원자력발전소 I&C 시스템을 위한 안전성분석 기법

2013.08.20

유준범
건국대학교
http://dslab.konkuk.ac.kr

Contents

- 안전성 분석
- 안전성 분석 대상: 원자력발전소 MMIS
- 안전성 분석 기법
  - 사고 모델
    - Chain-of-Event Model vs. STAMP
  - 안전성 분석 기법
    - FTA, FMEA, HAZOP vs. STPA
- Case Study: KNICS APR-1400 ESF-CCS
- 맺음말

안전성 분석

Hazard Analysis (위험요소 분석)

Hazard Analysis	위험요소(Hazard)에 대한 다양한 분석

위험요소(Hazard)를	찾는 (Identification)	기법 (Techniques)
위험요소가	미치는 영향(Effect)을 분석하는	
사고(Accident)의	원인(Cause)을 찾는 (Identification)	
고장(Failure)의	영향을 분석 및 예측하는	

안전성 분석 (Safety Analysis)

Safety Analysis	안전성(Safety)에 대한 다양한 분석

대상?	: 안전성이 중요한 시스템
	→ 안전최우선시스템(Safety-Critical System)

→ 안전최우선시스템의 안전성에 대한 다양한 분석

안전성 분석의 例

동아일보

착륙 사고의 원인은?

조종사 실수

공항의 구조적 문제

외부의 방해 (섬광 등)

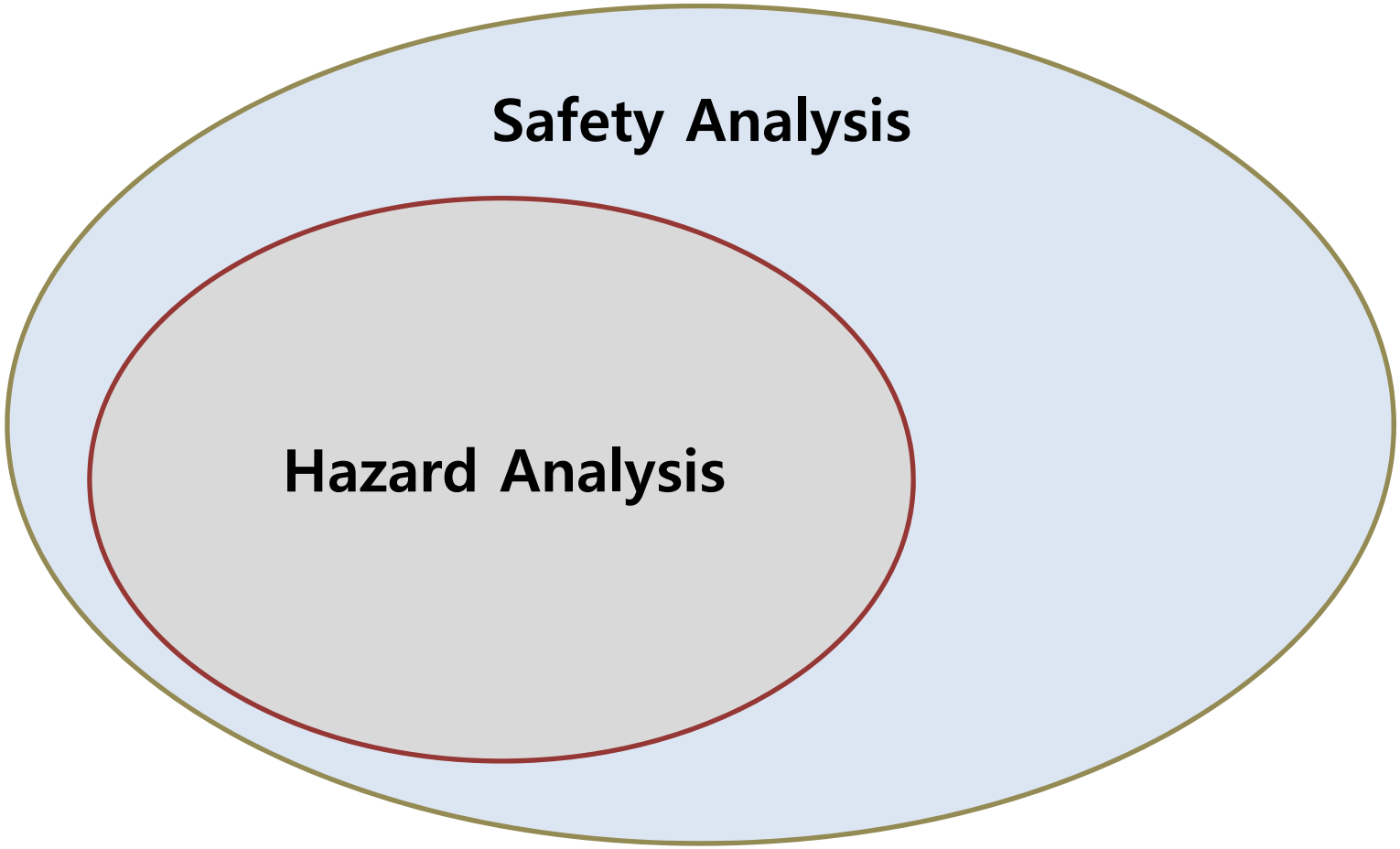
한국 문화의 특징

기타

기체 결함

관제탑 실수

공항 안전장비의 유지보수



Hazard Analysis가 Safety Analysis의 많은 부분을 차지하지만, 전체는 아니다!

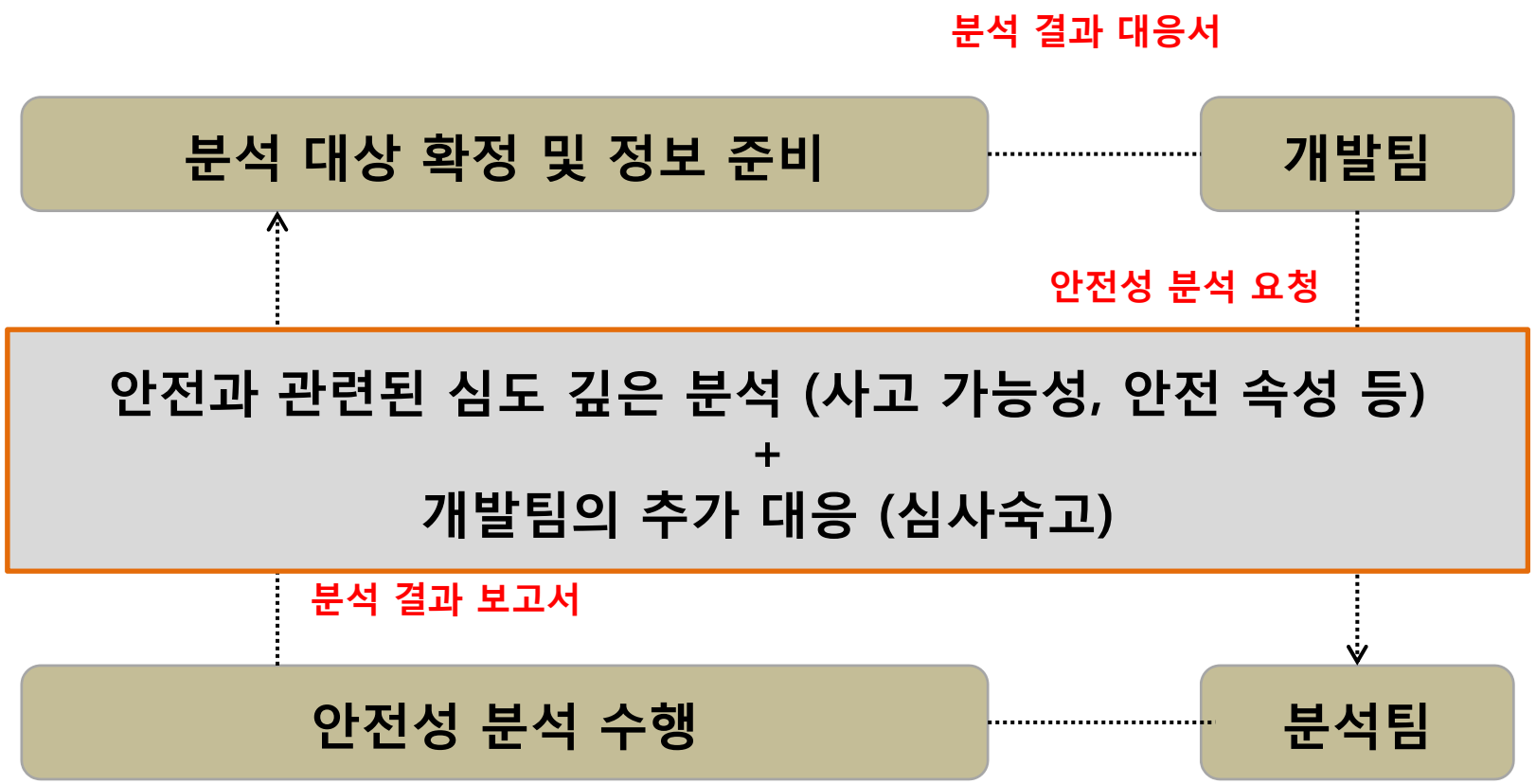
일반적으로,

Safety Analysis ≒ Hazard Analysis

정확하게는,

Safety Analysis ⊃ Hazard Analysis

안전성 분석 프로세스


분석 결과 대응서
분석 대상 확정 및 정보 준비
개발팀
안전성 분석 요청
안전과 관련된 심도 깊은 분석 (사고 가능성, 안전 속성 등)
+
개발팀의 추가 대응 (심사숙고)
분석 결과 보고서
안전성 분석 수행
분석팀

안전성 분석의 특징

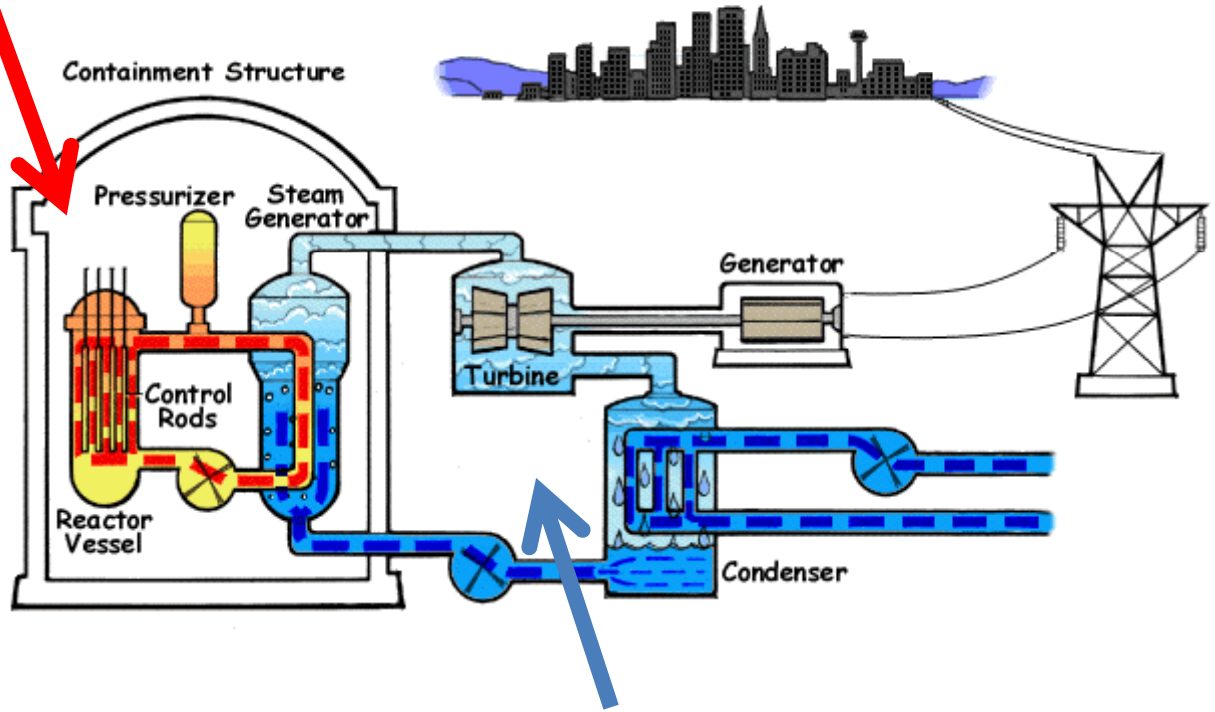
1	안전성 분석 전문가의 경험과 능력에 전적으로 의존한다.
2	안전성 분석 기법은 전문가의 체계적인 분석을 돕는 도구이다.
3	분석 대상과 목적에 따라 적절한 분석 기법을 선택해야 한다.

안전성 분석 대상:
원자력 발전소 MMIS

원자력발전소 구조

안전성 분석 대상

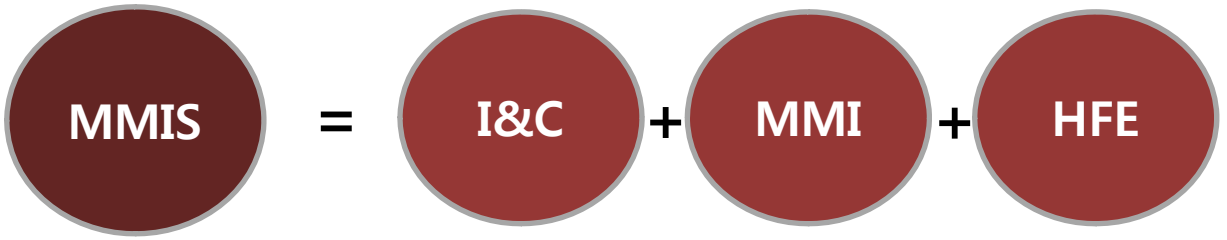
1차 계통 (방사선과 직접 관련된 계통)



2차 계통 (방사선과 관련 없는 계통)

MMIS (Man-Machine Interface System)

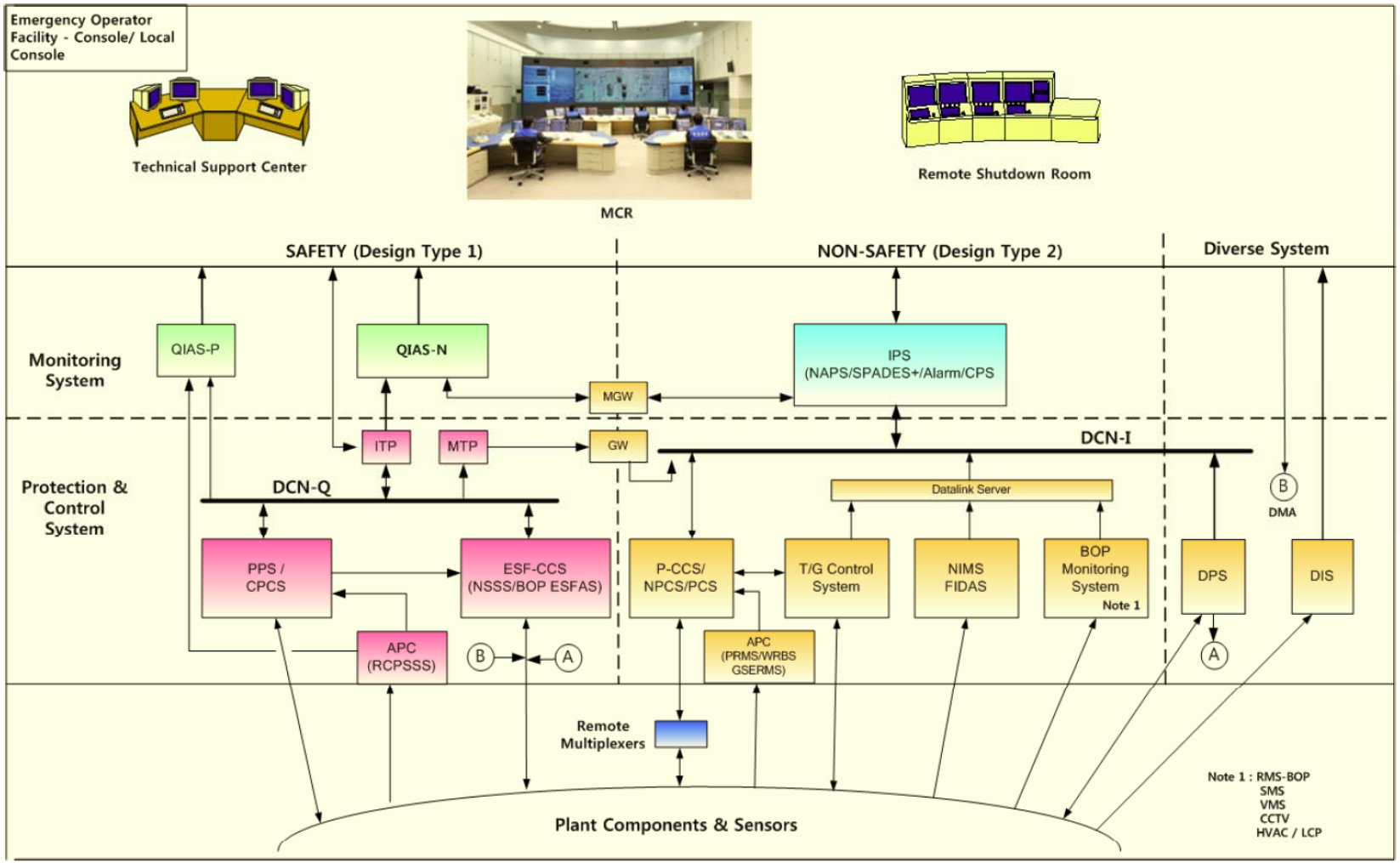
원자력발전소의 감시, 운전, 제어 및 1차적 안전을 담당하는 두뇌와 신경망



MMIS 주제어실 전경

Instrumentation & Control (I&C: 계측제어시스템)
Man-Machine Interface (MMI: 주제어실)
Human Factors Engineering (HFE: 인간공학)

KNICS I&C


Emergency Operator Facility - Console/ Local Console
Technical Support Center
MCR
Remote Shutdown Room
SAFETY (Design Type 1)
NON-SAFETY (Design Type 2)
Diverse System
Monitoring System
Protection & Control System
QIAS-P
QIAS-N
MGW
IPS (NAPS/SPADES+/Alarm/CPS
ITP
MTP
GW
DCN-I
DCN-Q
Datalink Server
B
DMA
PPS / CPCS
ESF-CCS (NSSS/BOP ESFAS)
P-CCS/ NPCS/PCS
T/G Control System
NIMS FIDAS
BOP Monitoring System
Note 1
DPS
DIS
APC (RCPSSS)
B
A
APC (PRMS/WRBS GSERMS)
A
Remote Multiplexers
Plant Components & Sensors
Note 1 : RMS-BOP
SMS
VMS
CCTV
HVAC / LCP

원자력발전소 안전계통

안전계통

과기부 고시 2002-21호 및 ANSI/ANS 51.1에 의거하여 다음에 해당되는 계통

- 안전등급 3 이상
- 전기등급 1E
- 품질등급 Q

전기등급 1E : 원자로 비상정지, 원자로건물 격리, 노심냉각 및 원자로건물과 원자로 열 제거에 필수적인 전기기기 및 계통과 외부 환경으로의 방사성물질의 대량 방출을 방지하는데 필수적인 전기기기 및 계통

품질등급 Q : 모든 전기등급 1E는 Q 등급

소프트웨어 (KOPEC 기준)

- Safety Critical (Protection) 등급
- Important to Safety 등급

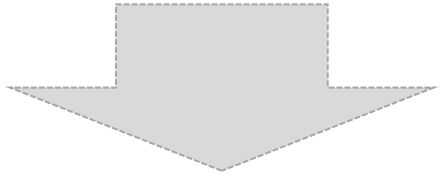
소프트웨어 (IEEE Std. 1012 기준)

- SW Level 4

원자력발전소 안전필수시스템

다음의 세 가지 조건을 동시에 만족하는 시스템

1. 1차 계통
2. SW Level 4 (IEEE Std. 1012)
3. SC (Safety-Critical) level



(1) RPS

(2) ESF-CCS

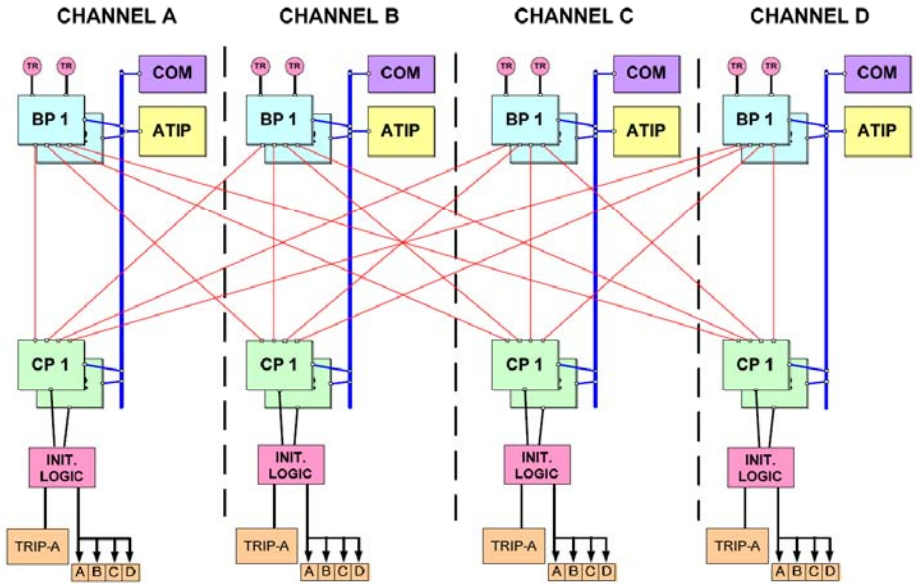
(3) CPCS

RPS (Reactor Protection System)

원자로보호계통 (RPS)

- 목적: 원자로 운전 제한치 초과 방지
- 기능: 원자로를 신속하고 확실하게 정지
- 다수의 PLC(Programmable Logic Controller)로 구현
  - 안전등급으로 인증된 기기사용
  - IEEE 603의 요건을 만족하는 설계구현
  - IEEE 7-4.3.2의 요건을 만족하는 하드웨어 및 소프트웨어 개발

PLCs in cabinets (RPS)



Channel Layout of KNICS RPS

ESF-CCS (Engineering Safety Factors – Component Control System)

공학적 안전 설비 작동 계통 (ESF-CCS)
- 목적: 설계기준 사고 時, 사고 결과를 허용치 이내로 유지
- 기능: 주요 감시변수들이 설정치에 도달하면 작동신호 발생
  - SIAS, CIAS, MSIS, CSAS, AFAS, CREVAS, FHEVAS, CPIAS

PLCs in cabinets (ESF-CCS)

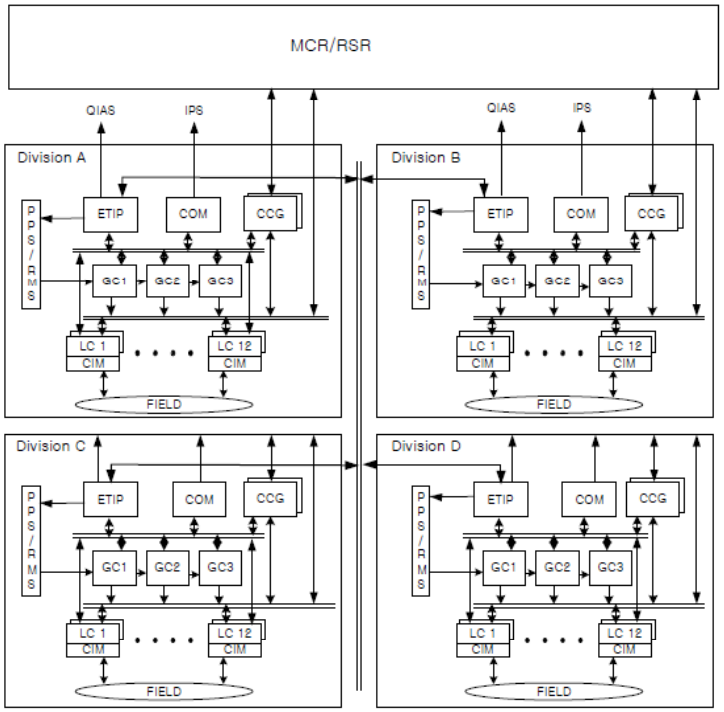


그림 6.1 공학적안전설비-기기제어계통 전체 구성 Ref [1]

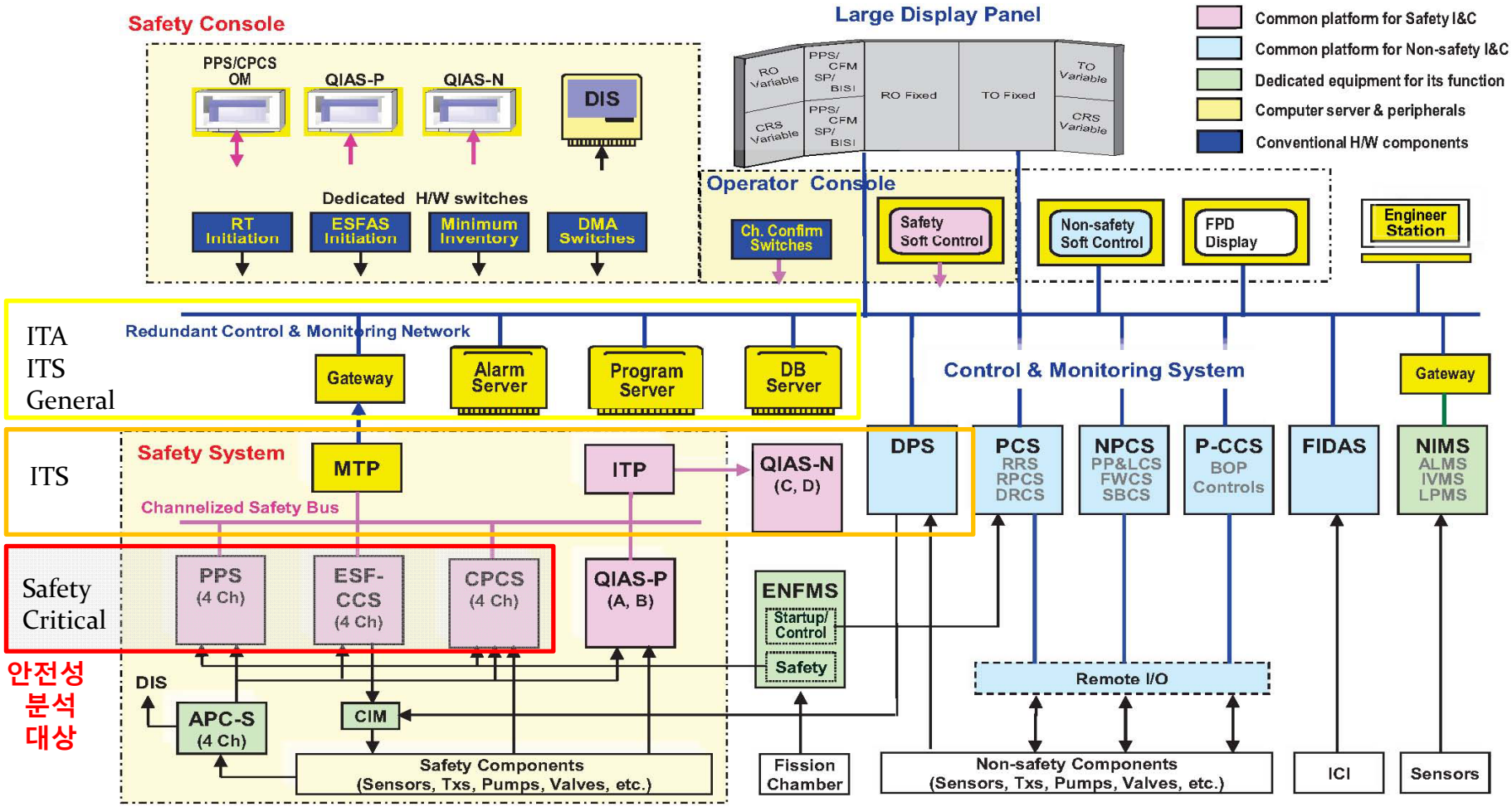
CPCS (Core Protection Calculator System)

원자로 보호 계통의 일부

- CPC 에서 핵비등 이탈율, 국부출력밀도 계산
- 저-핵비등 이탈율, 고-국부출력밀도 발생 時, DNBR/LPD 계산 없이, 원자로 트립 신호를 발전소 보호계통으로 전송(2/4논리 사용)

PLCs in cabinets (CPCS) - Westinghouse

MMIS SW 등급 분류



APC-S : Auxiliary Process Cabinet – Safety, CIM : Component Interface Module, CPCS : Core Protection Calculator System, DIS : Diverse Indication System, DMA : Diverse Manual ESF Actuation, DRCS : Digital Rod Control System, ENFMS : Ex-core Neutron Flux Monitoring System, FIDAS : Fixed In-core Detector Amplifier System, NPCS : NSSS Process Control System, PCS : Power Control System, QIAS-P/N : Qualified Indication & Alarm System - PAMI / Non-safety

안전성 분석 기법

사고 모델 (Accident Models)

Traditional model

Chain-of-Event 모델

vs.

New model

STAMP

CHAIN-OF-EVENT MODEL & TRADITIONAL HAZARD ANALYSIS

Chain-of-Event 모델

연속적인 이벤트(chains of events)로 인과관계를 구성한다.

이 이벤트의 체인을 끊을 수 있다면, 사고를 막을 수 있다.

사고(Accident)를 방지하기 위해서는

특정 원인 이벤트를 제거한다.

또는

이벤트 체인의 중간을 끊는다.

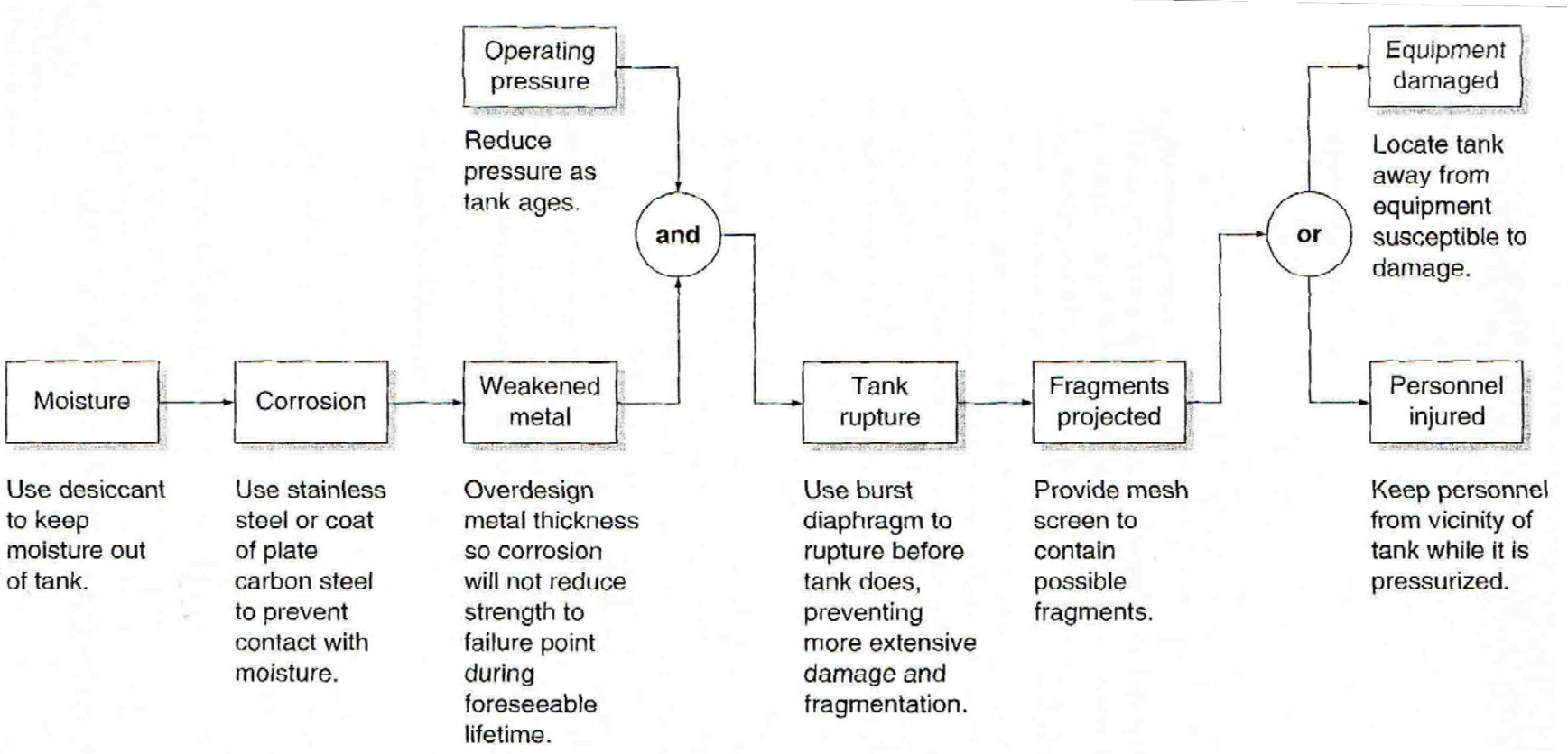


FIGURE 10.4
A model of the chain of events leading to the rupture of a pressurized tank. (Source: Adapted from Willie Hammer. *Product Safety Management and Engineering*, page 203. Englewood Cliffs, N.J.: Prentice-Hall, 1980. Reprinted with permission of Mrs. W. Hammer.)

Ref [2]

Chain-of-Event 모델의 기본 가정

사고는 컴포넌트의 고장으로 인해 발생한다.
Therefore, safety is increased by reducing component failures (*i.e.,* increasing reliability).
If components don't fail, accidents will not occur.

사고는 고장 이벤트의 연속적인 체인으로 인해 발생한다.
We can understand accidents and assess risk by looking only at the direct relationships between the events leading to the loss.

대부분의 사고는 운영자의 실수에 의해 발생한다.
Better training, rewarding good behavior and punishing bad behavior will eliminate accidents or reduce them significantly.

이벤트 체인에 기반한 확률적 위험 분석(Probabilistic risk analysis)이 안전성을 분석(communicate)하고 평가(assess)하기 위한 가장 좋은 방법이다.

대부분의 사고는 랜덤한 이벤트들이 동시에 발생함에 기인한다.

Assigning 질책 is necessary to learn from and prevent accidents or incidents.

"주된 원인(Root Cause)"을 찾을 수 있다면, 미래의 사고를 예방할 수 있다.

Chain-of-Event 모델 기반 안전성 분석 기법들

Technique	Type	Identify hazards	Identify root causes	Life-cycle phase	Qualitative/quantitative	Skill	Level of detail	I/D
PHL	CD-HAT	yes	no	CD-PD	qual.	SS	min.	I
PHA	PD-HAT	yes	partially	CD-PD	qual.	SS	Mod.	I/D
SSHA	DD-HAT	yes	yes	DD	qual.	SS, Eng, M&S	in-depth	I/D
SHA	SD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
O&SHA	OD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
HHA	HD-HAT	yes	yes	PD-DD-T	qual.	SS, Eng, M&S	in-depth	I/D
SRCA	RD-HAT	partially	no	PD-DD	qual.	SS	in-depth	–
FTA	SD-HAT DD-HAT	partially	yes	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
ETA	SD-HAT	partially	partially	PD-DD	qual./qua			
FMEA	DD-HAT	partially	partially	PD-DD	qual./qua			
FaHA	DD-HAT	yes	partially	PD-DD	qual.			
FuHA	SD-HAT DD-HAT	yes	partially	CD-PD-DD	qual.			
SCA	SD-HAT DD-HAT	partially	yes	DD	qual.			
PNA	SD-HAT DD-HAT	partially	no	PD-DD	qual./qua			
MA	SD-HAT DD-HAT	partially	no	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
BA	SD-HAT	yes	partially	PD-DD	qual.	SS, Eng	Mod.	I
BPA	DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	in-depth	D
HAZOP	SD-HAT DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	Mod.	I
CCA	SD-HAT DD-HAT	yes	partially	PD-DD	qual./quant.	SS, Eng, M&S	Mod.	D
CCFA	SD-HAT DD-HAT	yes	partially	PD-DD	qual.	SS, Eng, M&S	Mod.	D
MORT	SD-HAT DD-HAT	yes	partially	PD-DD	qual./quant.	SS, M&S	Mod.	D
SWSA	SD-HAT DD-HAT	yes	partially	CD-PD	qual.	SS, Eng, M&S	Mod.	–

- 매우 오래됨 (30년 이상)
- 대부분 시스템을 대상으로
- 다양한 적용 단계
- 다양한 장단점 및 특징

CD – conceptual design; PD – preliminary design; DD – detailed design; T – testing; SS – system safety; Eng – engineering electrical/mechanical/software; M&S – math & statistics; Mod. – moderate to in-depth. **Ref [3]**

Fault Tree Analysis (FTA)

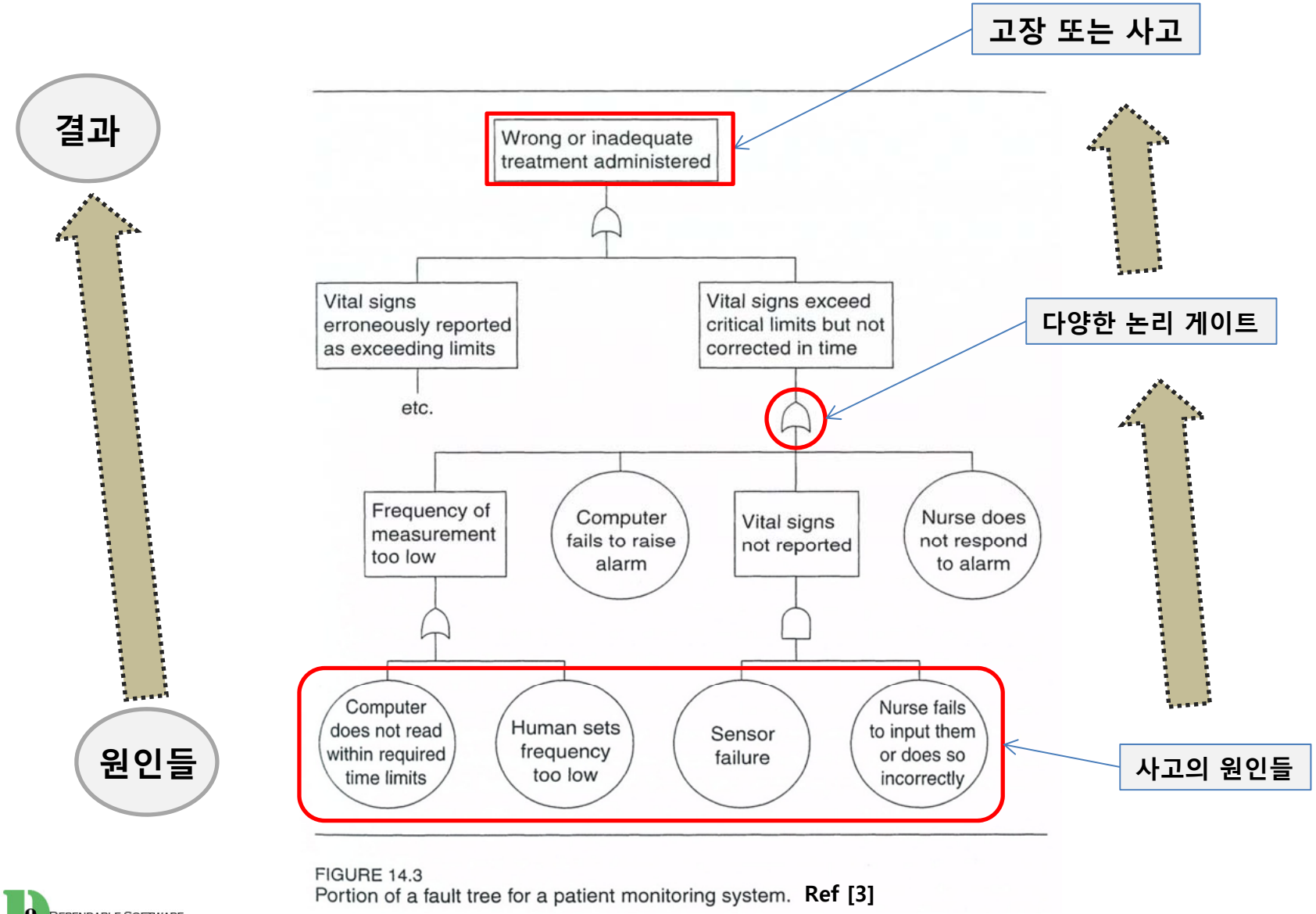


FIGURE 14.3
Portion of a fault tree for a patient monitoring system. **Ref [3]**

Failure Mode and Effect Analysis (FMEA)

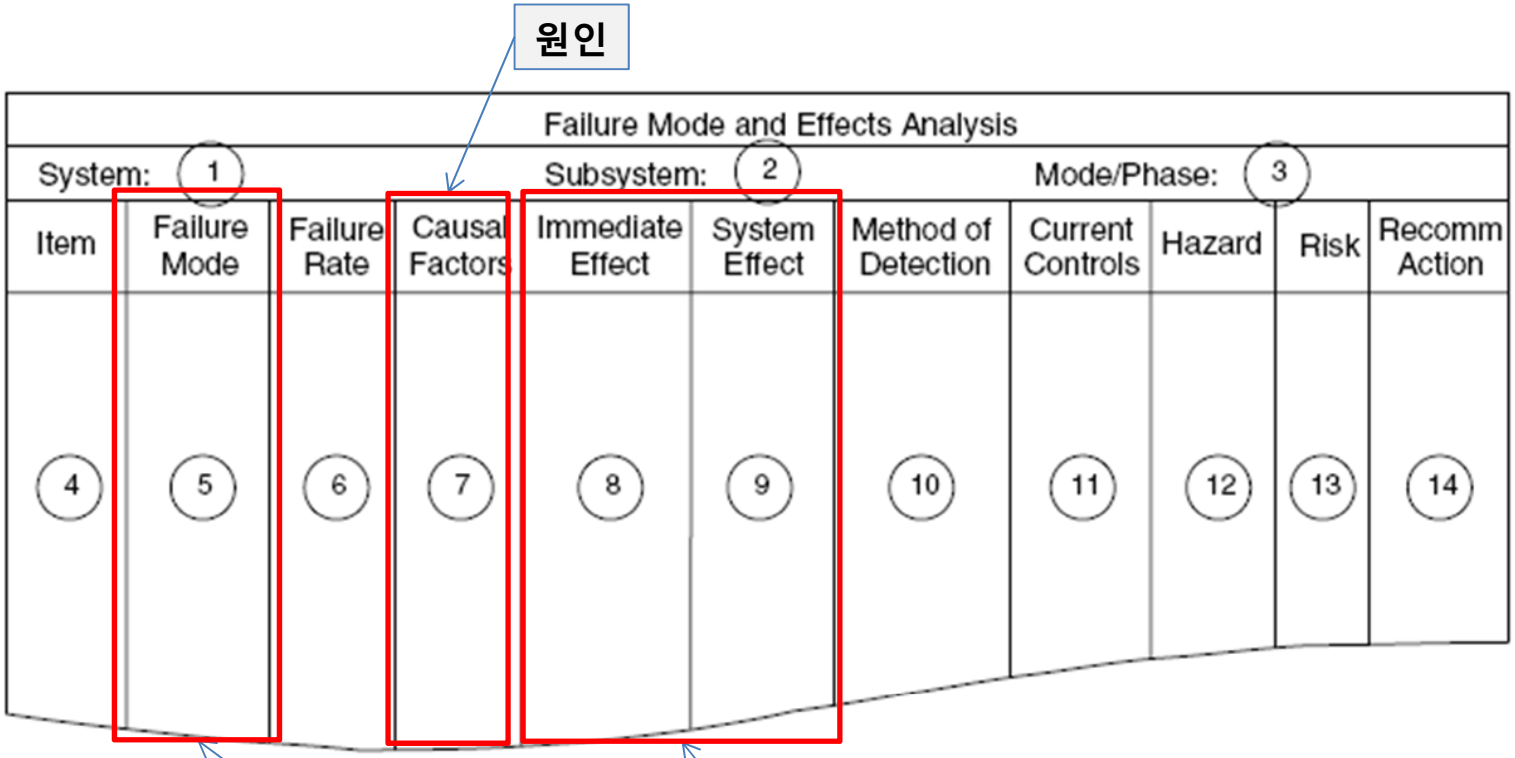


Figure 13.8 *Example FMEA worksheet 3—safety/reliability.* **Ref [3]**

HAZard and OPerability (HAZOP)

HAZOP Analysis										
No.	Item	Function/ Purpose	Parameter	Guide Word	Consequence	Cause	Hazard	Risk	Recommendation	Comments
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)

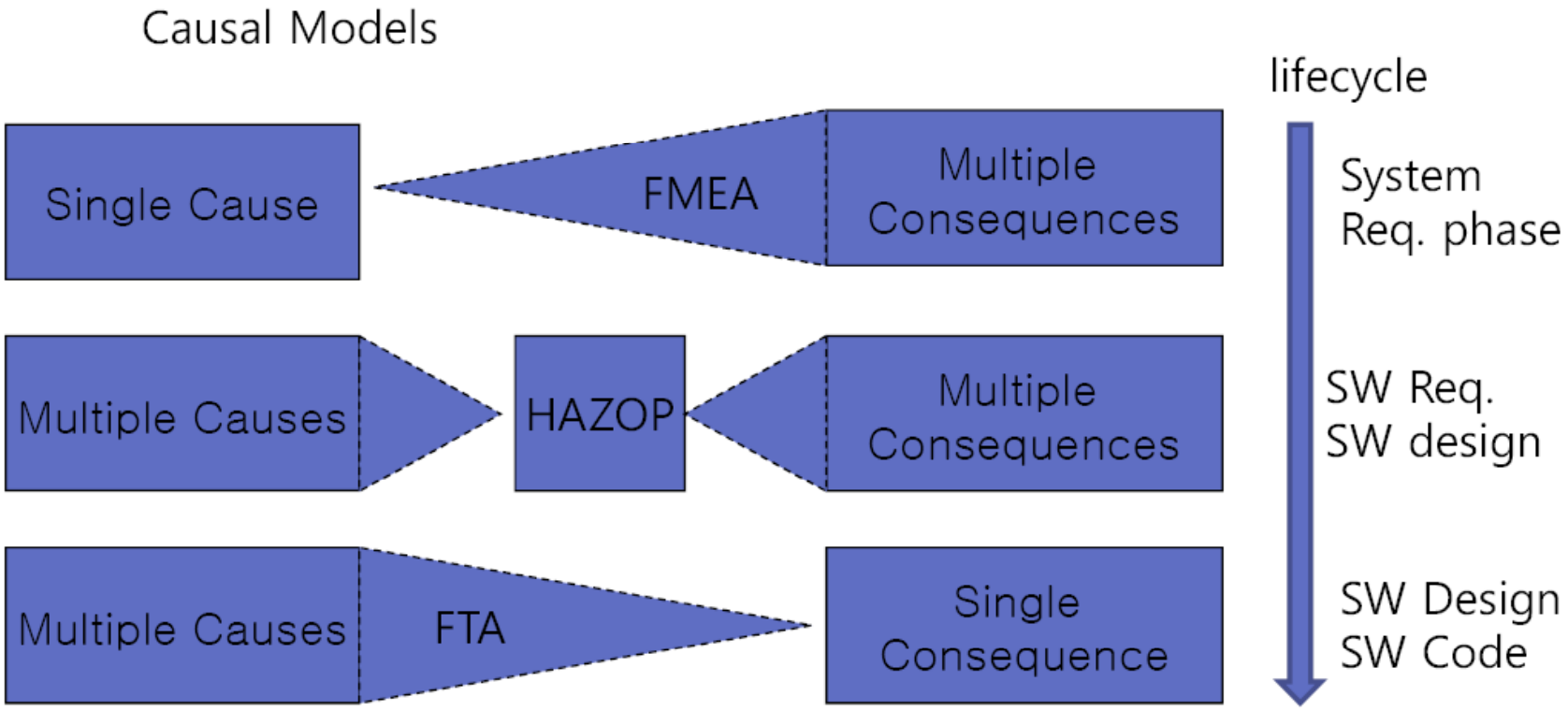
Guide Word

Figure 21.2 *Recommended HAZOP worksheet.* Ref [3]

사고의 영향

고장 위험 (Hazard)

Hazard Analysis의 적용 사례 (KNICS 사업)



Chain-of-Events 모델의 한계점

Claimed by Prof. N. Leverson, MIT

원인관계(Causality)를 너무 간단하게 생각한다.

Chain-of-Event 모델은 아래의 사항들을 다루지 않는다.

- Component interaction accidents (vs. component failure accidents)
- Indirect or non-linear interactions and complexity
- Systemic factors in accidents
- Human “errors”
- System design errors (including software errors)
- Adaptation and migration toward states of increasing risk

STAMP & STPA

STAMP (System-Theoretic Accident Model and Processes)

Systems theory에 기반하여, (not reliability theory)

사고를 dynamic control problem (vs. a failure problem) 관점에서 접근한다.

STAMP는 다음을 포함한다.

- Entire socio-technical system (not just technical part)
- Component interaction accidents
- Software and system design errors
- Human errors

Safety As A Control Problem

Safety is an emergent property that arises when system components interact with each other within a larger environment

A set of constraints related to behavior of system components (physical, human, social) enforces that property

Accidents occur when interactions violate those constraints (*i.e.,* a lack of appropriate constraints on the interactions)

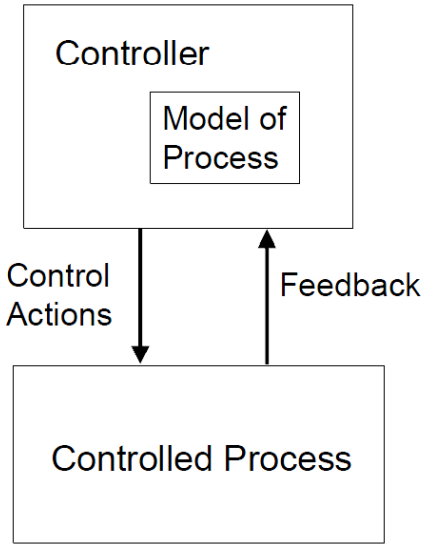
Goal is to control the behavior of the components and systems as a whole to ensure that safety constraints are enforced in the operating system.

STAMP

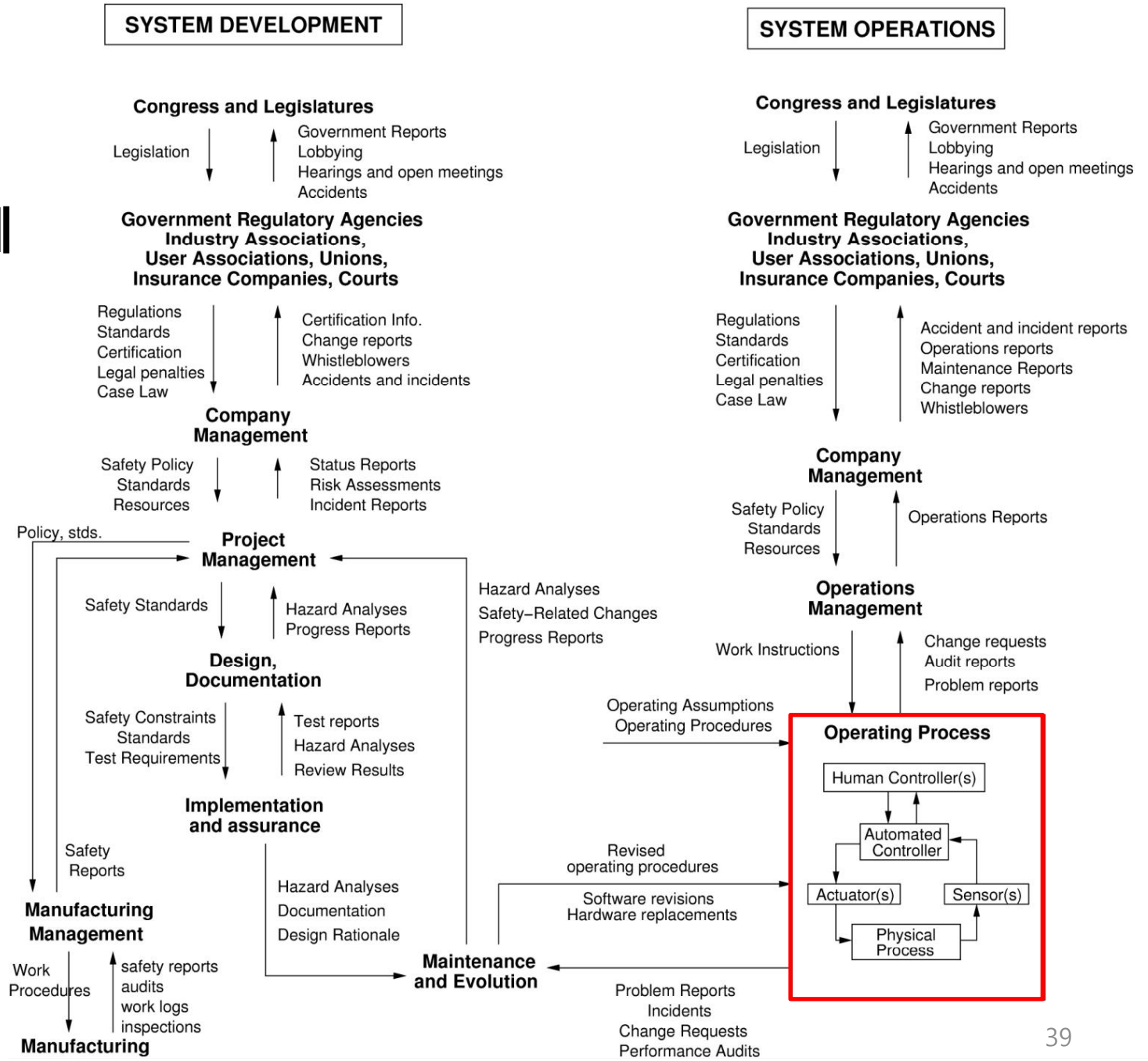
Treat safety as a dynamic control problem rather than a component failure problem

Events are the result of inadequate control

Result from lack of enforcement of safety constraints in system design and operations



Safety Control Structure의 예



Ref [4]

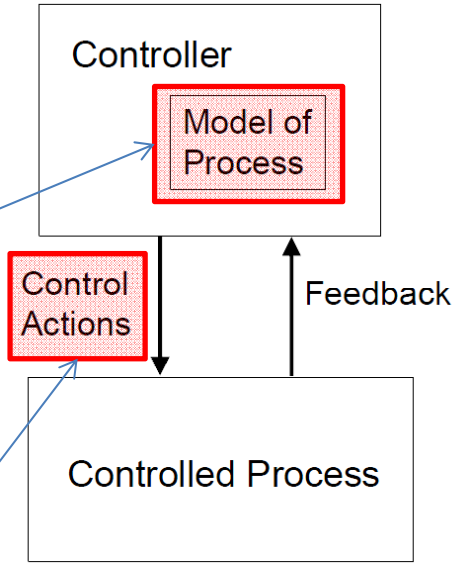
An Accident Occurs When

A. when models do not match actual processes

or / and

B. Control actions have problems such as

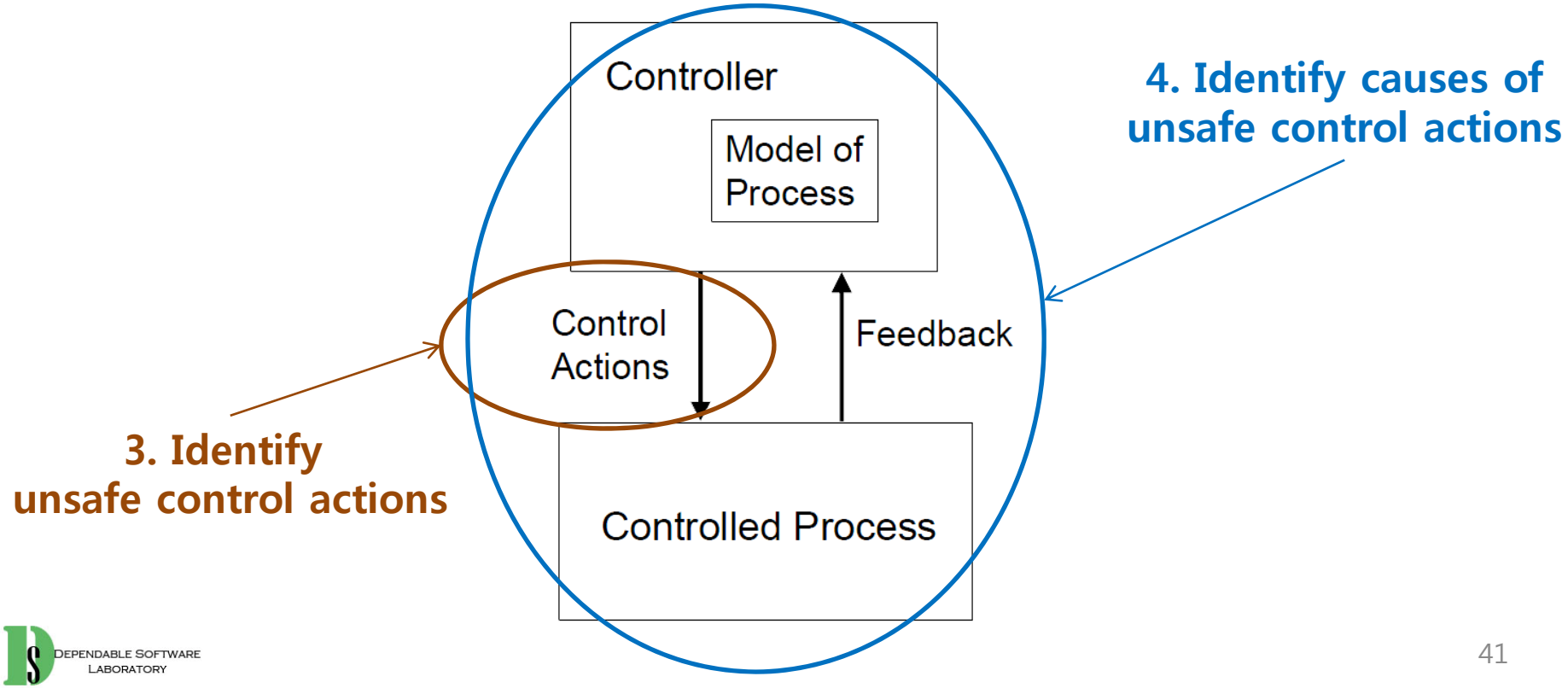
1. Required control commands are not given
2. Incorrect (unsafe) ones are given
3. Correct commands given at wrong time (too early, too late)
4. Control action stops too soon or applied too long



STPA (System Theoretic Process Analysis)

STAMP accident model에 기반한 safety analysis 기법

1. Identify a hazard
2. Construct a control structure for the hazard



Main Step 1 : Identify Unsafe Control Actions

1. A required control action is not provided or not followed

2. An incorrect or unsafe control action is provided

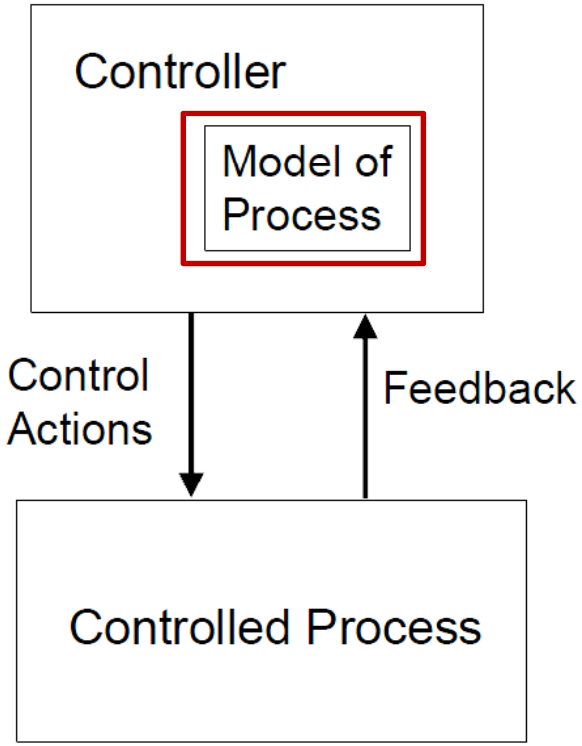
Control Action	1. Not given or not followed	2. Given incorrectly	3. Wrong timing or order	4. Stopped too soon

3. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence

4. A correct control action is stopped too soon

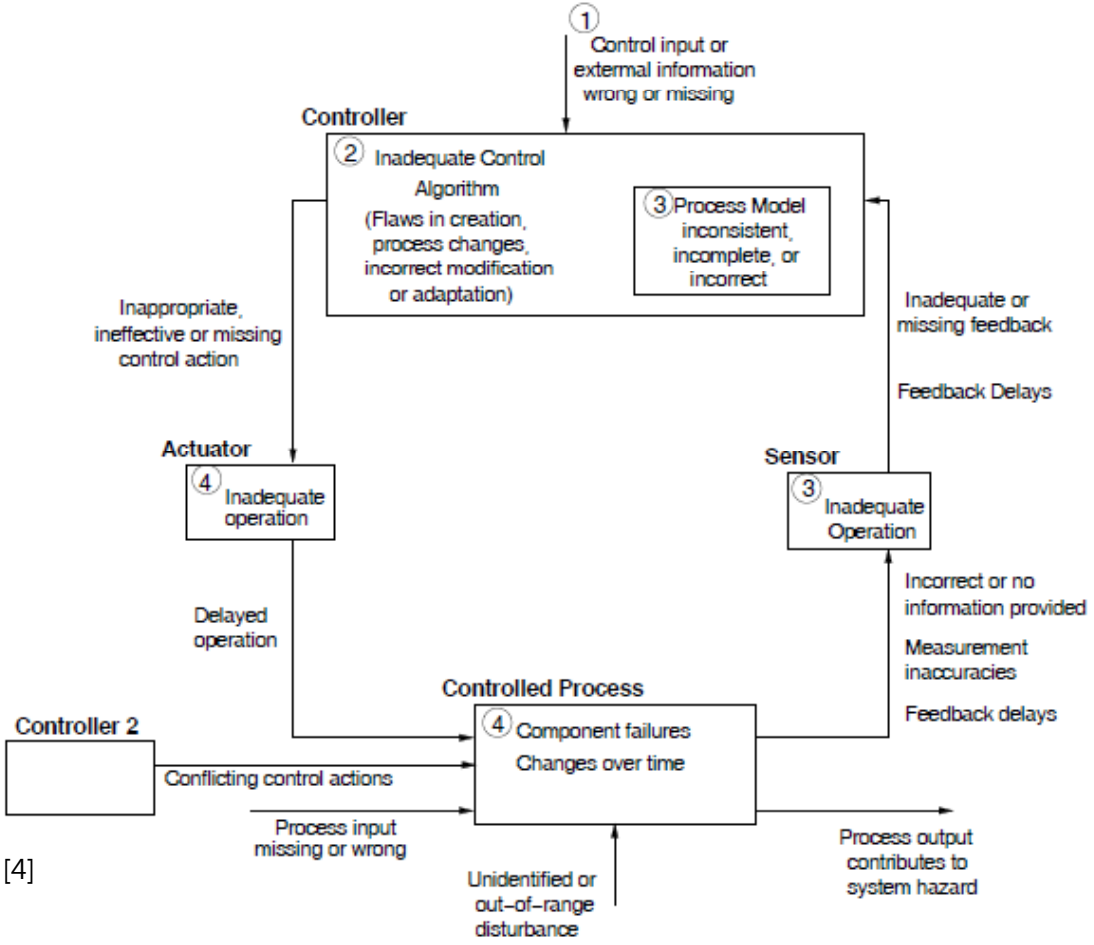
Main Step 2 : Identify Causes of Unsafe Control Actions

A. 각 Controller에 대한 Model of Process를 만든다.



Main Step 2 : Identify Causes of Unsafe Control Actions

B. 각 unsafe control action이 hazard의 원인이 될 수 있는지 잘 살펴본다.



Ref [4]

Main Step 2 : Identify Causes of Unsafe Control Actions

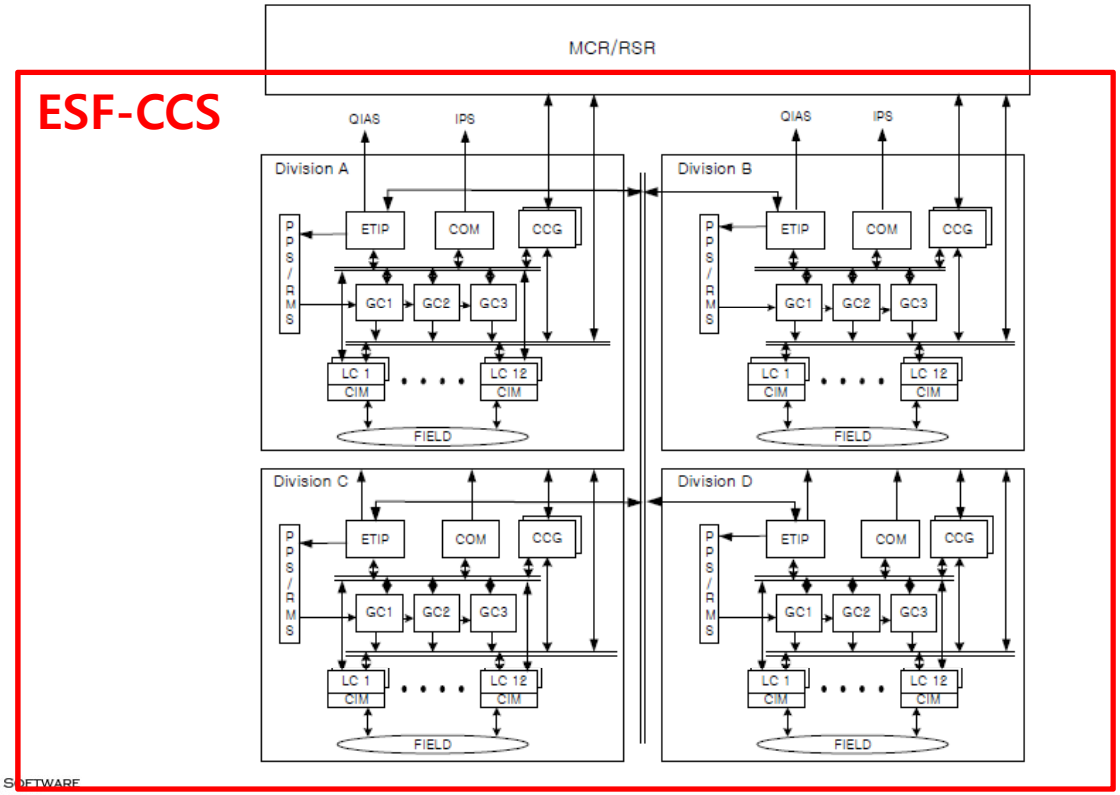
C. Consider how the designed controls could degrade over time and build in protection, including

- a. Management of change procedure
- b. Performance audit
- c. Accident and incident analysis

CASE STUDY:
KNICS APR-1400 ESF-CCS

ESF-CCS (Engineered Safety Features - Component Control System)

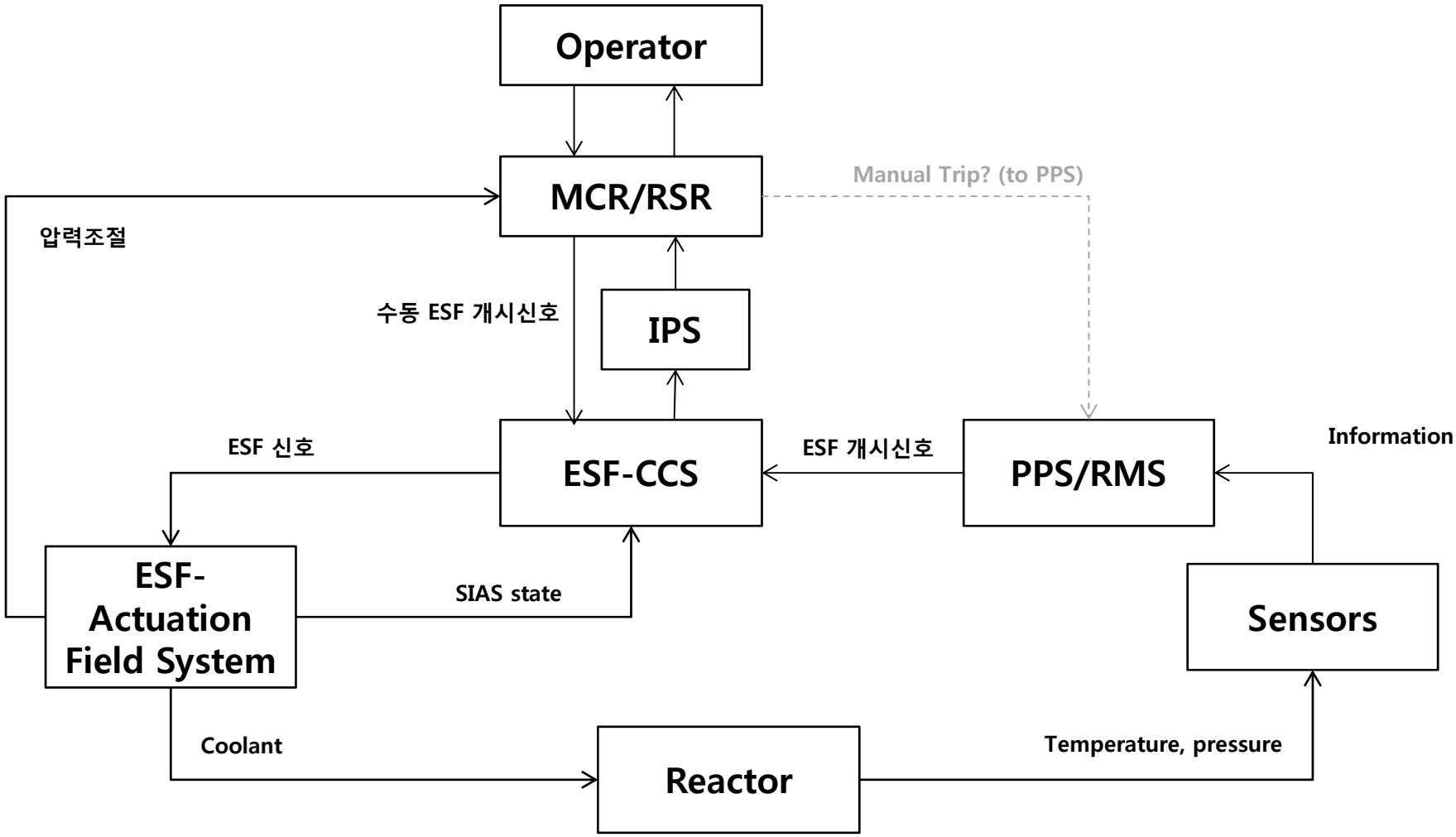
PPS와 RMS로부터 개시되는 8개의 기능으로 구성
- SIAS, CIAS, MSIS, CSAS, AFAS, CREVAS, FHEVAS, CPIAS)



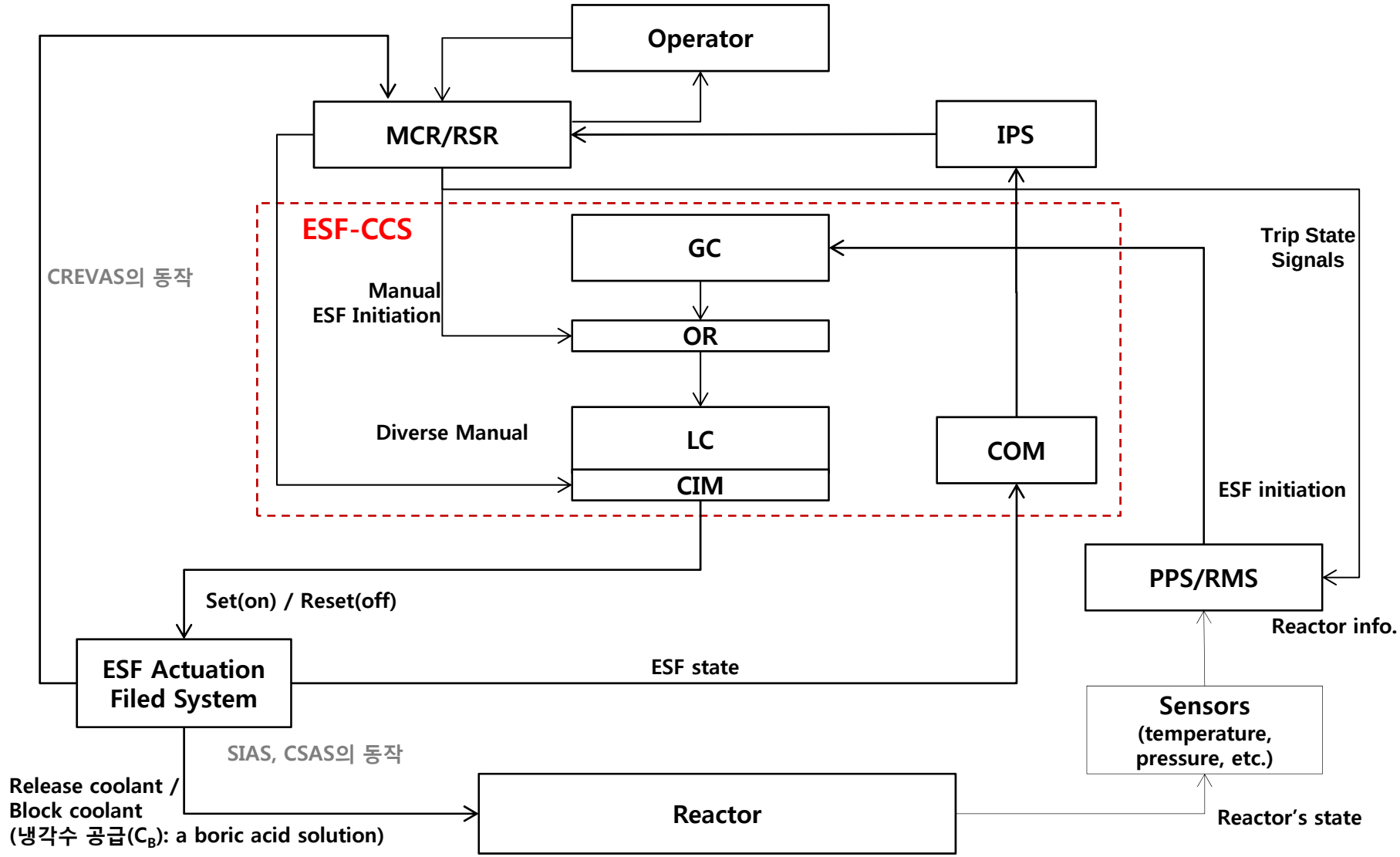
PPS : Plant Protection System
RMS : Radiation Monitoring System

Ref [1]

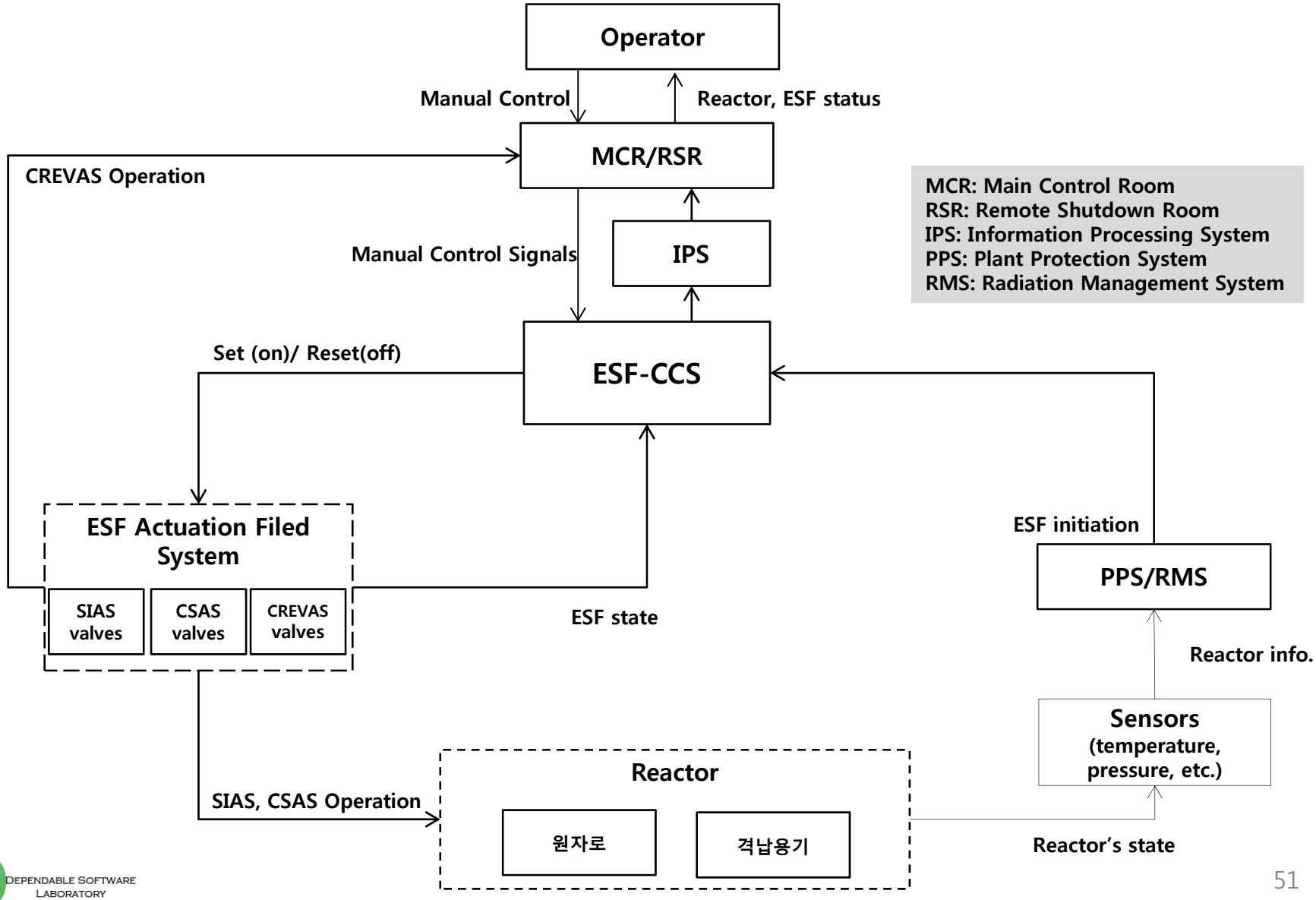
Control Structure (High-Level)



Control Structure (Low-Level)



Control Structure (Final Version)



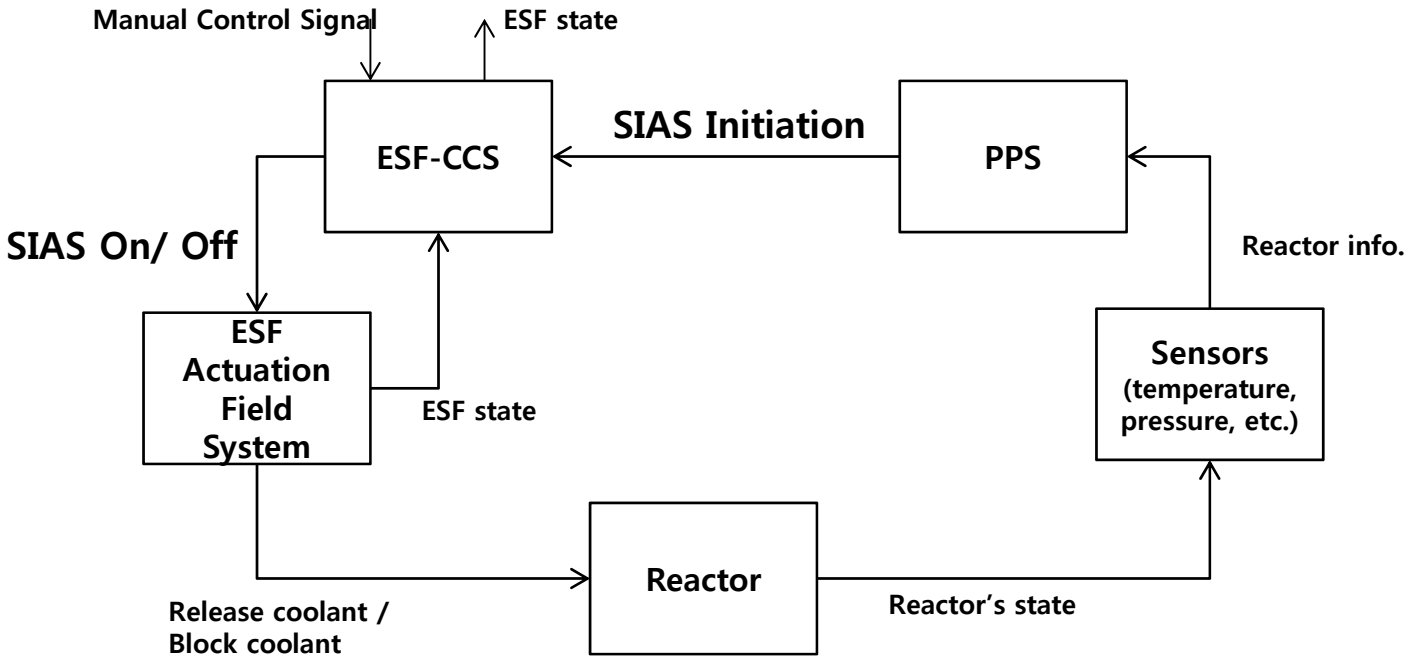
SIAS에 대한 STPA

Hazards Identification

Accident	노심 손상 사고
Safety Constraints	4 가지 사고 時, SIS가 반드시 동작해야 한다.
Hazards	SIS가 동작해야 하는 상황에서 SIS가 동작하지 않는다.
Functional Requirements	원자로냉각재상실사고(LOCA) 時, SIS 작동 이차측 열 제거원(급수) 상실(2ry Heat Sink Loss) 時, SIS 작동 증기관 또는 급수관 파열 時, SIS 작동 제어봉집합체 인출사고(Rod Ejection Accident) 時, SIS 작동

SIS : Safety Injection System

Control Structure



PPS에서 취득되는 안전주입작동 변수에 의한 안전주입작동 개시신호 발생 및 안전주입작동신호 발생

STPA Step 1: Identify Unsafe Control Actions

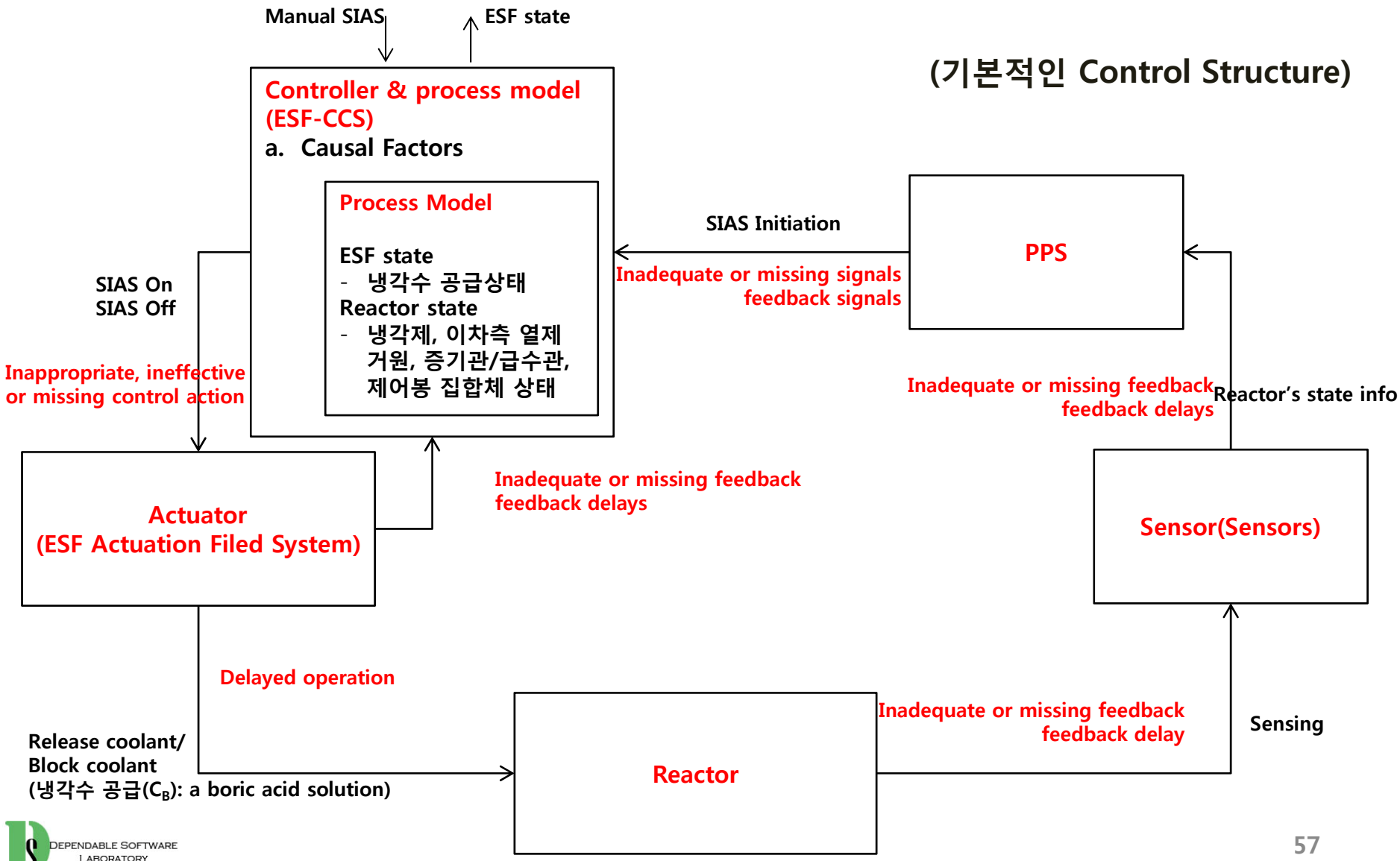
LOCA 관련

Control Action	A control action required for safety is not provided or is not followed	An unsafe control action is provided that leads to a hazard	A potentially safe control action is provided too late, too early, or out of sequence	A safe control action is stopped too soon
SIAS On (From ESF-CCS to ESF-AFS)	LOCA 시 SIAS On이 ESF로 전송되지 않음 (a1) 이차측 열제거원 상실 시 SIAS On이 ESF로 전송되지 않음 (a2) 증기관 또는 급수관 파열 시 SIAS On이 ESF로 전송되지 않음 (a3) 제어봉집합체 인출 시 SIAS On이 ESF로 전송되지 않음 (a4) Manual SIAS 발생 시 SIAS On이 ESF로 전송되지 않음 (a5)	LOCA가 발생 시 SIAS Off가 전송됨 (b1) 이차측 열제거원이 상실 시 SIAS Off가 전송됨 (b2) 증기관 또는 급수관이 파열 시 SIAS Off가 전송됨 (b3) 제어봉집합체 인출 시 SIAS Off가 전송됨 (b4) Manual SIAS 발생 시 SIAS Off가 전송됨 (b5)	LOCA 발생 전/후에 SIAS On이 전송됨 이차측 열 제거원 상실 전/후에 SI On이 전송됨 증기관 또는 급수관 파열 전/후에 SIAS On이 전송됨 제어봉집합체 인출사고 전/후에 SIAS On이 전송 됨 Manual SIAS 발생 전/후에 SIAS On이 전송됨	냉각수가 충분히 공급되지 않았는데 SIAS On이 멈춤
SIAS Off (From ESF-CCS to ESF-AFS)	-	LOCA발생 하지 않았을 때SIAS On가 전송됨 이차측 열제거원이 상실되지 않았을 때 SIAS On가 전송됨 증기관 또는 급수관이 파열 되지 않았을 때 SIAS On가 전송됨 제어봉집합체가 인출되지 않았을 때 SIAS On가 전송됨 Manual SIAS 발생되지 않았는데, SIAS On이 전송 됨	Reactor의 온도가 충분히 내려가지 않은 상황에서 SIAS Off가 전송 됨	-

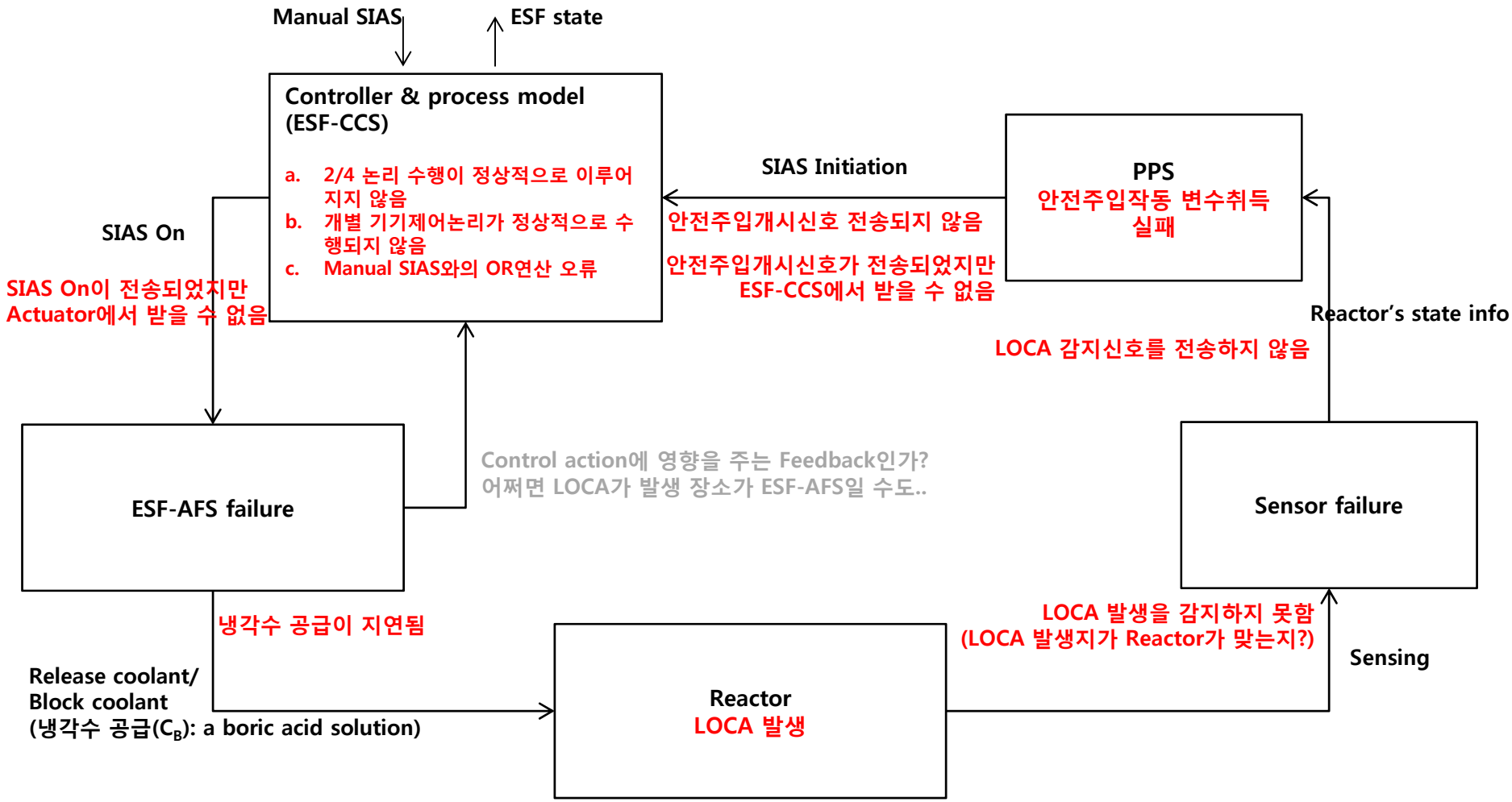
Safety Constraints, Created

Unsafe Control Action	Safety Constraints
냉각재 상실 시 SIAS On이 ESF로 전송되지 않아 노심이 손상됨	냉각재 상실 시에는 반드시 SIAS On이 전송되어야 함
이차측 열제거원 상실 시 SIAS On이 ESF로 전송되지 않음	이차측 열제거원 상실 시에는 반드시 SIAS On이 전송되어야 함
증기관 또는 급수관 파열 시 SIAS On이 ESF로 전송되지 않음	증기관 또는 급수관 파열 시에는 반드시 SIAS On이 전송되어야 함
제어봉집합체 인출 시 SIAS On이 ESF로 전송되지 않음	제어봉집합체 인출 시에는 반드시 SIAS On이 전송되어야 함
Manual SIAS 발생 시 SIAS On이 ESF로 전송되지 않음	Manual SIAS 발생 시 SIAS On이 반드시 ESF로 전송되어야 함
LOCA발생 시 SIAS Off 신호가 전송됨	LOCA시 SIAS Off가 전송되면 안됨
이차측 열제거원 상실 시 SIAS Off가 전송됨	이차측 열제거원 상실 시 SIAS Off가 전송되면 안됨
증기관 또는 급수관 파열 시 SIAS Off가 전송됨	증기관 또는 급수관 파열 시 SIAS Off가 전송되면 안됨
제어봉집합체 인출 시 SIAS Off가 전송됨	제어봉집합체 인출 시 SIAS Off가 전송되면 안됨
Manual SIAS 발생 시 SIAS Off가 전송됨	Manual SIAS 발생 시 SIAS Off가 전송되면 안됨
LOCA 발생 전/후에 SI On이 됨	LOCA 발생 즉시 SI On이 되어야 함
이차측 열 제거원 상실 시 발생 전/후에 SI On이 전송됨	이차측 열제거원 발생 즉시 SI On이 되어야 함
증기관 또는 급수관 파열 시 발생 전/후에 SIAS On이 전송됨	증기관 또는 급수관 파열 발생 즉시 SI On이 되어야 함
제어봉집합체 인출 시 발생 전/후에 SIAS On이 전송 됨	제어봉집합체 인출 발생 즉시 SI On이 되어야 함
Manual SIAS 발생 전/후에 SIAS On이 전송됨	Manual SIAS 발생 즉시 SIAS On이 전송되어야 함
냉각재가 충분히 제공되지 않은 시점에서 SIAS Off가 전송됨	냉각재가 충분히 제공될 때까지 SIAS Off가 전송되어서는 안됨

STPA Step 2: Identify Causal Factors



(a1) LOCA 시 SIAS On이 ESF로 전송되지 않음



a2 ~ a4 도 유사한 분석을 수행

Causal Factors (a1-a4)

LOCA 시 SIAS On이 ESF로 전송되지 않음 (a1-a4) (이차측열제거원 상실, 증기관 또는 급수관 파열, 제어봉집합체 인출)	발생위치, 신호명칭	Causal Factors
	Manual SIAS (To ESF-CCS)	들어온다고 해서 위험 상황이 발생하지 않음
	ESF-CCS	2/4논리 수행이 정상적으로 이루어지지 않음
		개별 기기제어논리가 정상적으로 수행되지 않음
		Manual SIAS와의 OR연산 오류
	SIAS On(ESF-CCS to ESF-AFS)	SIAS On 신호가 전송되지 않음
	ESF-AFS	ESF-AFS (Valves open) 가 정상 동작하지 않음
	Release Coolant (ESF-AFS to Reactor)	냉각수 공급이 지연됨
	Reactor	-
	Sensing (Reactor to Sensor)	LOCA가 발생했지만 전송되지 않음
	Sensor	LOCA 발생을 감지하지 못함
	Reactor's state (Sensor to PPS)	LOCA 감지신호를 전송하지 않음
		LOCA 감지신호 전송이 지연됨
	PPS	안전주입작동 변수취득을 하지 못함
	SIAS Initiation (PPS to ESF-CCS)	안전주입개시신호가 전송되지 않음
		안전주입개시신호가 전송되었지만 ESF-CCS에서 받을 수 없음

맺음말

Hazard Analysis	위험요소(Hazard)에 대한 다양한 분석
Safety Analysis	안전성에 대한 다양한 분석
	Safety Analysis ⊃ Hazard Analysis
	안전성 분석 전문가의 경험과 능력에 전적으로 의존한다.
	안전성 분석 대상(Target)을 잘 알아야 한다.
Accident Model	Chain-of-Event vs. STAMP
	Accident Model에 따라 다른 분석 기법을 사용한다.
	FTA, FMEA, HAZOP 등 다수 vs. STPA

참고문헌

[1] 한국형 표준 원전 계통 실무(교육자료), 한국원자력연구원 원자력교육센터 (KNTC), http://www.kntc.re.kr/openlec/nuc/Atomicpile/Index.htm

[2] SAFEWARE: System Safety and Computers, Nancy G. Leveson

[3] Hazard Analysis Techniques for System Safety, Clifton A. Ericson

[4] Engineering a Safer World: Systems Thinking Applied to Safety, Nancy G. Leveson

KU KONKUK UNIVERSITY

감사합니다!!!

http://dslab.konkuk.ac.kr