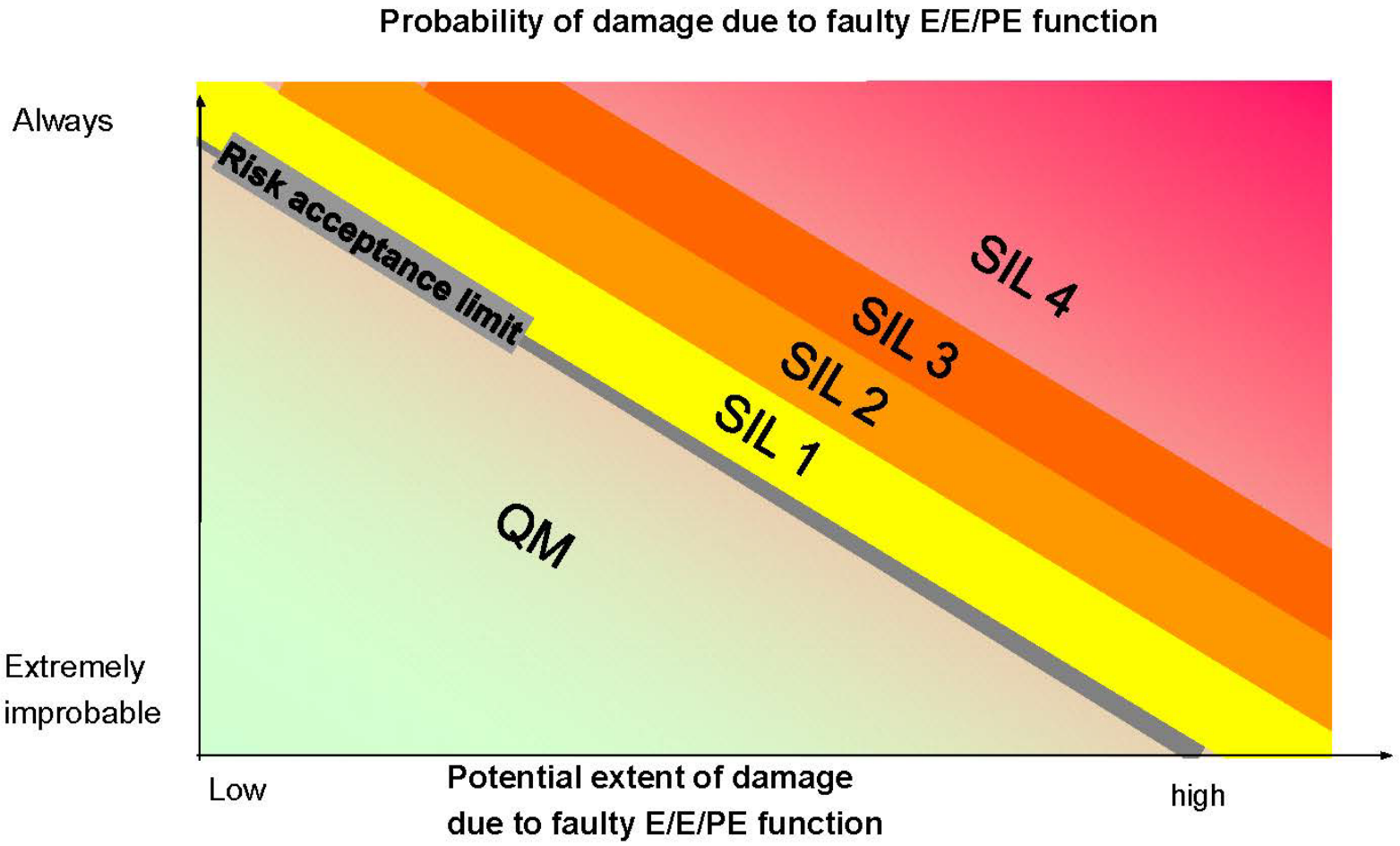
Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Functional Safety**
  → RISK를 Acceptable한 수준으로 감소시키는 것



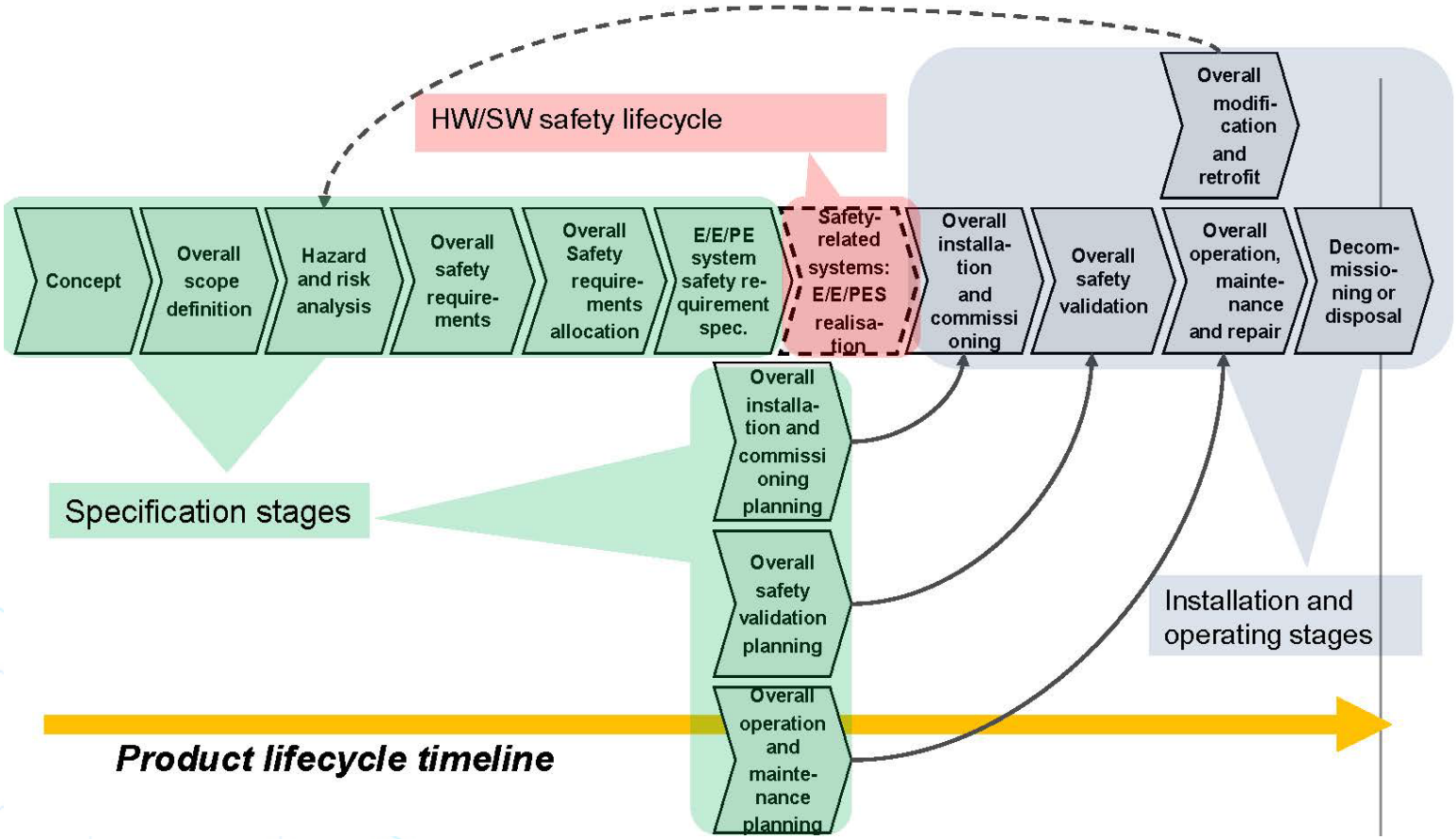
Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Safety Integrity Level**



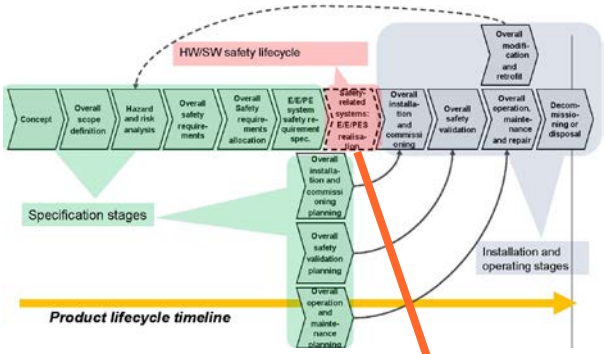
Ⅱ. IEC61508 vs. IEEE 1012

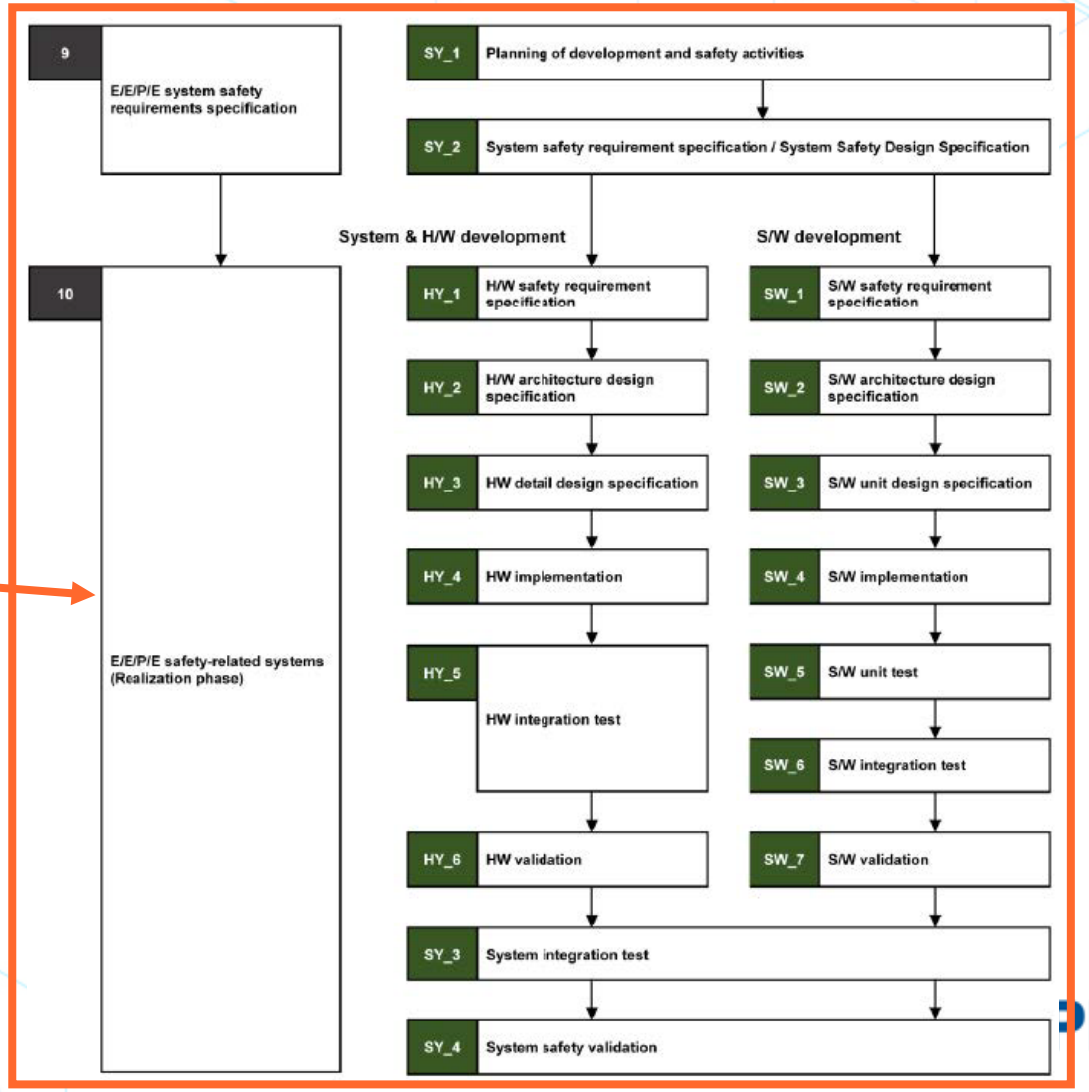
- **IEC 61508 Life Cycle**



Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Life Cycle**





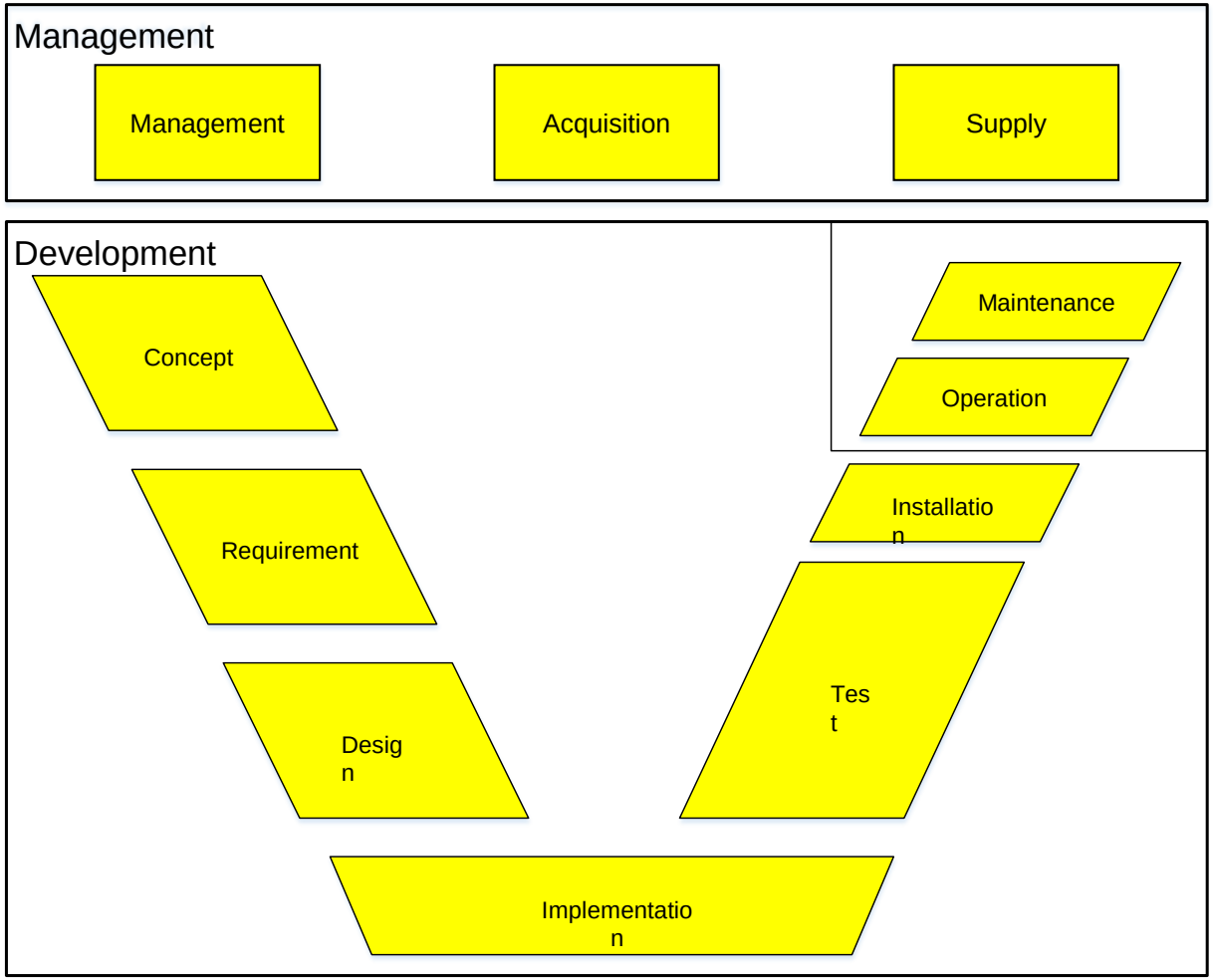
Ⅱ. IEC61508 vs. IEEE 1012

- **S/W V&V와 SIL 비교**

	Q Grade(S/W V&V)	SIL 3
AppliedStandard (적용규격)	법규 기반(원자력안전법) -Mandatory (Law)	기술규격 기반(IEC 61508) -State of the art(Technical recommendation)
Life Cycle (주명주기)	Software Development Process 기반에 Acquisition과 Supply 관점 추가적용	Software Development Process 기반에 System, Hardware 개발관점 추가적용
MajorPocus (주요관점)	Supply Manage + SW Development (법요건상) 성능시험 통과 SW V&V 수행 근거 자료(SW 존재시)	Development (System, HW, SW) 기술규격 기반 활동(IEC 61508 -V&V활동)
Integrity level (무결성수준)	IEEE 1012 기반	IEC 61508 기반
Documentation (문서화)	무결성 수준에 따라 문서가 변동됨 예) Integrity level이 1이라면 SW 시험을 전혀 하지 않아도 됨.	무결성 수준에 따라 문서가 변동되지 않음 -모든 활동은 문서화가 되어야 함 -문서는 동일하나 적용되는 기법만 변동됨

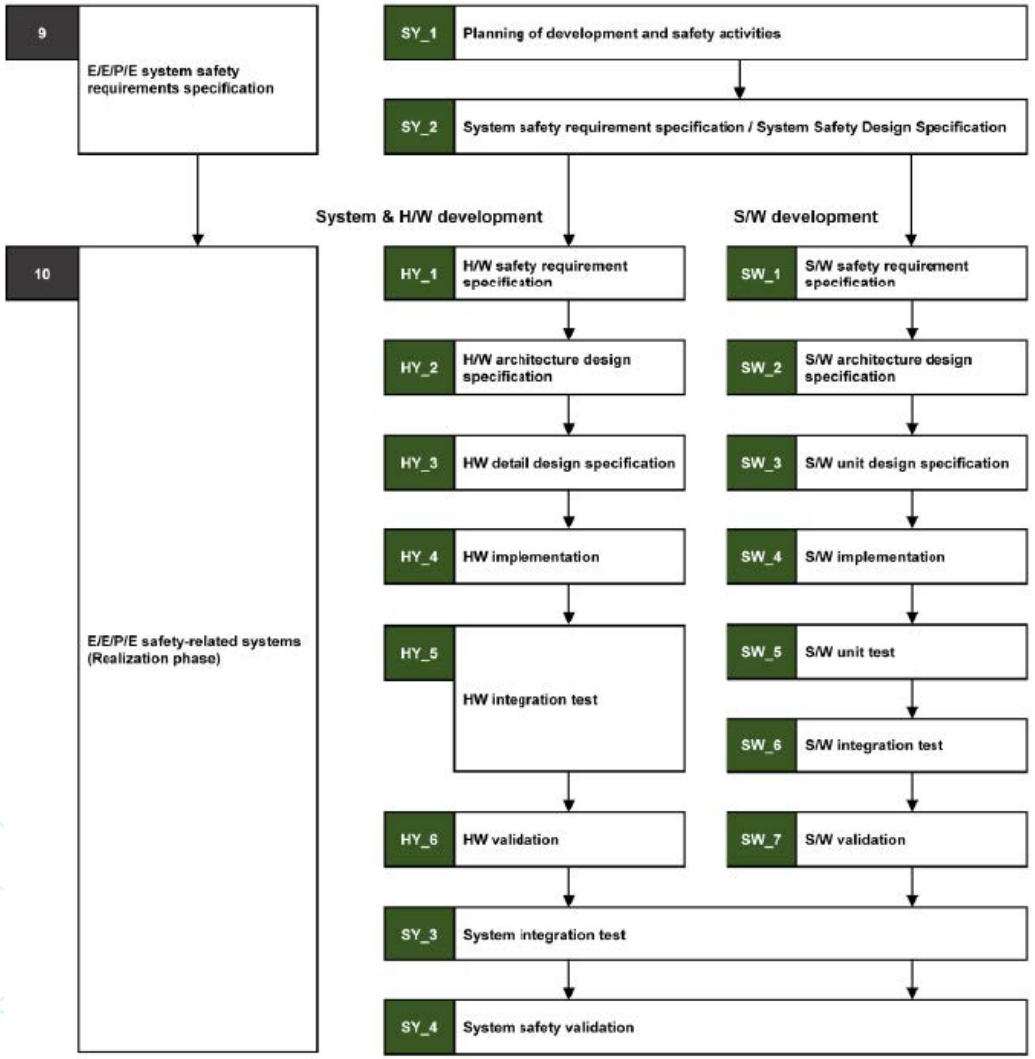
Ⅱ. IEC61508 vs. IEEE 1012

- **IEEE 1012 Life Cycle**



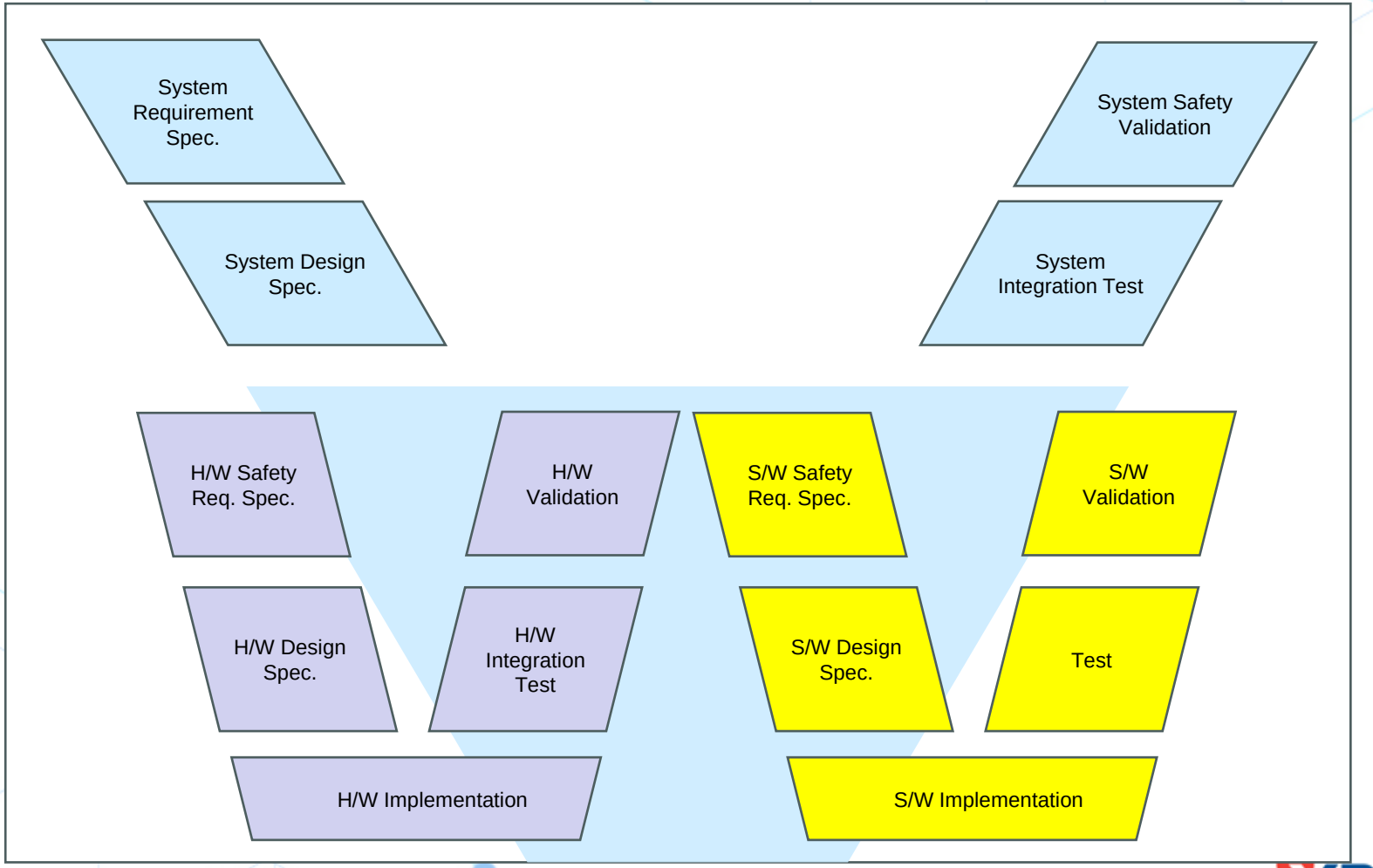
Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Life Cycle**



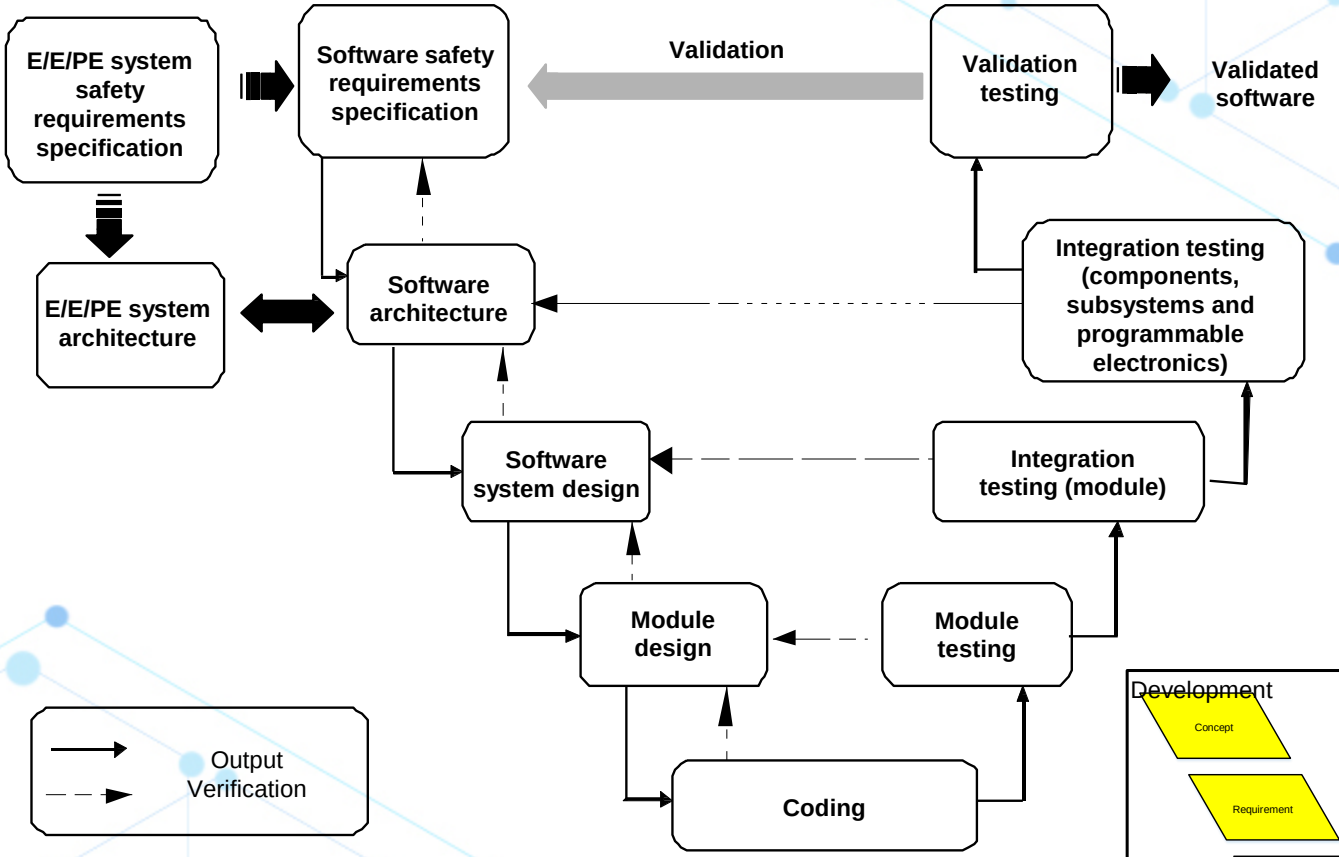
Ⅱ. IEC61508 vs. IEEE 1012

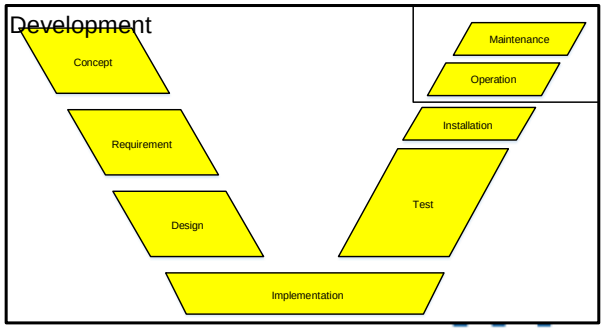
- **IEC 61508 Life Cycle**



Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Life Cycle (V-Model)**





Ⅱ. IEC61508 vs. IEEE 1012

- **Safety Integrity Level**

SIL = Safety Integrity Level

- 4-level scale (SIL 1, 2, 3, 4)
- At SIL 1 and higher, additional risk reduction measures must be taken
- SIL 4 describes the highest risk potential
- The SIL is allocated to safety functions and to the requirements for the safety functions

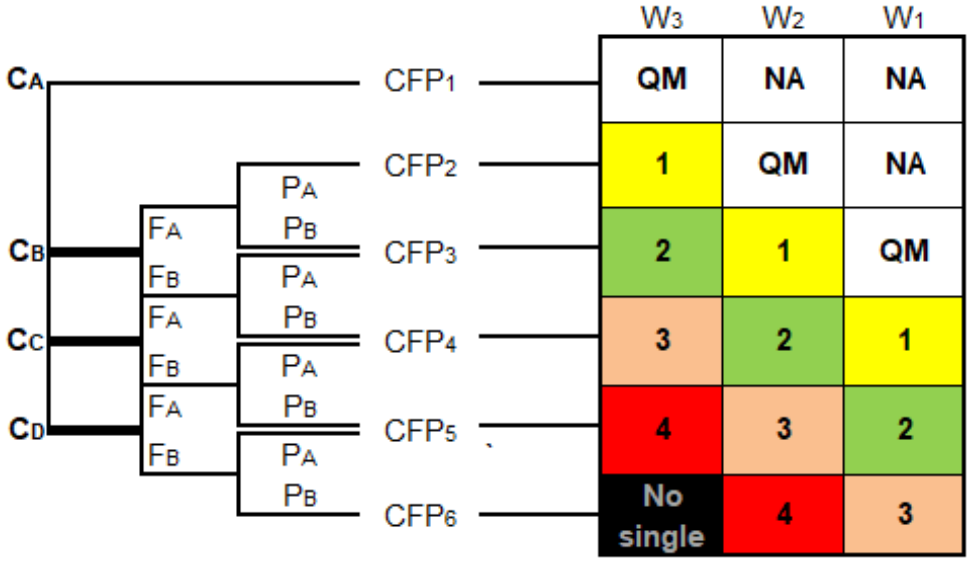
Ⅱ. IEC61508 vs. IEEE 1012

- **IEEE 1012 Risk Based Integrity Level**

		오류의 원인이 되는 작동 상태의 발생 가능성(likelihood) (가능성(likelihood)의 감소 순서)			
		Reasonable (근거 있는)	Probable (개연성 있는)	Occasional (가끔)	Infrequent (드문)
Consequence (결과)	Catastrophic (재앙적인)	4	4	4 or 3	3
	Critical (주요한)	4	4 or 3	3	2 or 1
	Marginal (주요하지 않은)	3	3 or 2	2 or 1	1
	Negligible (무시할 만 한)	2	2 or 1	1	1

Ⅱ. IEC61508 vs. IEEE 1012

- **IEC 61508 Safety Integrity Level (Graph Method)**



2.1 Consequence of the hazardous event (C);

Class	Designation	Criteria
C_1	Minor injury	단순 타박상, 멍이 듬
C_2	Major Injury(Serious permanent injury to one or more persons)	골절, 손가락 절단
C_3	Death to one or Several person	세트물 낙하에 대한 관련자 사망
C_4	Very many people killed	구조물 파손에 의한 공연장 세트물 붕괴 및 관련자 사망

2.2 Frequency of, and exposure time in, the hazardous zone (F);

Class	Designation	Criteria
F_1	Rare to more often exposure in the hazardous zone	위험한 상황에 가끔 노출
F_2	Frequent to permanent exposure in the hazardous zone	위험한 상황에 매우 빈번하게 노출

2.3 Possibility of failing to avoid the hazardous event (P);

Class	Designation	Criteria
P_1	Possible under certain conditions	위험한 상황이 발생할 경우, 경보 발생 작업자 대피할 수 있는 시간을 벌어줌
P_2	Almost impossible	위험한 상황이 발생함과 동시에 충돌사고가 발생하여 대다수의 작업자들에게 상해를 입힐 수 있음

2.4 Probability of the unwanted occurrence (W).

Class	Designation	Criteria
W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	위험 상황이 거의 발생할 가능성이 매우 낮음,
W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	위험 상황이 발생할 가능성이 약간 있음

Ⅲ. 과제 진행

Ⅲ. 과제 진행

- **Safety Integrity Level 3 (과제 요구 사항)**

➢ **Safety integrity :**

➢ **Probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time**

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	10^{-9} to < 10^{-8}
3	10^{-8} to < 10^{-7}
2	10^{-7} to < 10^{-6}
1	10^{-6} to < 10^{-5}

Ⅲ. 과제 진행

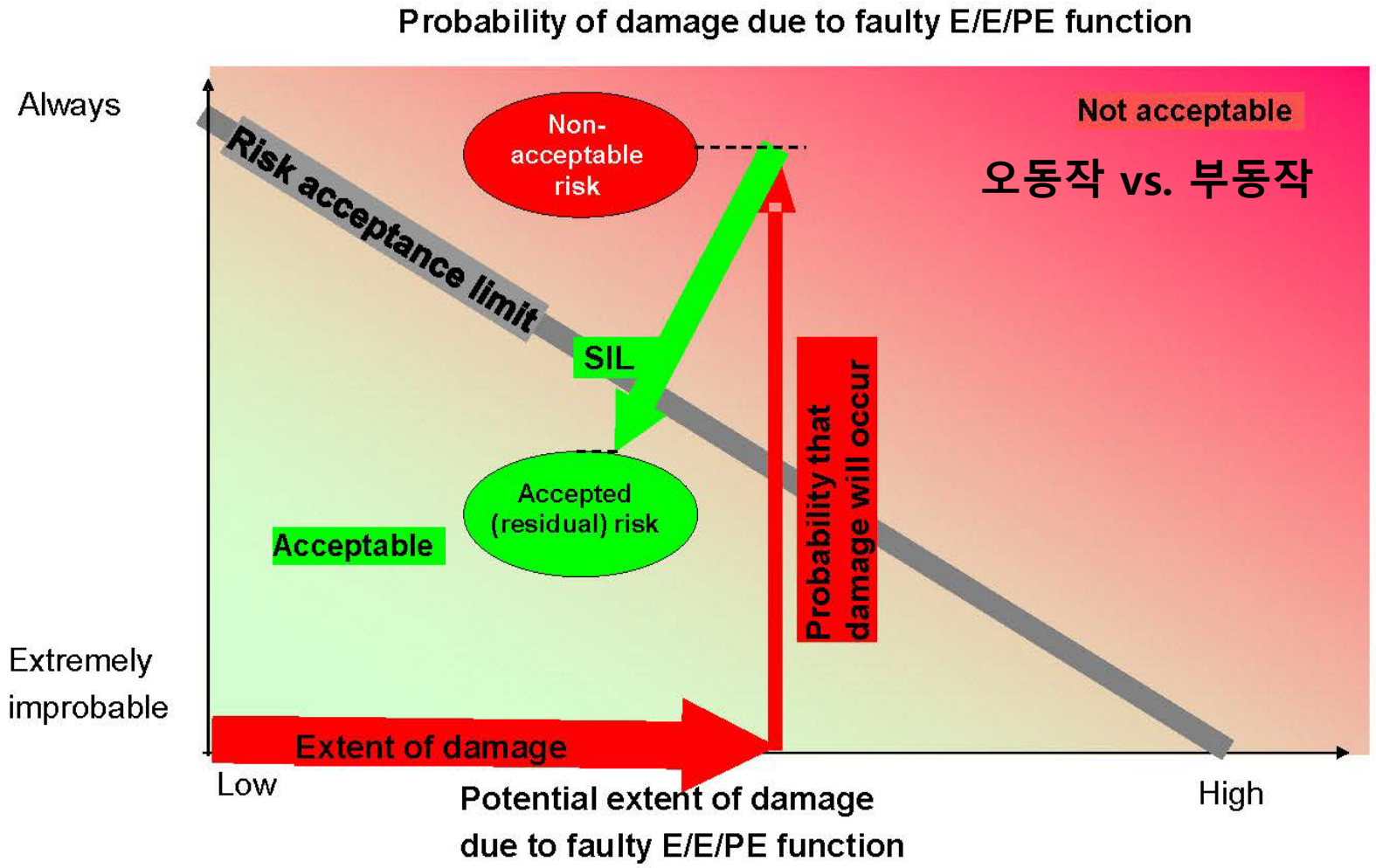
- **Hazard Analysis & Risk Assessment**
  - **Hazard : A hazard is any source of potential damage, harm or adverse health effects on something or someone.**
  - **Risk : Likelihood and severity of hazardous events.**

- **사용자 요구에 의한 SIL 적용이므로 HARA 과정 없이 SIL Class 및 Safety Function 정의**

Attribute	Description
Demand rate	High Demand mode
Average probability of a dangerous failure on demand	SIL3: PFH < 10^{-7} /h
DC and diagnostic method	Hardware fault tolerance: 2 SFF ≥ 60%/(each subsystems) with self-diagnostic measures DC ≥ 60%
MTTR / Mean Time to Restoration and MRT / Mean Repair Time	Maximum of 24 hour repair time

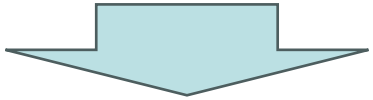
Safe Failure Fraction : Rate of failures that are neither dangerous nor undetected over the total rate
Diagnostic Coverage : Rate of detected dangerous failures over the rate of all dangerous failures

Ⅲ. 과제 진행


Probability of damage due to faulty E/E/PE function
Always
Extremely improbable
Not acceptable
오동작 vs. 부동작
Non-acceptable risk
Risk acceptance limit
SIL
Accepted (residual) risk
Acceptable
Probability that damage will occur
Extent of damage
Low
High
Potential extent of damage due to faulty E/E/PE function

Ⅲ. 과제 진행

- **Reliability of Protective Relay**
  - **Dependability:**
    - **The measure of the certainty that the relays will operate correctly for all the faults for which they are designed to operate.**
  - **Security:**
    - **The measure of the certainty that the relays will not operate incorrectly for any fault.**

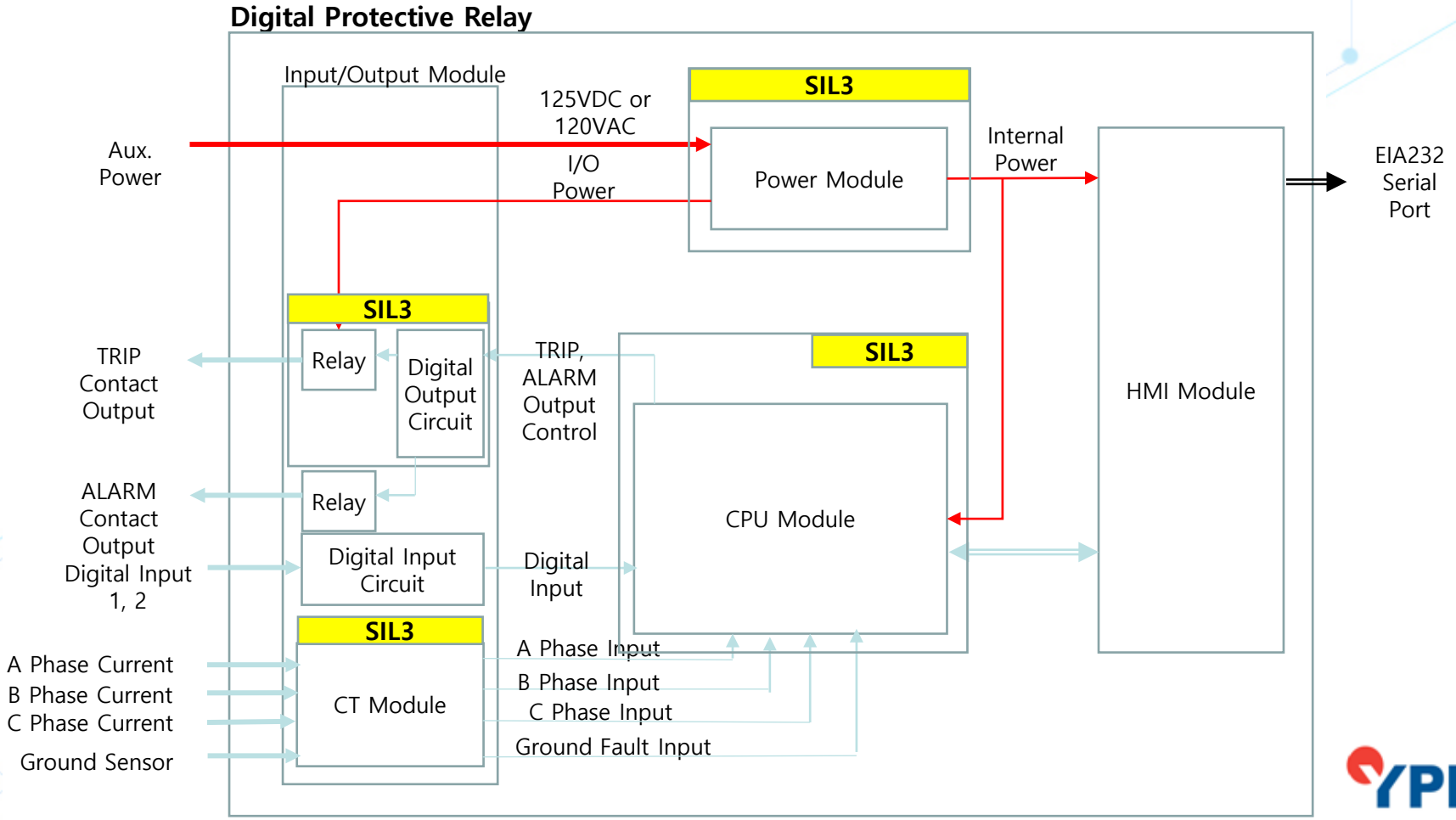


Safe State ??

Ⅲ. 과제 진행

- **Safety Function 및 Safety Related Module 정의**

➢ **Safety Function : 보호계전기는 계통에 고장이 발생했을 때 TRIP 신호를 출력해야 한다.**



Ⅲ. 과제 진행

- **Techniques and Measures**
  - Failure detection by on-line monitoring
  - Comparator
  - Majority voter
  - Tests by redundant hardware
  - Monitored redundancy
  - Electrical/electronic components with automatic check
  - Analogue signal monitoring
  - Self-test by software
  - RAM Test
  - Monitored outputs

    ……

Q & A