한국원자력연구원
Korea Atomic Energy Research Institute

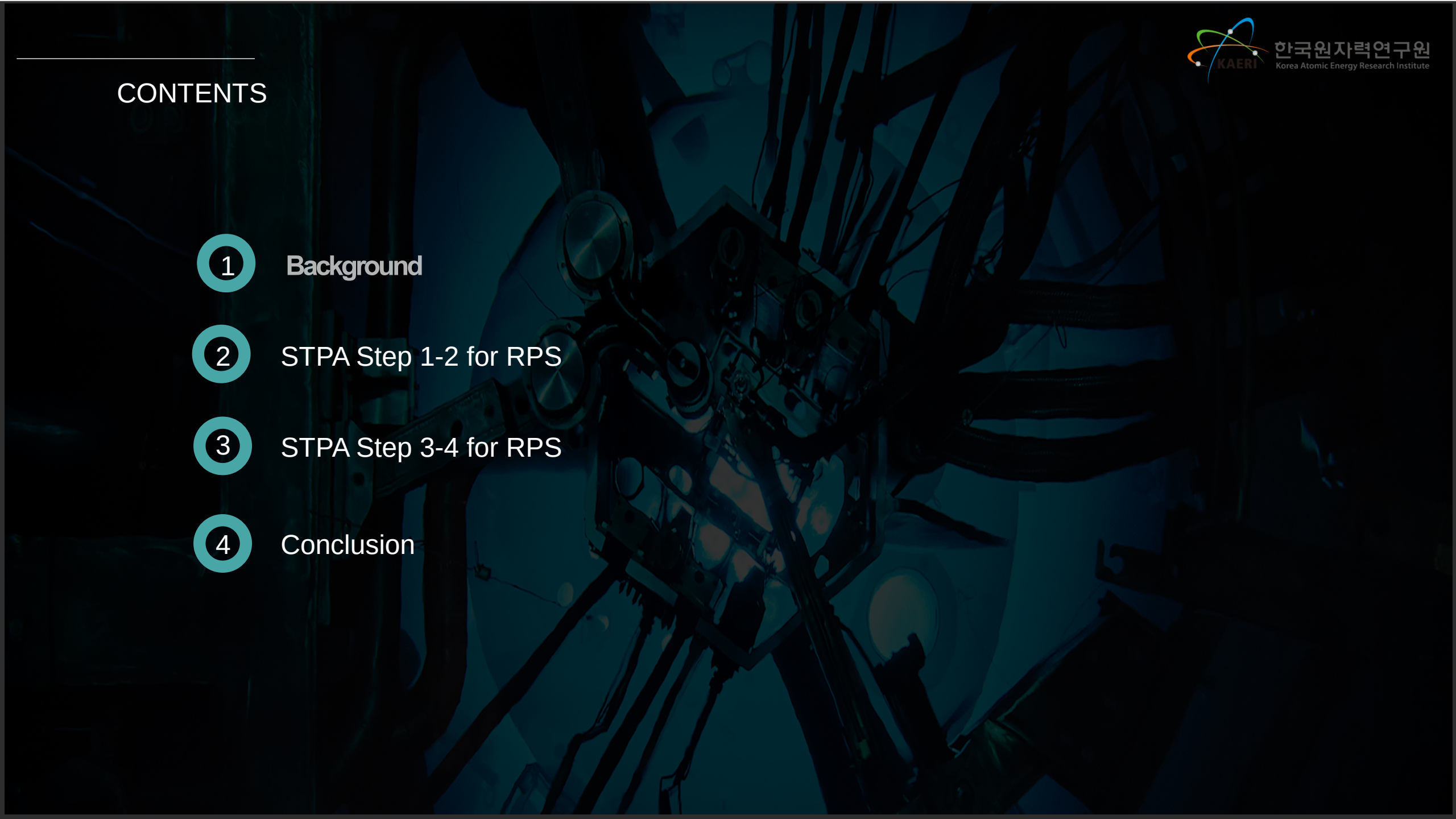
A preliminary study on application of STPA to Reactor Protection System for Defense-in-Depth and Diversity

D3 관점에서의 RPS의 STPA 적용 연구

은형석[1,2*], 허윤아[3], 유준범[3], 지은경[2], 백종문[2], 신성민[4], 이준구[1]

1: 한국원자력연구원 경수형SMR원자로기술개발부
2: 한국과학기술원 전산학부 3: 건국대학교 컴퓨터공학부
4. 한국원자력연구원 리스크평가부

*hseun@kaeri.re.kr



한국원자력연구원
Korea Atomic Energy Research Institute

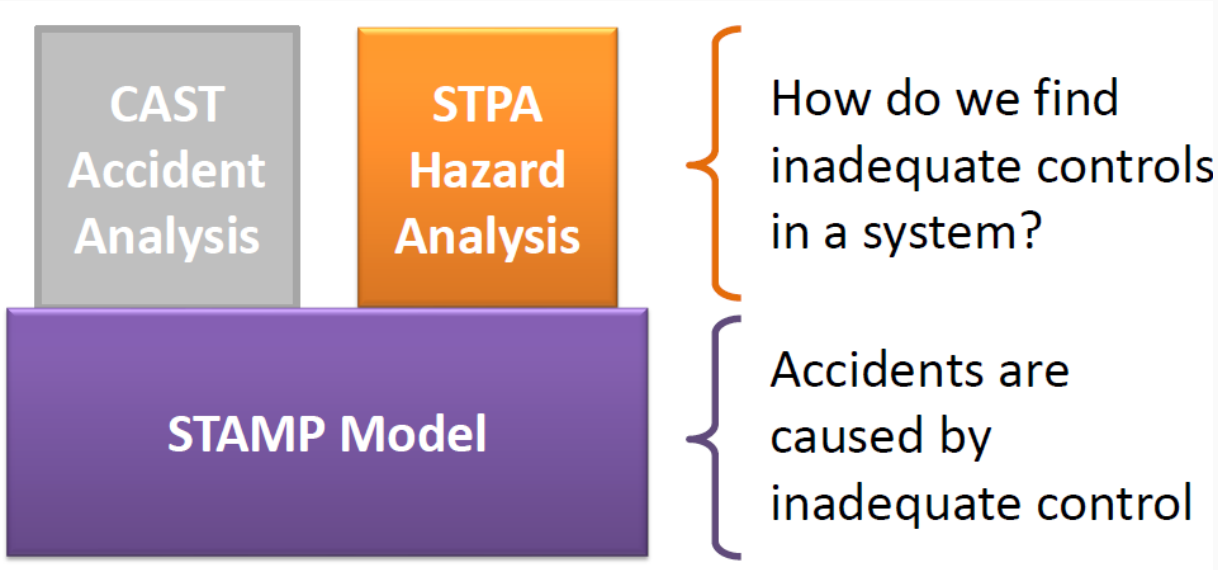
CONTENTS

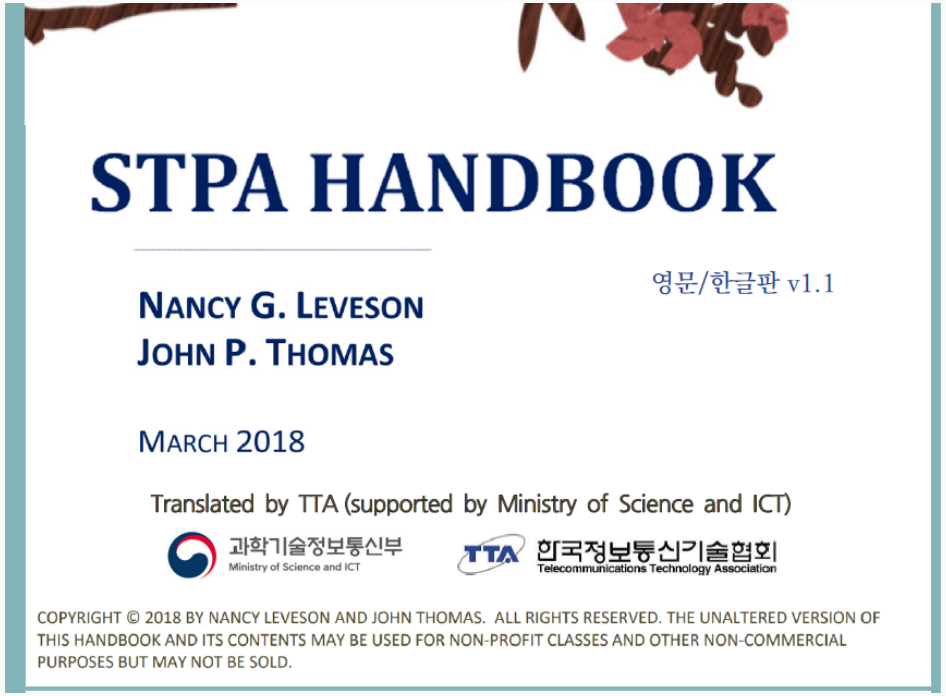
Part 1.

Background

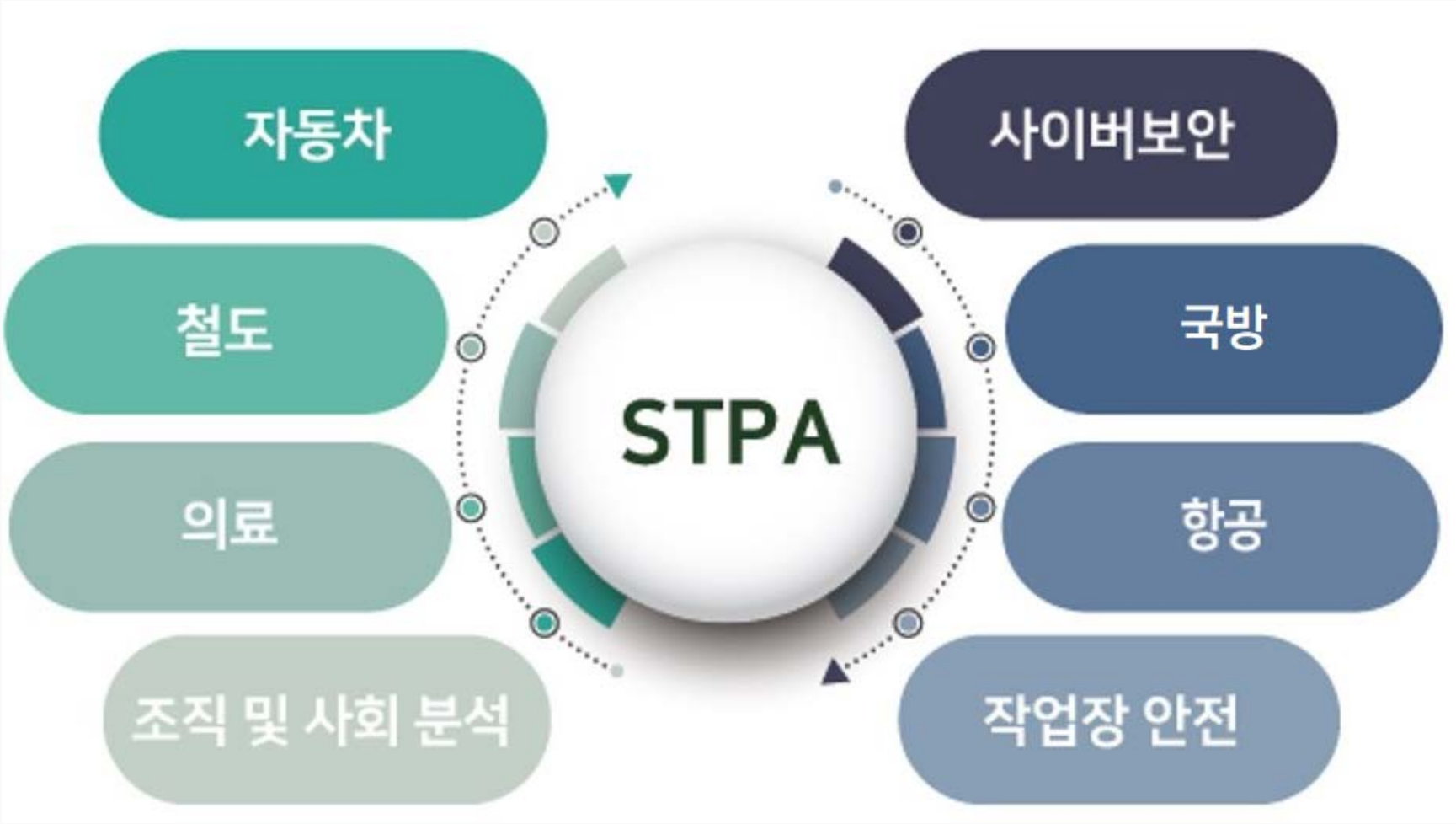
1 STPA (System-Theoretic Process Analysis)

- STAMP (System-Theoretic Accident Model and Processes) 모델을 기반으로 하는 위험분석 (Hazard analysis) 기법
  - Nancy Leveson (MIT) (2012) → N. Leveson and J. Thomas (2018) "STPA Handbook"
  - 과기부 와 TTA(한국정보통신기술협회) 에서는 STPA 핸드북 발간 (2019.12)
- 위험을 유발할 수 있는 "부적절한 제어"로 사고가 발생한다는 관점 (Not Only "Failure")





1 STPA (System-Theoretic Process Analysis)



1 STPA (System-Theoretic Process Analysis)

Warsaw Crash

- Software algorithm to ensure aircraft has landed:
  - Must be 6.3 tons on each main landing gear strut
  - Wheel must be turning at least 72 knots
- Off-nominal landing conditions at Warsaw
  - Crosswind landing (one side first)
  - Wet runway: wheels hydroplane

Lufthansa 2904, Airbus A320

SW operated exactly as designed, no failure!

A New Approach to Software Safety Using STPA

John Thomas
(MIT 항공우주공학과 디렉터)

그 결과 비행기가 충돌했습니다. 무엇이 실패했습니까? 모든 부품이 우리가 설계한 대로 정확하게 작동했습니다.

* FMEA : Failure Modes & Effects Analysis
FTA : Fault Tree Analysis

1 STPA (System-Theoretic Process Analysis)

◦ 전통적인 분석 방법론인 FMEA, FTA는 시스템 고장 모드를 평가하는데 사용되었으나, 이러한 방법은 현대 디지털 제어시스템에 적용시 한계를 보이고 있음

◦ The NRC participants recognized that **STPA is a good complement** to existing regulatory activities …

: NRC 참여자들은 **STPA가 기존 규제 활동을 잘 보완한다는 것을 인지**했습니다. STPA는 현재 NRC 규제 검토 및 감독 프로세스에서 제대로 표현되지 않은 부분을 체계적으로 분석합니다.

- 안전 시스템의 유지 관리 및 운영과 관련된 위험
- 복잡한 소프트웨어 상호 작용 및 새로운 위험 식별

1 STPA (System-Theoretic Process Analysis)

◦ NuScale은 계측시스템에 STPA를 적용하였고, 이를 NRC가 인정하여 인허가 승인하였음.

Systems-Theoretic Process Analysis

The STPA is a process analysis method based on STAMP. In this method, control structures within the system under analysis are identified and diagrammatic representations (models) of those control structures are constructed. The structures defined in this way may or may not reflect the physical structures of the system, but represent the functional controllers, actuators, controlled processes,

◦ NuScale의 STPA

◦ 현 NuScale의 STPA 담당자는, 6년간 STPA를 경험한 숙련자로 계측제어에 30년 경험자

1 STPA (System-Theoretic Process Analysis)

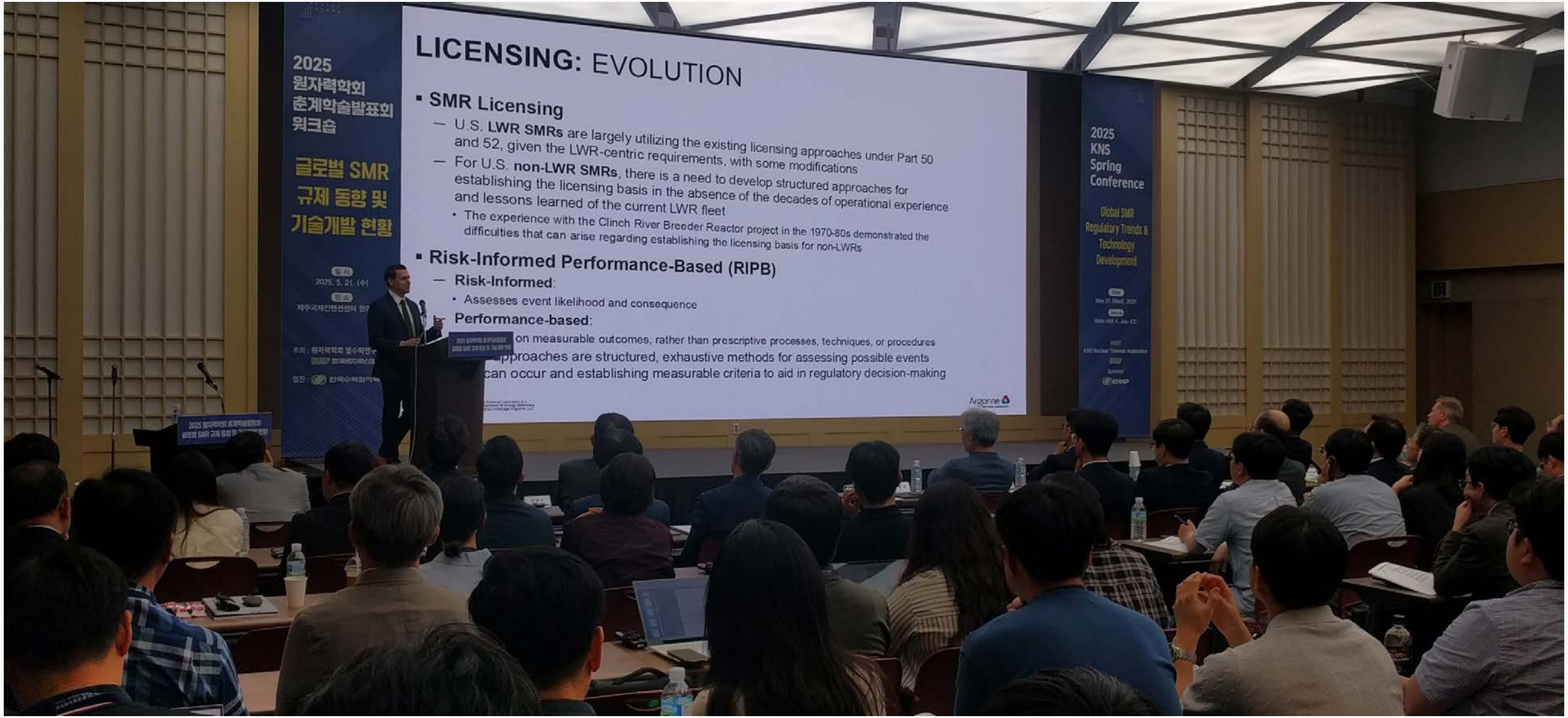
◦ Branch Technical Position (BTP) 7-19. Rev.9

◦ The reviewer should consider whether the D3 assessment is adequate to identify and defend against CCF vulnerabilities.. .. risk of CCF vulnerabilities using a risk-informed approach and applied design techniques, prevention measures, or mitigation measures commensurate with the risk significance of the postulated CCF

: 검토자는 D3 평가가 CCF 취약성을 식별하고 방어하기에 적절한지 고려해야 합니다..

신청자는 위험 정보 접근 방식 (Risk-informed approach) 을 사용하여 CCF 취약성의 위험을 평가하고 가정된 CCF의 위험 중요성에 상응하는 설계 기술, 예방 조치 또는 완화 조치를 적용합니다.

1 STPA (System-Theoretic Process Analysis)



1 STPA (System-Theoretic Process Analysis)

◦ STPA :

1단계: Loss 및 Hazard 정의

- 손실(Loss) 정의
- 위험(Hazard) 정의

2단계: Control Structure 도식화

- 제어 관계에 따른 개체(컴포넌트) 식별
- 제어명령, 피드백, 프로세스 모델 등 도식화

3단계: Unsafe Control Action 도출

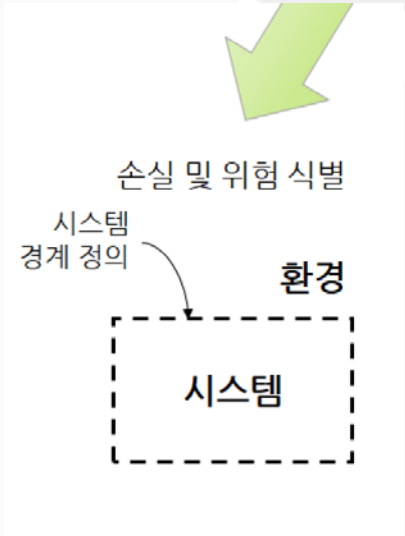
- 4가지 유형*에 따른 Unsafe Control Action 도출

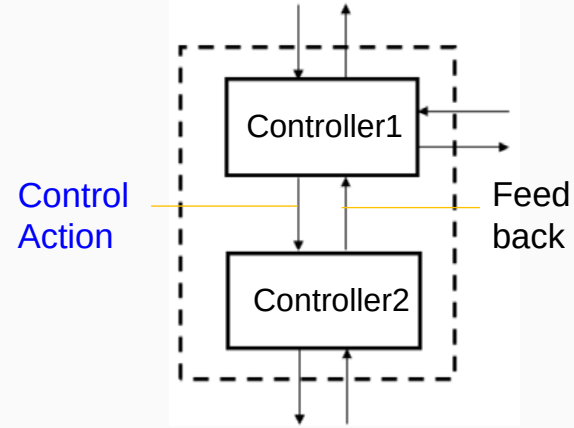
* 4가지 유형

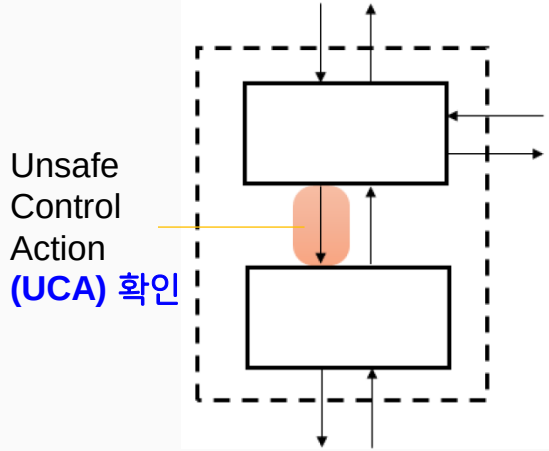
① CA is not provided
② UCA is provided
③ CA is too early, too late, out of sequence
④ CA is stopped too soon, applied too long

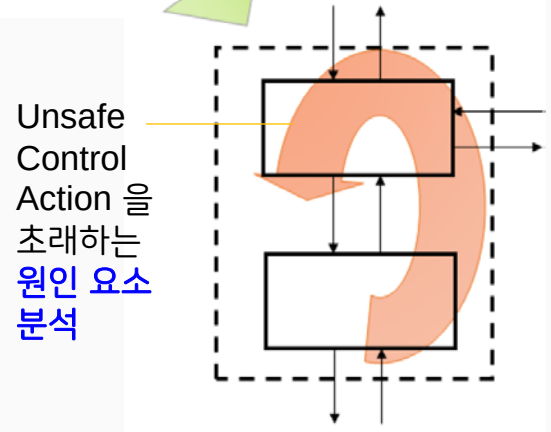
4단계: 원인 시나리오 도출

- Unsafe Control Action 발생 원인 도출
- Loss Scenario (손실 시나리오 도출)









1 STPA (System-Theoretic Process Analysis)

컨트롤 액션	제공하지 않음이 위험을 유발함	제공함이 위험을 유발함	너무 일찍, 너무 늦게, 잘못된 순서	너무 빨리 중지됨, 너무 오래 적용됨
브레이크	UCA-1: BSCU 오토브레이크가 BSCU 작동개시 중일 때 착륙활주 동안 브레이크 컨트롤 액션을 제공하지 않는다. [H-4.1]	UCA-2: BSCU 오토브레이크가 정상적인 이륙 중 브레이크 컨트롤 액션을 제공한다. [H-4.3, H-4.6] UCA-5: BSCU 오토브레이크가 착륙활주 동안 제동 수준이 불충분한 브레이크 컨트롤 액션을 제공한다. [H-4.1] UCA-6: BSCU 오토브레이크가 착륙활주 동안 방향성 있거나 비대칭적인 브레이크 컨트롤 액션을 제공한다. [H-4.1, H-4.2]	UCA-3: BSCU 오토브레이크가 터치다운 후 너무 늦게(>TBD초) 브레이크 컨트롤 액션을 제공한다. [H-4.1]	UCA-4: BSCU 오토브레이크가 항공기 착륙 시 너무 일찍 (지상활주 속도가 TBD에 도달하기 전에) 브레이크 컨트롤 액션 제공을 중지한다. [H-4.1]

Part 2.

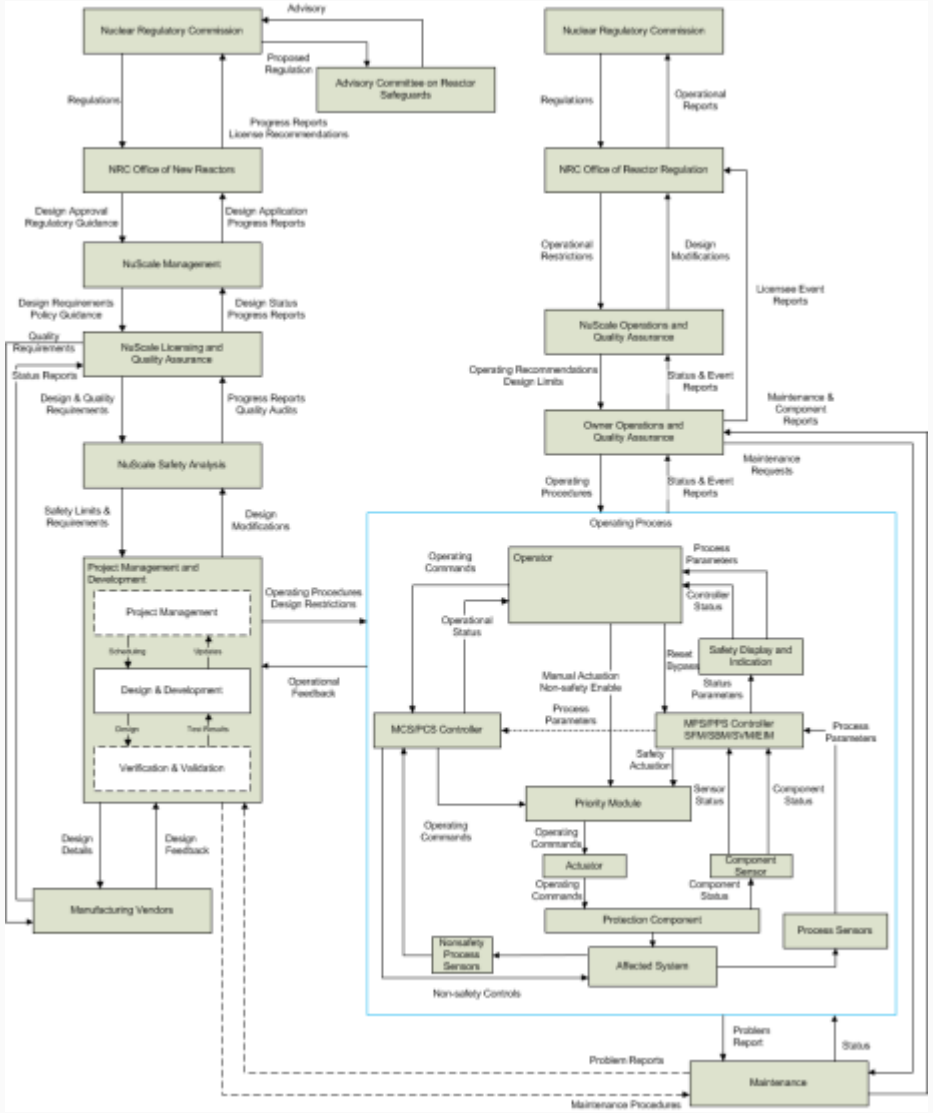
STPA STEP 1~2 :
Loss / Hazard / Control structure

2 STEP1 : Define Purpose of the Analysis

ID	Loss name
L-1	Loss of life; injury to people
L-2	Damage to environment (e.g. contamination, release)
L-3	Loss of power generation
L-4	Financial losses (e.g. repair)
L-5	Loss of reputation, goodwill, trust, investor confidence

ID	Hazard name		Links
H-1	Digital CCF occurrence	Digital Fault에 의한 CCF	L-1,2,3
H-2	Human Error	인지오류	L-1,2,3
H-3	False positive indication or alarm	정상을 표시못하는 경우	L-3
H-4	False negative indication or alarm	비정상을 표시못하는 경우	L-1,2
H-5	Unexpected reactor trip	예상하지 않은 CEA 전체 낙하	L-3,4,5
H-6	Failure of reactor trip	원자로 정지를 위한 Scram 실패	L-1,2,5
H-7	Time delay in signal processing	신호처리의 시간지연	L-3
H-8	Abnormal fluctuation in input signal	입력신호의 비정상적인 유동	L-3
H-9	Maintenance Error	유지보수 오류	L-1,2,3,4
H-10	Regulatory licensing basis violation	안전규제위반	L-1,2,3,4,5

2 STEP 2: Control Structure for NuScale SMR

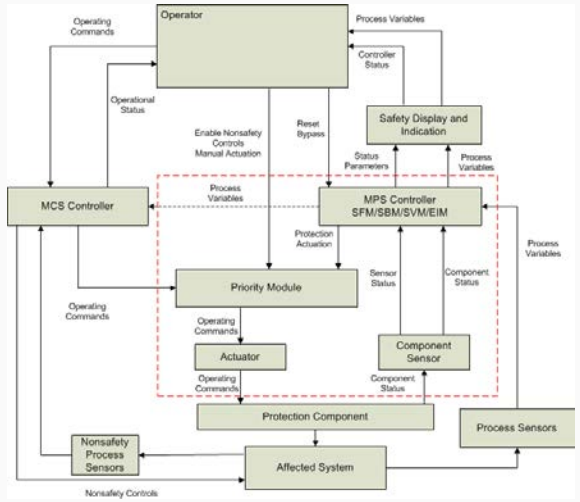


Handbook: 시스템 뿐만 아니라 관련 Activity 또한 Control Structure에 표시되어야함.

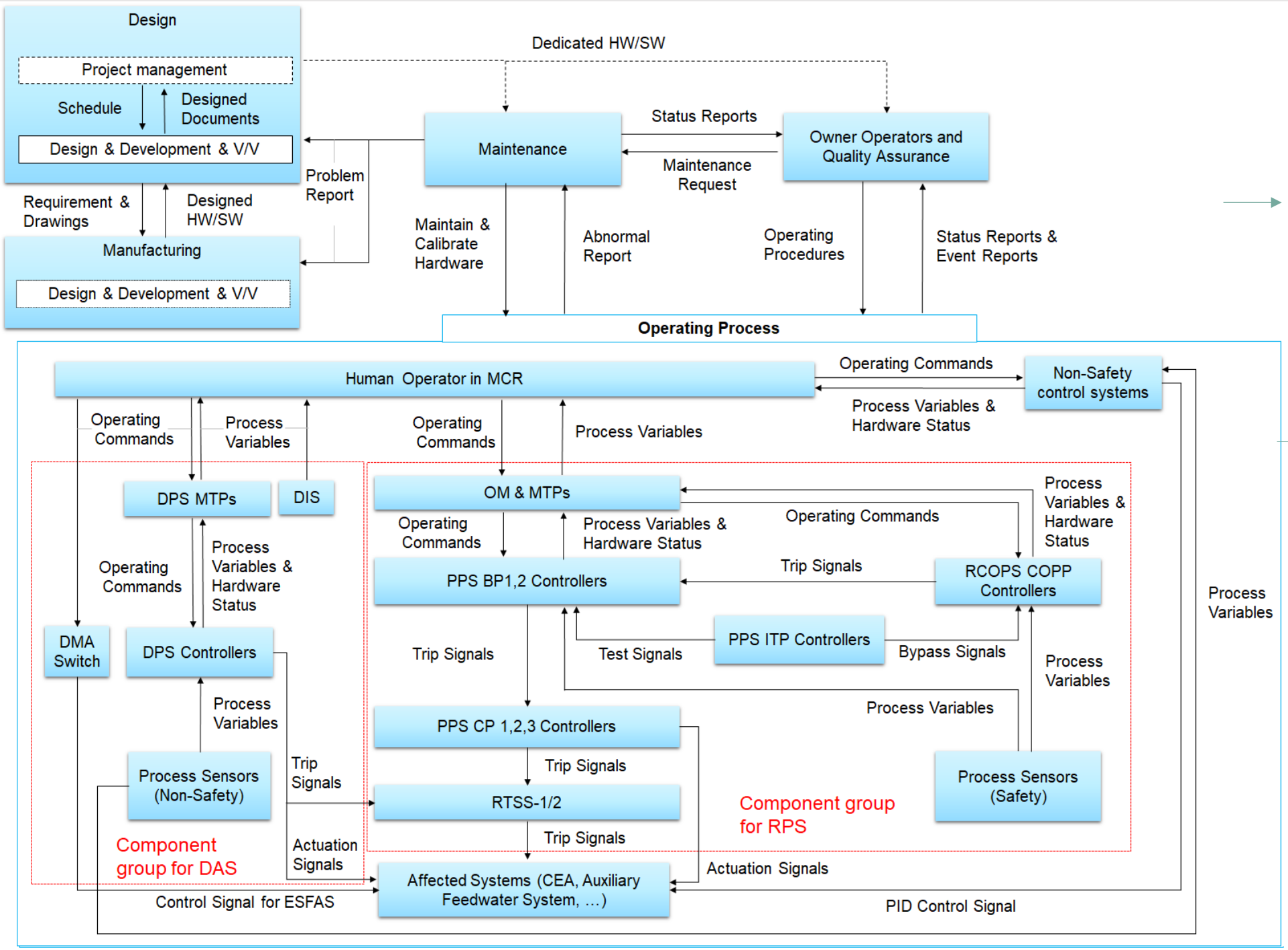
NuScale은 전체 Activity 에 대한 Control Structure를 잡은 뒤 이를 세분화 하였음. (해당 Diagram은 FSER에서 공개하지 않았으나 발표자료에 낮은 해상도 그림으로 존재함)

→ 이를 확인하여, APR1400 I&C 측면에서 필요한 Scope에 맞는 전체 프로세스에 대한 Control Structure 를 그린 뒤 상세화함

NuScale 발표자료



FSER의 Figure로 공개

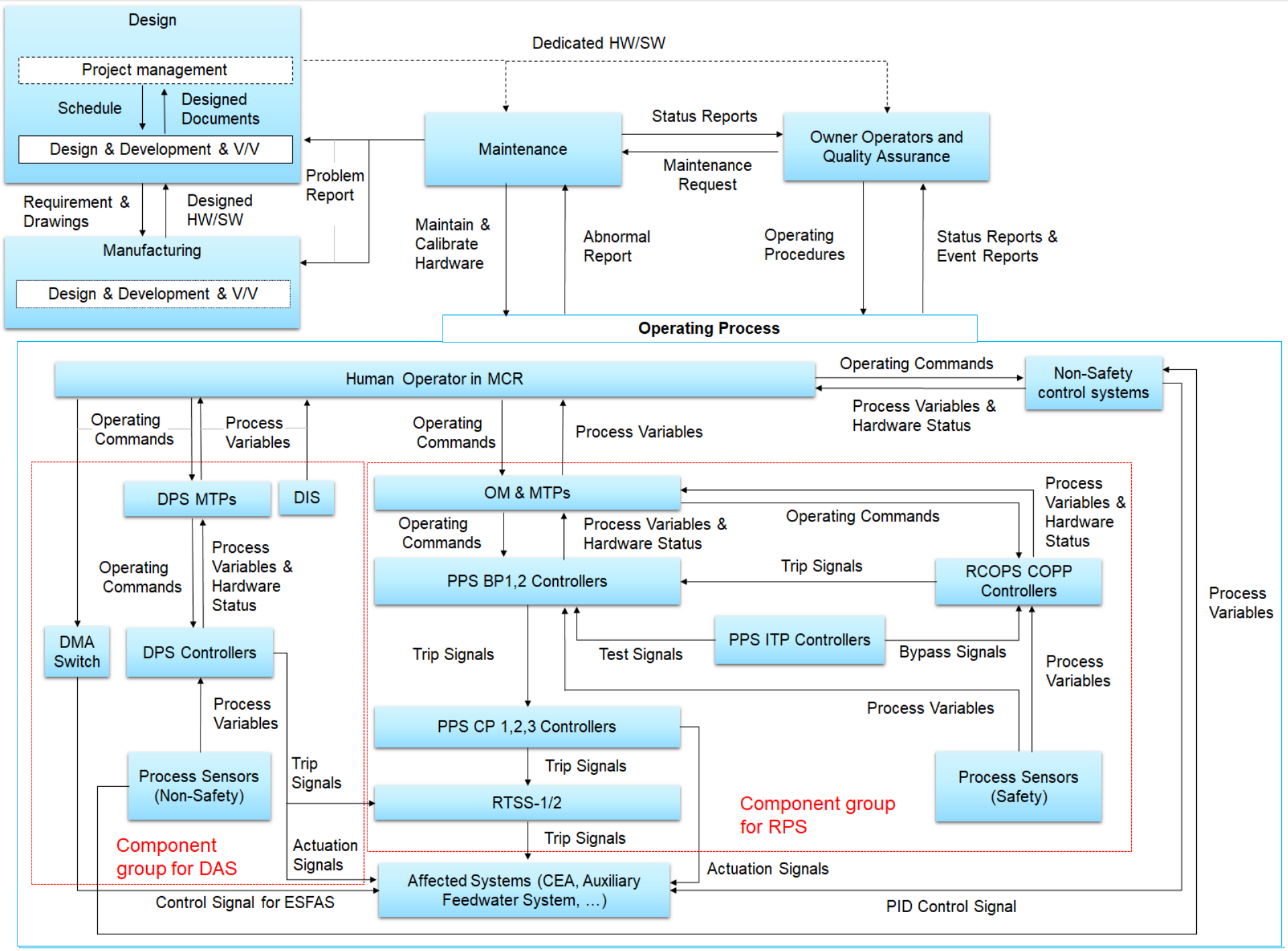


Project Activity:

설계, 운영, 유지보수 프로세스
(기관과 조직간의 상호작용)

Operating Process:

시스템 작동
(시스템 간의 상호작용)

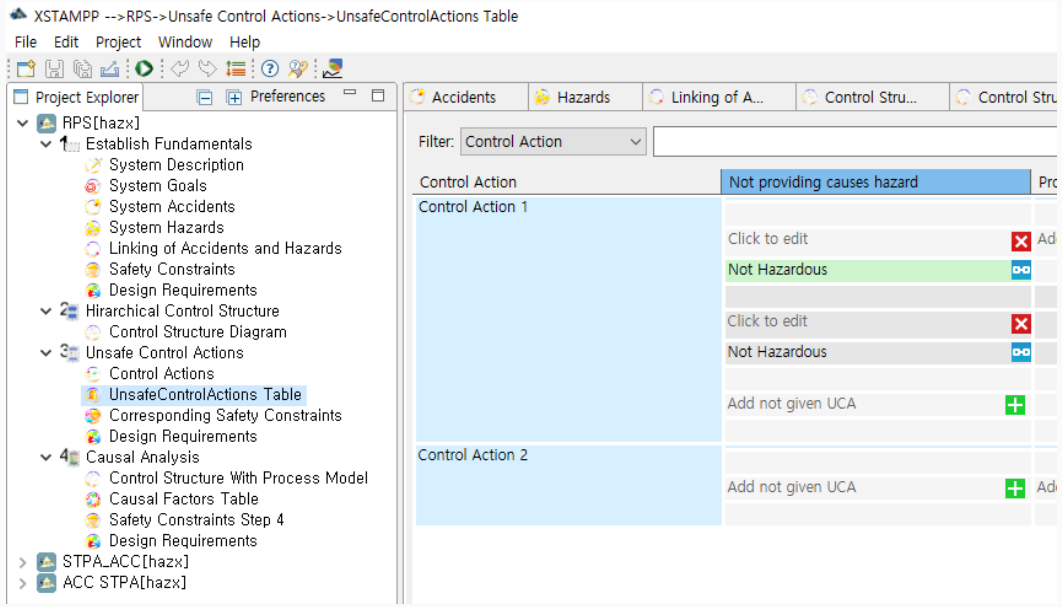


- 신한울 1,2호기, 새울 3,4호기 기준 Control Structure 도식화
- RPS Function에 해당하는 Component Group을 할당함.
- D3 분석을 위해 DPS Function + DMA Switch 까지 포함하는 DAS Component를 도식화

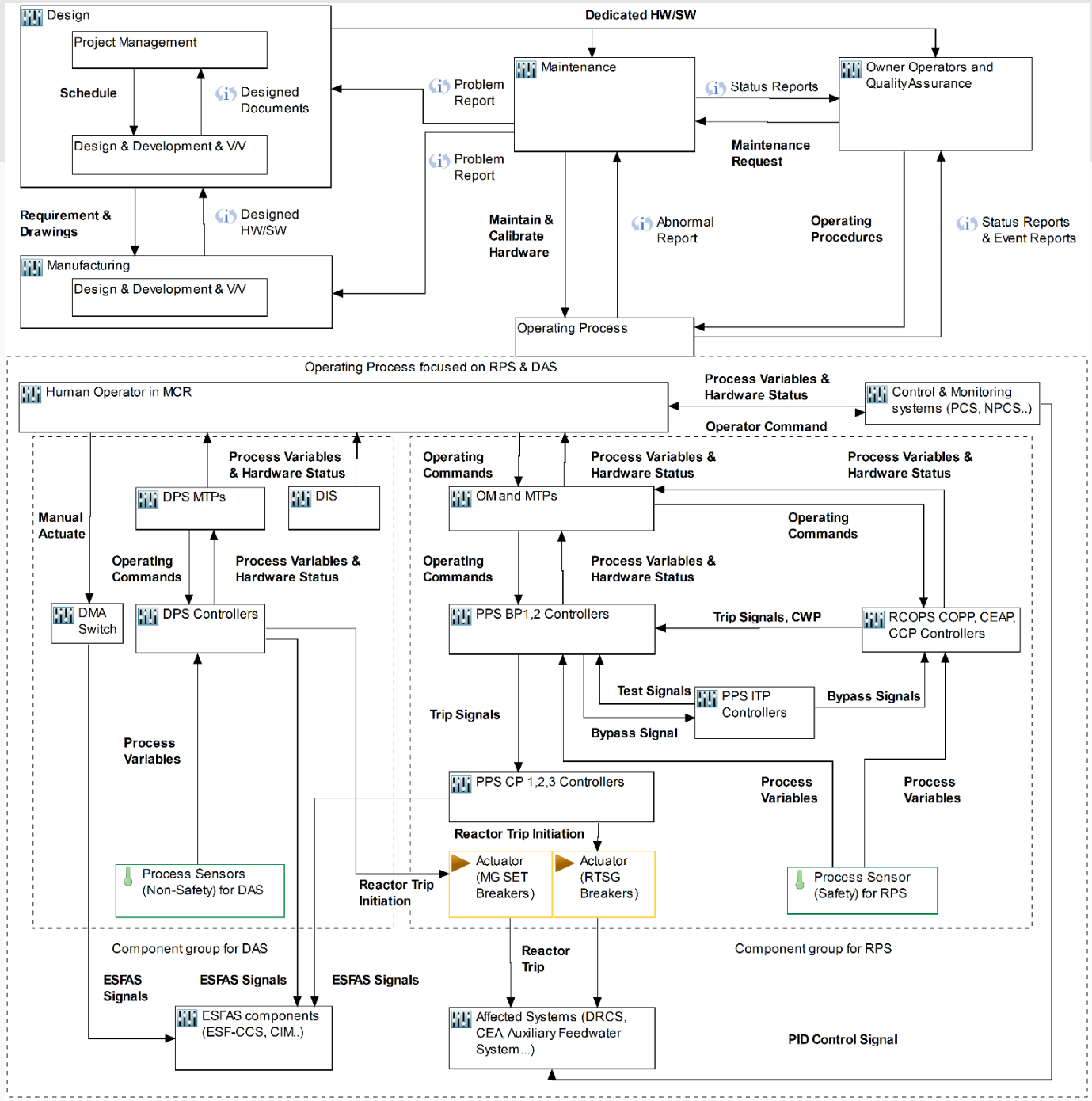
DAS : Diverse Actuation System

2 STEP 2: Control Structure

- STPA 전문 툴 사용 : XSTAMPP



- 공개되지 않은 설계 디테일을 그림에 싣는 것은 문제가 될 수 있으므로, 인터넷 검색가능 자료(FSAR, TR)에 공개된 내용에 한함.



Part 3.

STPA STEP 3~4 : UCA / Loss Scenarios

3 STEP 3 : Identify Unsafe Control Actions

- Unsafe Control Action (UCA)

Control Structure | Unsafe Control Ac... | Corresponding Saf... | Design Requireme... | Causal Factors Ta... | Safety Constraints | Control Structure ... | Control Actions

Corresponding Safety Constraints - RPS

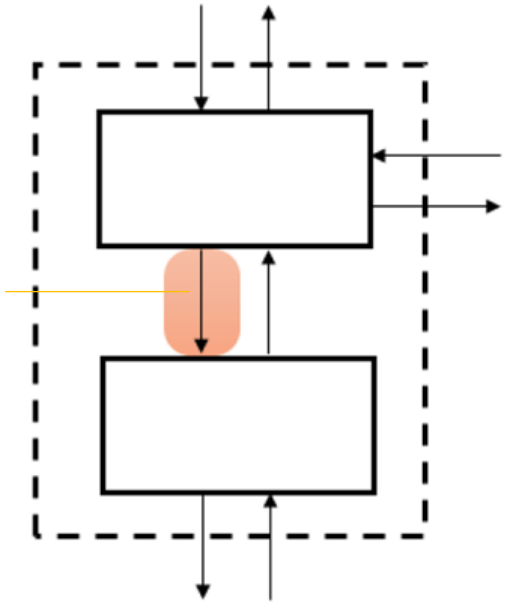
Filter: Control Action

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Schedule	N/A Not Hazardous Add not given UCA	Project Delay Not Hazardous Add given incorrectly UCA	N/A Not Hazardous Add wrong timing UCA	N/A Not Hazardous Add stopped too soon UCA
Operating Commands	UCA1.12 S0 OM and MTP do not provide a setpoint modification (including manual reset) signal when the operator sends request to change the setpoints. [H-5] [H-6] UCA1.82 S0 OM and MTP do not provide a bypass signal when the operator sends request to bypass channel(s). [H-5] [H-6] Click to edit Not Hazardous Add not given UCA	UCA1.13 S0 OM and MTP provide a incorrect setpoint value when the operator sends request to change the setpoints. [H-3] [H-8] UCA1.85 S0 OM and MTP provide a incorrect bypass signal in normal operation. [H-5] Add given incorrectly UCA	UCA1.14 S0 OM and MTP provide a setpoint modification signal too late when the operator sends request to change the setpoints. [H-6] [H-7] Add wrong timing UCA	UCA1.15 S OM and MTP provide a setpoint change signal within an insufficient amount of time and the signal is not received by th processor. [H-6] Add stopped too soon UCA
Maintain & Calibrate Hardware	UCA1.18 S0 Large uncertainties can be occured due to uncalibrated process instruments. [H-8] Add not given UCA	UCA1.19 S0 Large uncertainties can be occured due to incorrect process instruments. [H-8] Add given incorrectly UCA	N/A Not Hazardous Add wrong timing UCA	N/A Not Hazardous Add stopped too soon UCA
Operating		UCA1.22 S0		

Unsafe Control Action (UCA) 확인

+

제약사항 도출

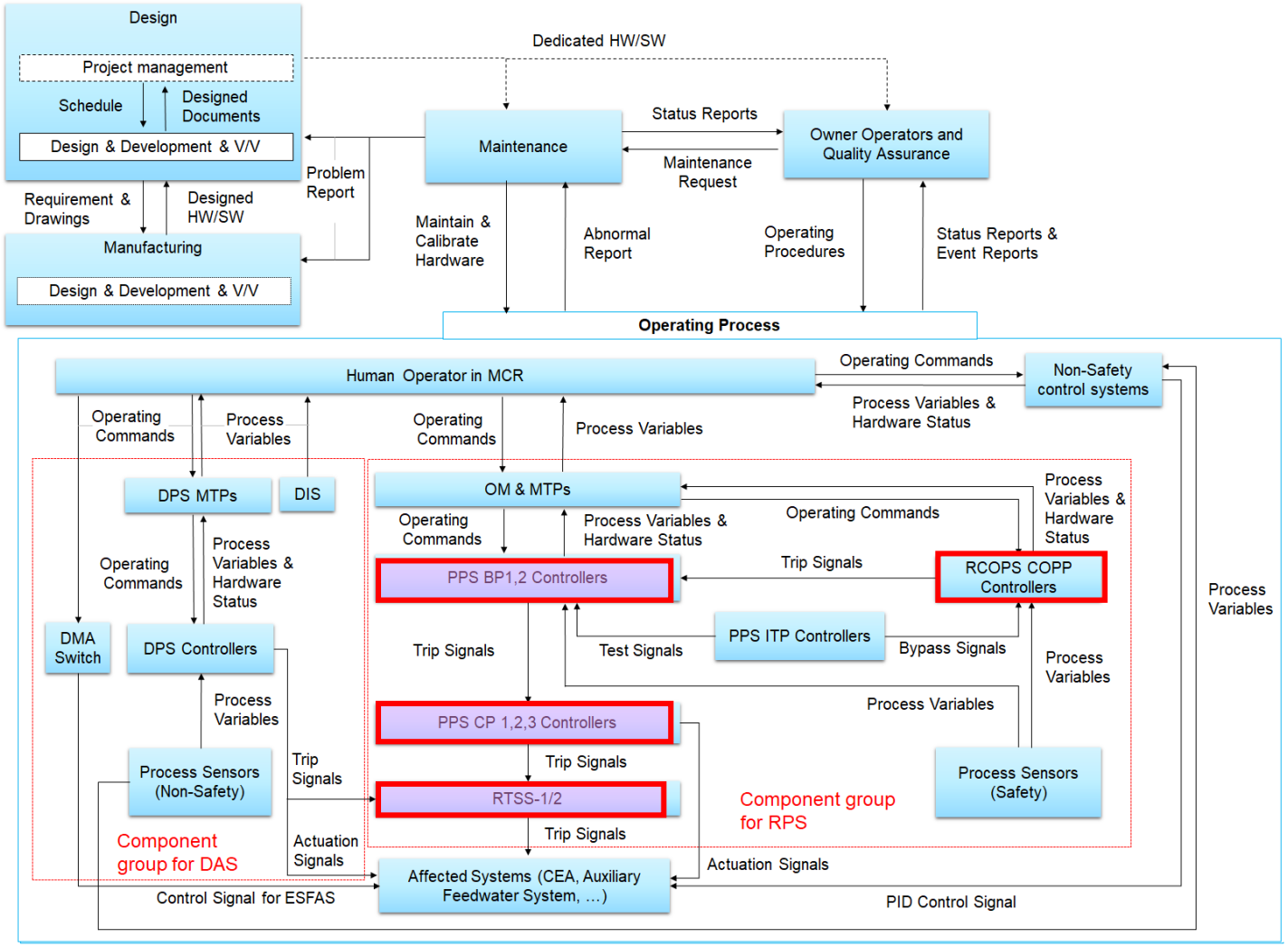


Items	#
Control Actions	34
UCA & Safety Constraints (UCA 및 안전제약 도출)	94
Causal Factor Tables (원인요소 분석)	39

3 STEP 4 : Identify Loss Scenarios

- Loss Scenario 확인
  - 한빛 4호기 (1998) : 조절제어봉 4,5번 그룹 낙하 인지 타이밍 문제로 제어봉 위치전도로 채널 트립
  - UCA : 변수의 부적절한 딜레이 전달

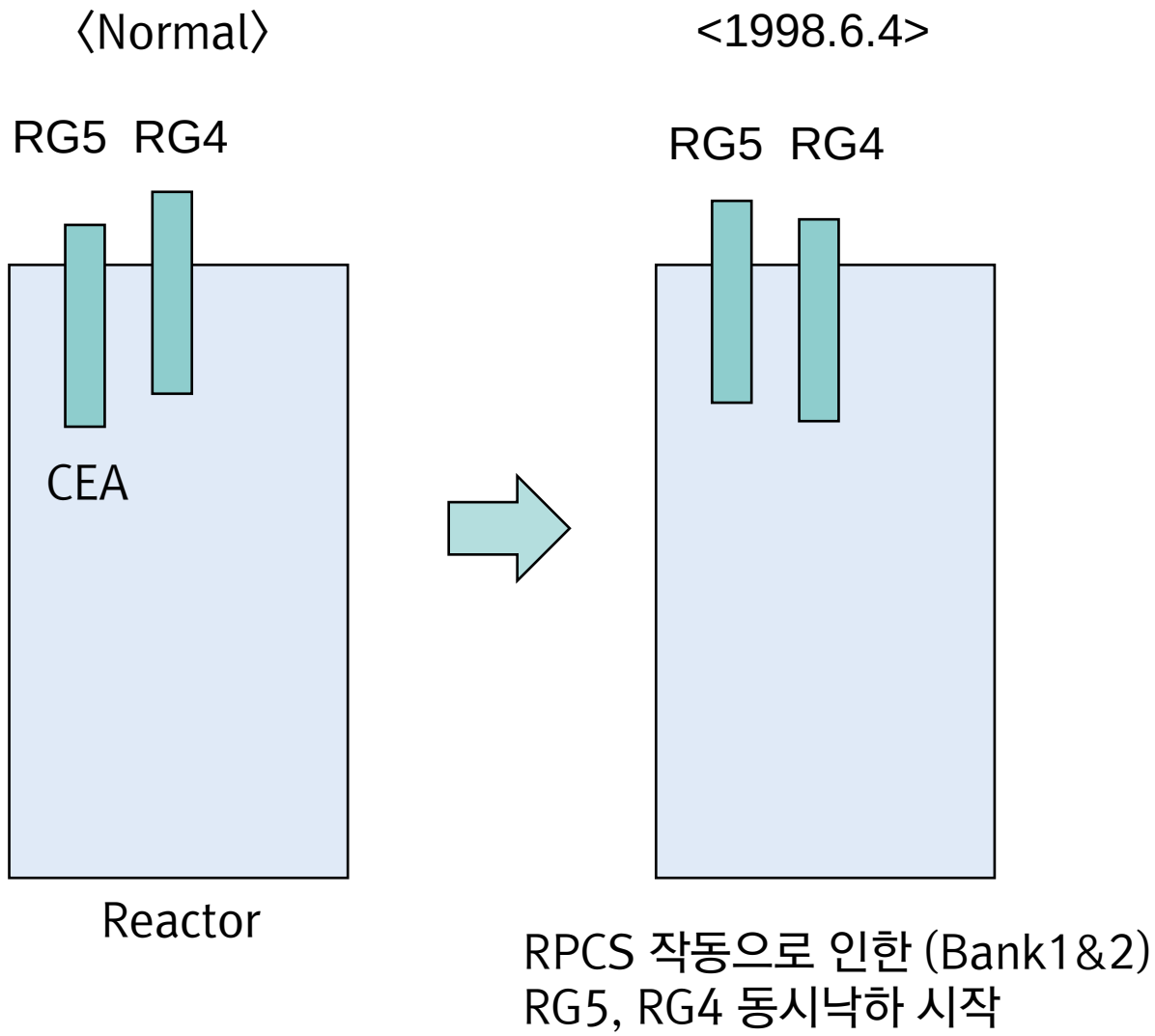
Unsafe Control Actions	Causal Factor
[UCA1.105] A processor provides process values and hardware status with inappropriate communication delays. [H-2, H-7]	Communication delay time related to CEA is not sufficient. [SC1.105]



3 STEP 4 : Identify Loss Scenarios

- Loss Scenario 확인
  - 한빛 4호기 (1998) : 조절제어봉 4,5번 그룹 낙하 인지 타이밍 문제로 제어봉 위치전도로 채널 트립
  - UCA : 변수의 부적절한 딜레이 전달

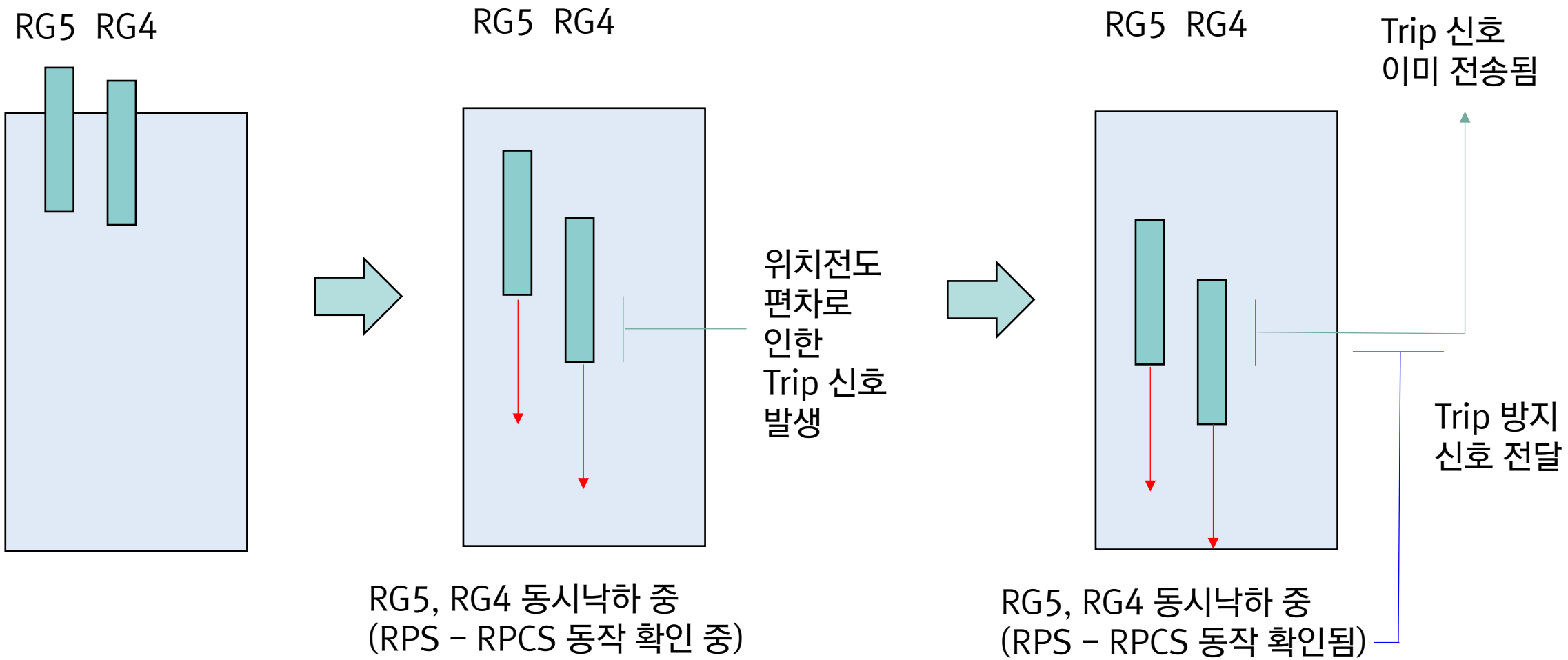
Unsafe Control Actions	Causal Factor
[UCA1.105] A processor provides process values and hardware status with inappropriate communication delays. [H-2, H-7]	Communication delay time related to CEA is not sufficient. [SC1.105]



RG: Regulating Group

3 STEP 4 : Identify Loss Scenarios

<1998.6.4>

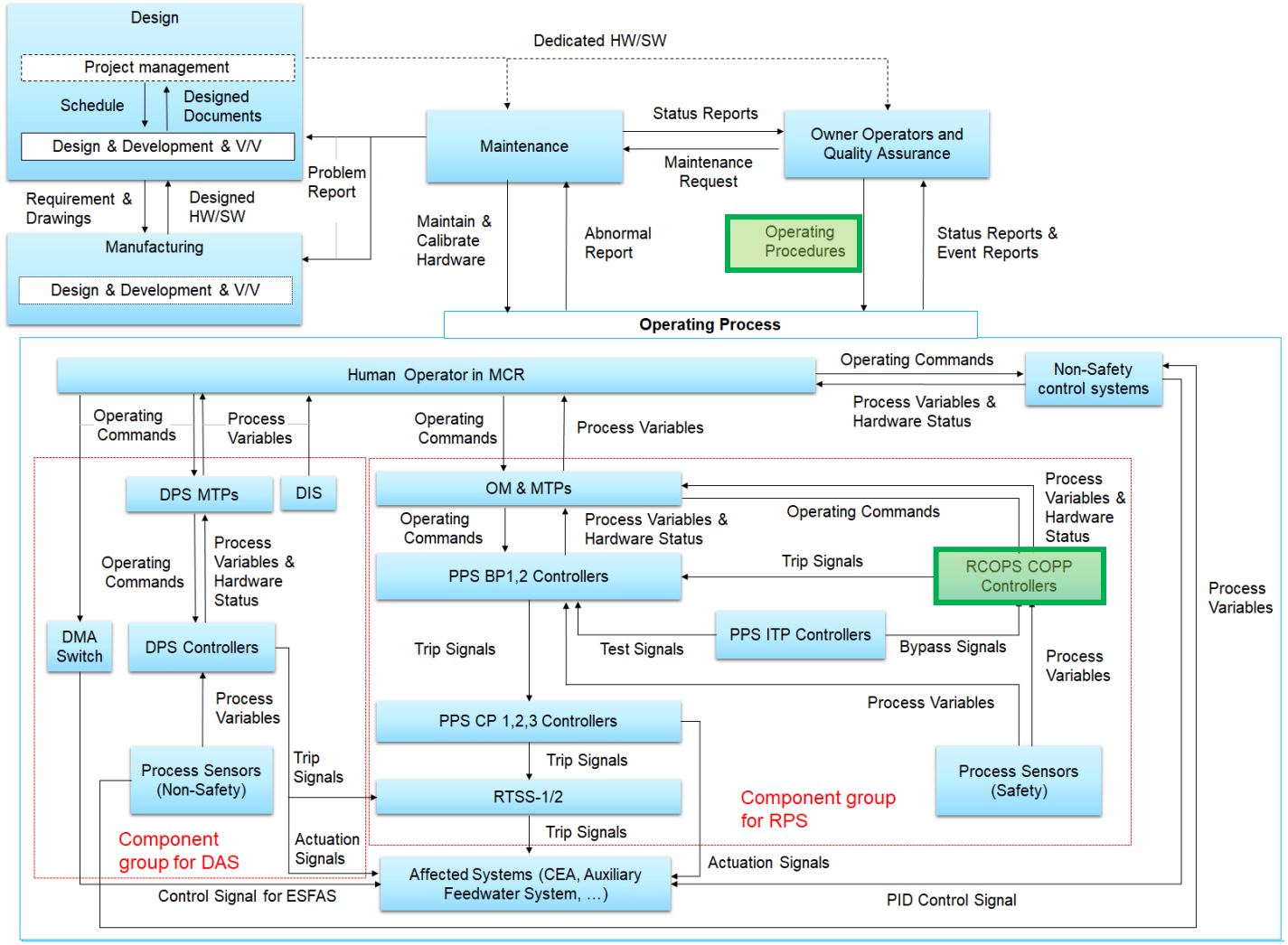


RG: Regulating Group

3 STEP 4 : Identify Loss Scenarios

- Loss Scenario 확인
  - 실제 이에 대한 조치는 운전원 절차서 수정 으로 이어졌고
  - 후속 APR1400에서는 CPCS S/W 개선으로 반영됨.

Unsafe Control Actions	Causal Factor
[UCA1.105] A processor provides process values and hardware status with inappropriate communication delays. [H-2, H-7]	Communication delay time related to CEA is not sufficient. [SC1.105]



3 Other examples

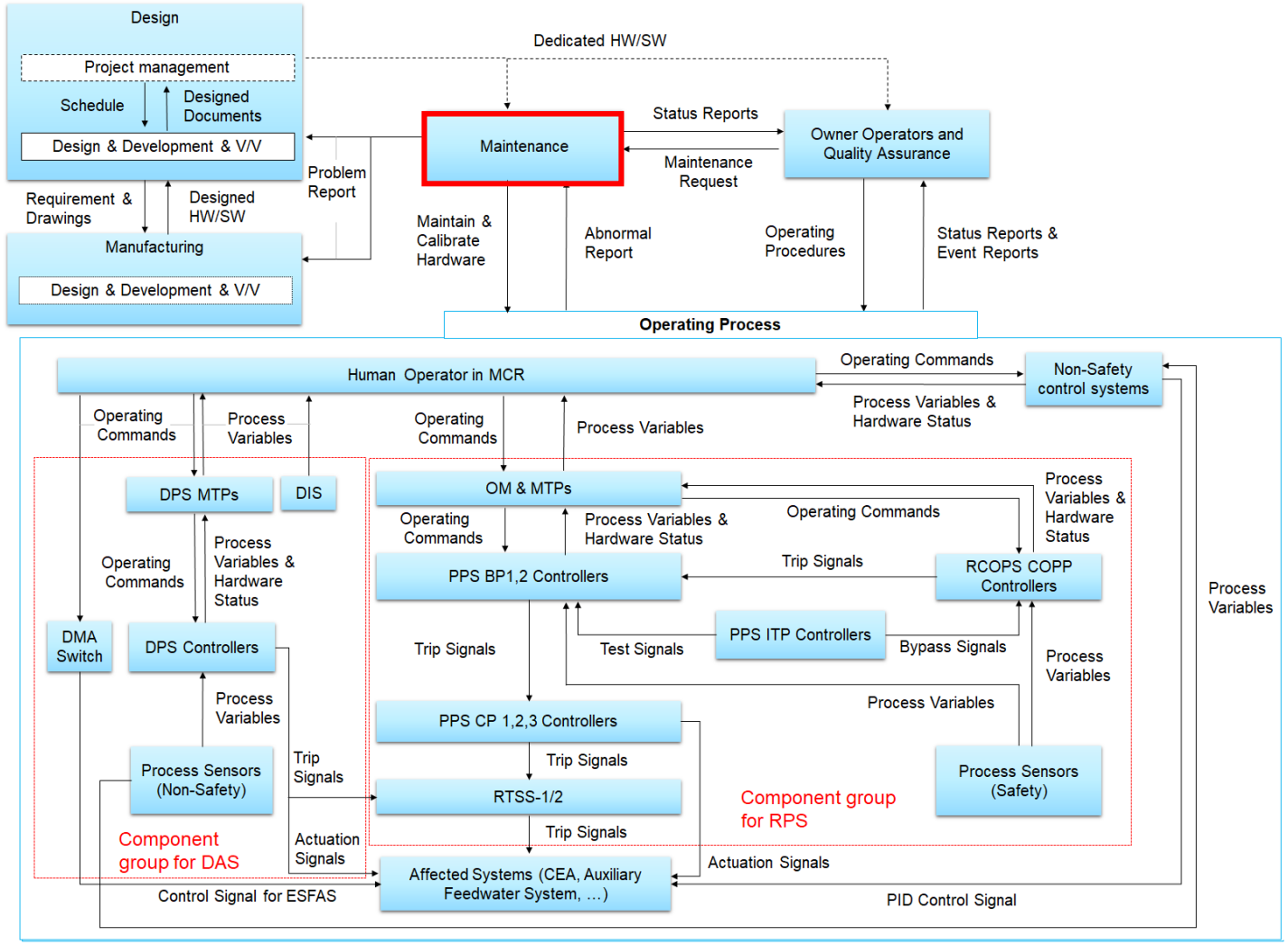
- Unsafe Control Action (UCA) 예
  - UCA1.193 : Spare sets of hardware or software with a design flaw (e.g., an internal digital fault) can be replaced at once during a maintenance period. [Hazard 1,3]
  - 예: 잠재적 고장을 지닌 PLC Controller 버젼이 RPS를 대상으로 정비기간에 다수 교체되었을 때

Component	Unsafe Control Actions	Causal Factor
Maintenance	[UCA1.18] Large uncertainties can be occurred due to uncalibrated process instruments. [H-8]	Uncalibrated sensors are used during operation. [SC1.18]
	[UCA1.141] QA does not provide a maintenance request even if the hardware is abnormal. [H-3, H-9]	Abnormal hardware is used with false positive indication. [SC1.19]
	[UCA1.193] Spare sets of hardware or software with a design flaw (e.g., an internal digital fault) can be replaced at once during a maintenance period. [H-1, H-3]	Abnormal hardware is replaced with false positive indication. [SC-23, SC-187]

3 Other examples

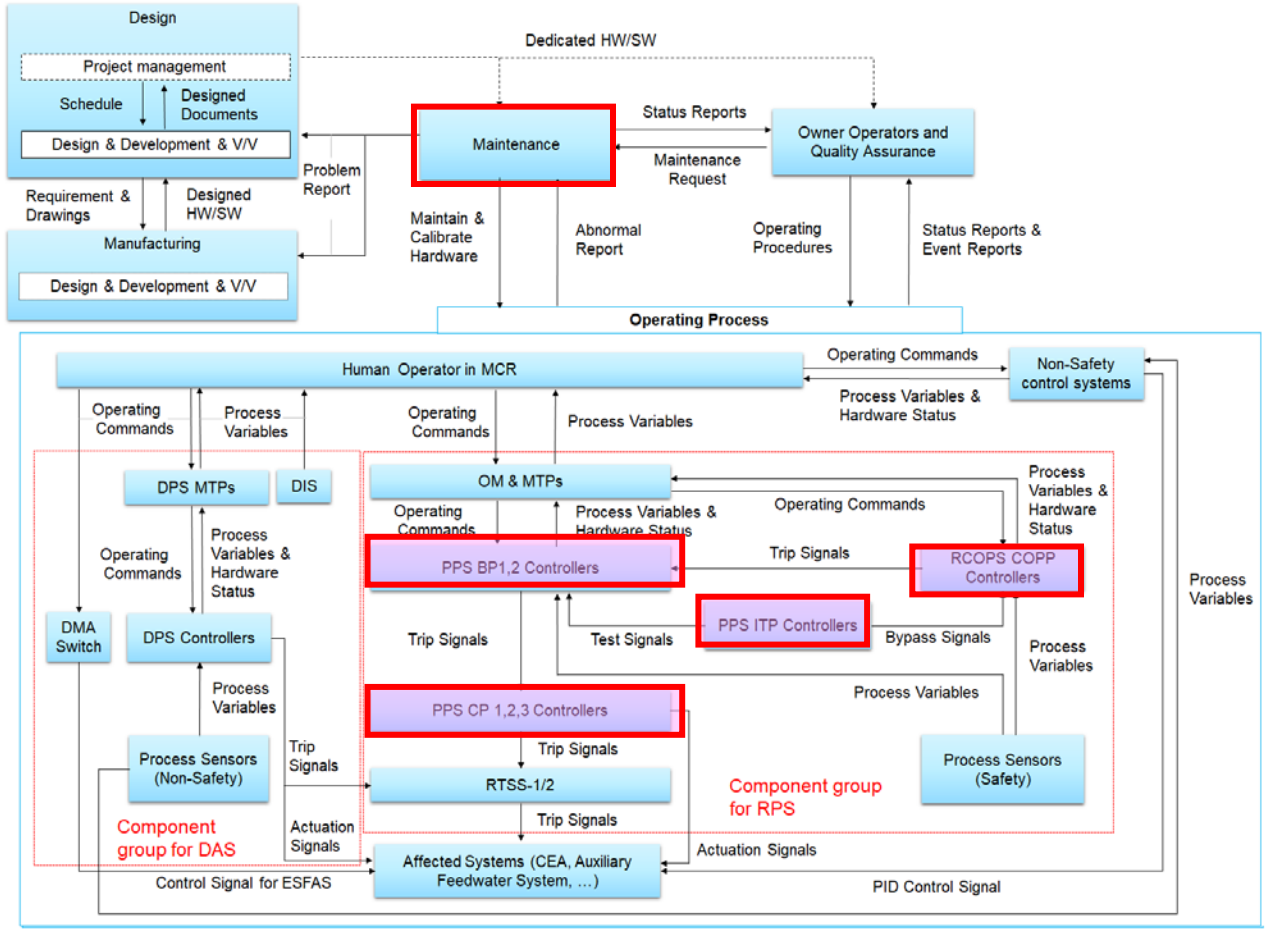
◦ Unsafe Control Action (UCA) 예

Unsafe Control Actions	Causal Factor
[UCA1.18] Large uncertainties can b e occurred due to uncalibrat ed process instruments. [H-8]	Uncalibrated sensors are used during operati on. [SC1.18]
[UCA1.141] QA does not provide a ma intenance request even if th e hardware is abnormal. [H-3, H-9]	Abnormal hardware is used with false positive indication. [SC1.19]
[UCA1.193] **Spare sets of hardware or software with a design flaw (e.g., an internal digit al fault) can be replaced a t once during a maintenan ce period.** [H-1, H-3]	Abnormal hardware is replaced with false posi tive indication. [SC-23, SC-187]



3 Other examples

- Loss Scenario 예
  - RPS Controller가 모두 교체된 상태에서 특정 Single Event가 발생할 경우



Part 4.

Conclusion

4 Conclusion

- NuScale 은 이미 STPA로 인허가를 받았기에, 한국 또한 지침 혹은 권고가 있을 것으로 예상됨
- D3 관점에서 RPS의 STPA 분석. 기존 FMEA 등으로 어려웠던 분석이 STPA로 가능함을 확인.
- 실제 상용원전의 사례를 대비하여 몇가지 Loss 시나리오를 도출.
- 거의 모든 신호라인들과 시스템 로직을 알아야 하므로,

  계통/SW 담당자들 개입없이는 STPA 분석은 쉽지 않을 것이라 여겨짐.

- 실제 정식 STPA 적용은 이 예비 연구보다 훨씬 더 시간이 많이 소모될 것으로 보임.

Thank you

한국원자력연구원
은 형 석