

KNS Spring Meeting, May 22-23, 2025

안전등급 디지털 I&C 계통의 CCF 대응을 위한 심층방어 및 다양성 (D3) 설계

[신한울 3,4호기 BTP 7-19, Rev.8 적용 위한 D3 설계]

2025. 5. 22

한국전력기술(주)

계측제어설계실

오 양 군

목 차

I 국내 원전 D3 요건의 변경이력 및 적용현황

II BTP 7-19, Rev.8 CCF/D3 요건 및 설계 적용

III BTP 7-19, Rev.9 CCF/D3 요건 및 대응

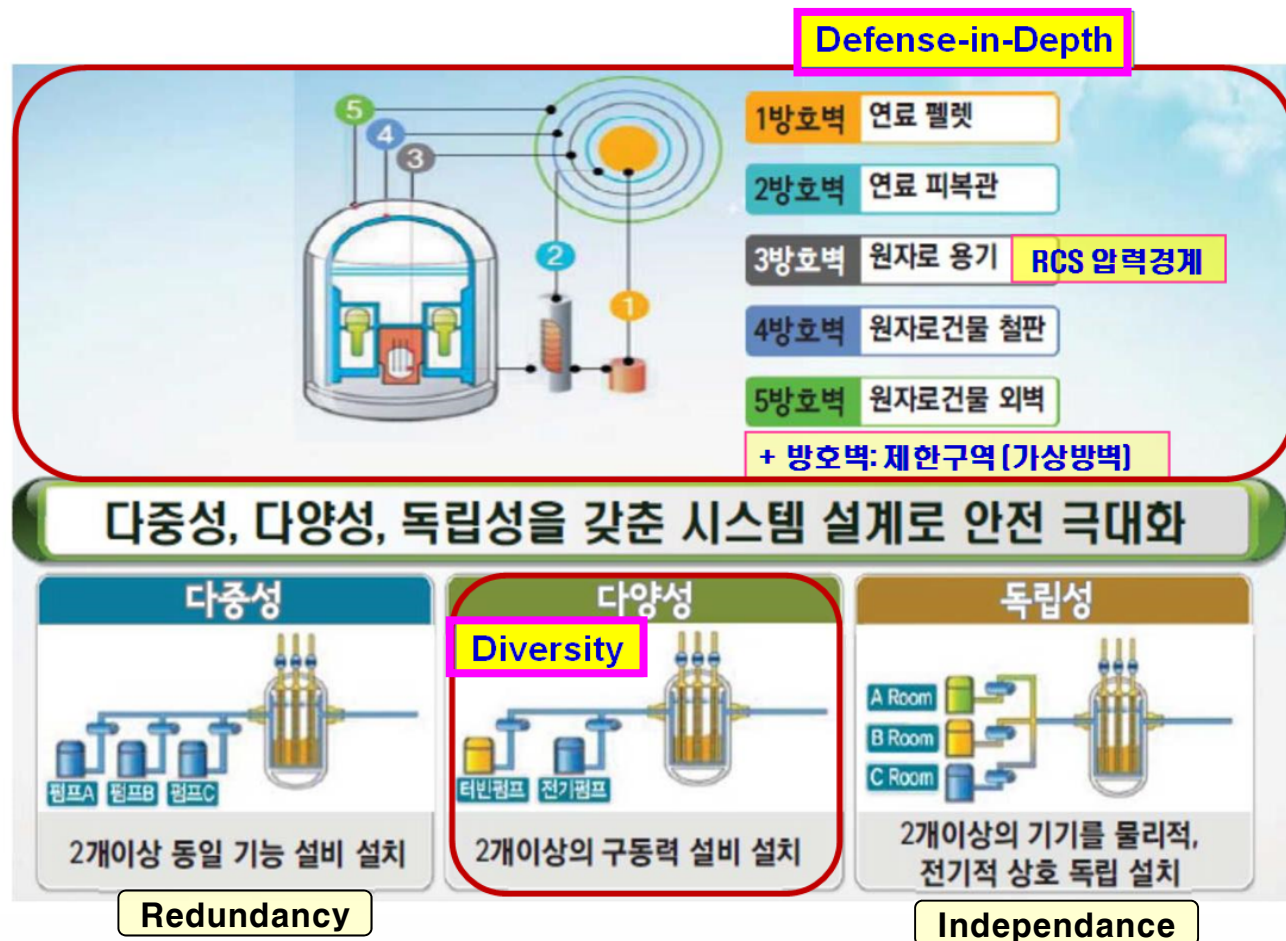
IV CCF/D3 요건 변화추세 및 설계

V 후속연구 및 Q&A

I. 국내 원전 D3 요건의 변경이력 및 적용현황

■ D3 (Defense-in-Depth & Diversity: 심층방어 및 다양성)

목적: 심층방어(DiD) 및 다양성(Diversity)을 갖추어 → 어떤 결함(공통원인고장 등)에 의한 사고가 → 계속 확대되어 → 방사능이 외부로 누출되는 것을 방지한다.



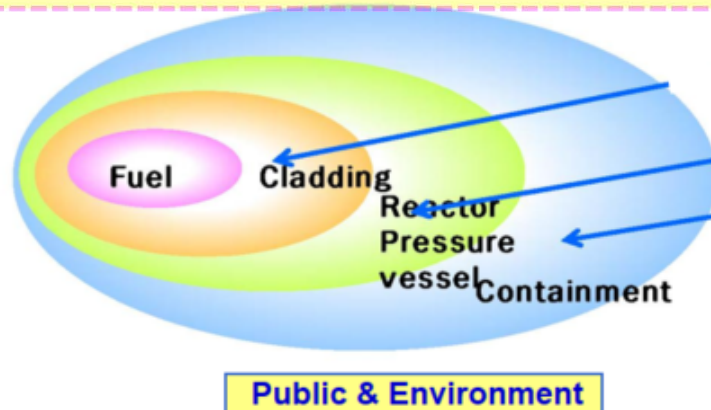
I. 국내 원전 D3 요건의 변경이력 및 적용현황

❖ Typical Plant DiD vs. I&C Echelon of Defense

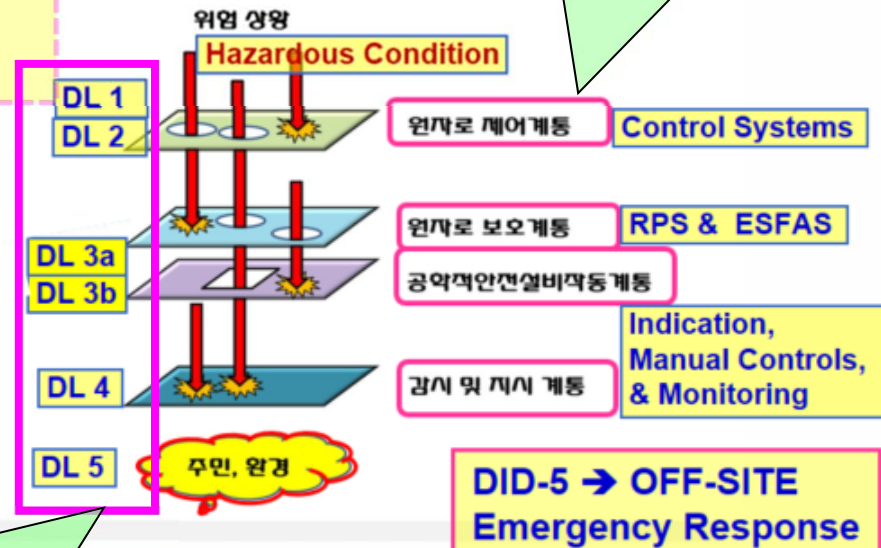
참조: NUREG/CR-6303 (2.2절), Dec. 1994

- “Echelons of defense” are specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it.

- Control System
- Reactor Trip System
- Engineered Safety Features Actuation System (ESFAS)
- Monitoring and Indicator System



원전의 계측제어 설비는 DiD 위해 4체계(4-Echelons) 방어 수단을 갖추고 있음.



유럽 EUR Rev.E DiD 등급 분류

[참조] 유럽 EUR Rev.E DiD Levels

Levels of DiD	Objective	Essential means	Radiological safety objectives (1)	EUR radiological targets (2)		Plant States	Design conditions
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	O1	Doses to the public during Normal Operation* and Anticipated Operational Occurrences* (Section 2.1.3.2.2 ; Discharge targets given in Table 2)	Operational States*	Normal Operation*	DBC-1
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features				Anticipated Operational Occurrences*	DBC-2
Level 3a	Control of Design Basis Accidents*	Safety Systems* and accident procedures	O2	Targets for Design Basis Accidents* given in Appendix B	Accident Conditions*	Design Basis Accidents*	DBC-3 DBC-4
Level 3b	Control of Complex Sequences* & prevention of core melt	Dedicated Safety Features for DEC* to prevent core melt and accident procedures		Target for Complex Sequences* given in Appendix B		Design Extension Conditions*	Complex Sequences*
Level 4	Control of accidents with core melt to limit off-site releases	Dedicated Safety Features for DEC* to mitigate core melt and accident management	O3	CLI target for Severe Accidents* given in Appendix B			Severe Accidents*
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	On-site and Off-site emergency preparedness and response	-	-		-	-

Table1: EUR representation of **Defence-in-Depth*** and associated **Plant States***, based on **WENRA** and **IAEA** approaches.

- (1) See **WENRA** RHWG Report Safety of new NPP designs, March 2013, for the explanation of safety objectives O1, O2, O3
 (2) **EUR** Radiological targets are defined in accordance with **EUR** safety objectives given in section 2.1.3



EUROPEAN UTILITY REQUIREMENTS FOR LWR NUCLEAR POWER PLANTS

I. 국내 원전 D3 요건의 변경이력 및 적용현황

한울5,6호기에 국내 최초로 Digital PPS/ESFAS-AC
위해 SRM-SECY-93-087 요건 적용

- USNRC → **SRM-SECY-93-087**(July 1993) ← SECY-93-087(April 1993)

- ❖ II.Q "Defense Against **Common-Mode Failures** in Digital Instrumentation and Control Systems" ← Digital I&C 계통의 CMF에 대한 방어요건을 제시



- USNRC → **BTP HICB-19, Rev.4** (June 1997)

- ❖ "Guidance for Evaluation of Defense-in-Depth & Diversity in Digital I&C Systems" ← D3 평가지침

국내 최초의 APR1400 새울1,2호기부터 Digital
안전등급 I&C 설계 위해 BTP HICB-19 요건 적용



- 국내 원전의 계통설계 적용 → **BTP HICB-19, Rev.4** D3 요건을 반영

- ❖ APR1400: 새울 1,2, BNPP 1,2,3,4, 신한울 1,2호기의 DPS, DIS 설계에 적용



- USNRC → **BTP 7-19, Rev.5** (Mar. 2007)

- ❖ Guidance for Evaluation of Diversity & Defense-in-Depth (D3) in Digital Computer-based I&C Systems ← D3 평가지침

- ❖ 특징: [1] 용어변경: **CMF(Common-Mode Failure)** → **CCF(Common-Cause Failure)**,
[2] LB-LOCA 관련 CMF 취약점은 누설-검출과 사전에 준비된 운전-절차에 근거하여
시정조치가 가능함을 허용한다는 설명을 삭제 → DPS에 SIAS/CIAS 추가됨



- 국내 계통설계 적용 → **BTP 7-19, Rev.5** D3 요건 → 새울 3,4호기 DPS/DIS/D3 적용

I. 국내 원전 D3 요건의 변경이력 및 적용현황

BTP 7-19, Rev.6 부터 'Spurious Actuation' 요건 등장

- USNRC → BTP 7-19, Rev.6 (July 2012)
 - ❖ "Guidance for Evaluation of D3 in Digital Computer-based I&C Systems"
 - ❖ 특징: [1] 운전원-수동조치 → HFE 분석 포함. [2] CCF 오작동 영향을 검토, [3] 시험성이 100% 입증되면 S/W CCF가 없는 것으로 간주 가능

● 국내 SD 적용 → BTP 7-19, Rev.6 D3 요건 → NRC-DC D3 TeR 적용

- USNRC → BTP 7-19, Rev.7 (Aug. 2016)
 - ❖ D3 평가의 기술적 변경사항 없음 (참조한 RG, Std 등을 Update)

- USNRC → BTP 7-19, Rev.8 (Jan. 2021) → Rev.9 (May 2024)
 - ❖ "Guidance for Evaluation of Defense-in-Depth & Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems" ← 잠복한 설계결함에 의한 CCF 관점에서의 D3 평가지침
 - ❖ 특징: [1] CCF에 의한 오작동, 부분작동 + 오지시 결합을 고려, [2] Rev.5에서 삭제된 Justification 내용을 재기술, [3] 안전-중요도에 따른 계통분류를 설명.

[오작동] 외에도 [Partial Act]+[False Ind], [Total Act-Failure]+[False Ind] 고려를 추천

I. 국내 원전 D3 요건의 변경이력 및 적용현황

● 국내 SD → BTP 7-19, R8 D3 요건 → 신한울 3,4호기 DPS/DIS/D3 적용

(SRM-SECY-93-087) & (BTP 7-19, Rev.8) → 신한울3,4호기 D3 요건의 Couple!

● USNRC → SECY-22-0076 (Aug. 2022)

❖ Expansion of Current Policy on Potential CCFs in Digital I&C Systems
→ (확장된) RPS D3 분석방법 제시 ← 리스크정보접근(RIA)을 확장하여 적용

● USNRC → SRM-SECY-22-0076 (Mar. 2023)

❖ Staff Req. – SECY-22-0076 - Expansion of Current Policy on Potential CCFs in Digital I&C Systems → NRC가 DiD 평가에 RIA 승인한 내용을 설명

(SRM-SECY-22-0076) & (BTP 7-19, Rev.9) → 신규 D3 요건의 Couple!

● USNRC → BTP 7-19, Rev.9 (May 2024) → 수출용 APR1000에 적용 진행중

❖ 제목: Rev.8 대비 동일함 ← CCF 관점에서의 D3 평가지침

❖ 특징: [1] CCF는 Single Random 고장과 다름을 설명, [2] I&C의 CCF 대응방법을 체계적으로 설명 (1안: 안전등급 I&C 내부적으로 해결, 2안: 다양성 수단을 사용, 3안: CCF 결과가 허용-가능함을 설명, 4안: 리스크-중요도 상응하는 CCF 대응조치)

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

- ❖ BTP 7-19, Rev.8 CCF/D3 요건의 계통설계 적용
 - 신한울3,4호기 고장유형-3 RPS/ESFAS 오작동(Spurious Operation) 분석
 - 신한울3,4호기 CCF에 의한 RPS/ESFAS 부분-오작동 및 QIAS-P 오지시 평가
 - 신한울3,4호기 CCF에 의한 RPS/ESFAS 다수 안전기능의 동시-오작동 평가
- ❖ CCF 대상-여부 판단 시 참조
 - BTP 7-19, Rev.8: 단일/랜덤/종속(Cascading) 고장은 CCF 평가에서 배제
 - SECY-22-0076, "The nuclear power industry is implementing modern digital I&C technologies. - - -, they can also introduce new types of potential systematic, nonrandom, concurrent failures of redundant elements, also known as CCFs, in the design of protection systems." (밑줄 표시한 부분은 USNRC 10 CFR 50, App. A에도 동일하게 기술됨)
 - CCF 평가대상: 다중화된(Redundant) 설비의 기능 수행에 영향이 있는 체계적인(Systematic), 랜덤하지 않은(Non-random), 동시성(Concurrent) 있는 고장
 - CCF 오작동: 다중화된 설비에서, 입력에 응답을 못하는 무-작동 혹은 입력과 관계 없는 불필요한-작동을 의미. 2개 이상의 설비가 동시성을 갖고, 랜덤하지 않으며, 체계적 분석이 가능한 고장만이 오작동 평가의 대상임 (단일-랜덤-고장은 미포함)

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

[1] 신한울3,4호기 고장유형-3 RPS/ESFAS 오작동 분석

- BTP 7-19, Rev.8 적용에 따라 고장유형-3 분석을 추가 수행 (고장유형-3은 입력변수 값이 계통의 작동 혹은 트립을 요구하지 않는 경우임에도 불구하고, 해당 안전계통의 S/W CCF로 인해서 불필요한 작동 혹은 트립을 발생시키는 오작동을 의미함)
[참고: '고장유형-1'은 방어계층 간에 상호작용으로 인해 발생하는 고장이며, '고장유형-2'는 보호계통이 CCF로 인해 안전기능을 작동시키지 못하는 고장]

● RPS 고장유형-3 원자로정지 오작동 시나리오 및 평가결과

- ❖ 오작동 시나리오/후속영향: CCF로 인한 원자로정지 오작동에 의한 원자로 트립 신호는 RTSS의 원자로정지 스위치기어를 작동시켜서, 제어봉 구동 전원을 자동으로 차단하므로, 노심에 제어봉이 삽입되고, 이후 운전원의 '원자로정지 후 운전 절차(Plant Post Reactor Trip Procedure)'가 수행되면 발전소는 안전정지상태에 도달이 가능함.
- ❖ 평가 결과: CCF로 인한 원자로정지 오작동은 발전소 안전을 위협하지 않음.
- ❖ 평가 근거: 정상운전 중에 불필요한 원자로정지가 발생하면 발전소 안전에 문제를 발생시키지 않으며, 후속 안전조치가 가능함. (참조: SAR 15장은 불필요한 원자로 정지를 초기사건으로 고려하지 않음)

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

❖ 신한울 3,4호기 고장유형-3 ESFAS 오작동 분석

- 안전주입 오작동
- 보조급수 오작동
- 원자로건물 살수 오작동
- 원자로건물 퍼지격리 오작동 (A/E)
- 원자로건물 격리 오작동
- 주증기 격리 오작동
- 주제어실 비상환기 오작동 (A/E)
- 핵연료취급지역 비상환기 오작동 (A/E)

● 고장유형-3 ESFAS 안전주입 오작동 시나리오 및 평가 (예)

- ❖ 오작동 시나리오/후속영향: RCS의 정상 운전압력이 유지되는 중에 CCF로 인한 ESFAS의 오작동으로 안전주입신호(SIAS)가 발생해서 SI 펌프를 작동시키면, SI 펌프 체절수두압력 (Shut-off Head Pressure)이 RCS 정상운전압력 대비 낮으므로, 안전주입계통 밸브의 작동 여부와 관계없이 안전주입 발생은 불가능함.
- ❖ 평가 결과: CCF로 인한 안전주입 오작동은 발전소 안전을 위협하지 않음.
- ❖ 평가 근거: 안전주입(SI) 오작동은 SAR 15.5.1절 비상노심냉각계통의 부주의한 작동 사건과 같이 전개됨. RCS 정상운전 중에는 SI 펌프의 체절수두압력이 RCS 정상 운전압력 대비 낮으므로 SIS 밸브 작동 여부와 관계없이 실제 안전주입 발생은 불가능함. (정지운전 중에 안전주입-오작동은 계통에 과압을 초래할 수 있지만, SAR 15장에서 평가한 결과의 허용기준 이내임을 확인함.)

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

[2] 신한울3,4호기 CCF에 의한 부분-오작동+오지시 평가

- 신한울3,4호기의 공통원인고장 평가는 [1] 기능-관점에서, [2] 2개-이상 부분/전체 설비에서, [3] 동시에 발생하는 오작동을 평가함.
- 신한울3,4호기는 다양성 I&C를 포함 → CCF로 인한 안전기능의 부분-작동 상황에서 (QIAS-P의 오지시 가능성을 가정하더라도) 운전원은 안전계통의 CCF 영향을 받지 않는 DIS 및 IPS의 가용한 다양성 지시정보를 참조하여 안전조치 수행이 가능함.

● CCF에 의한 원자로정지 오작동 + 오지시 대응(예)

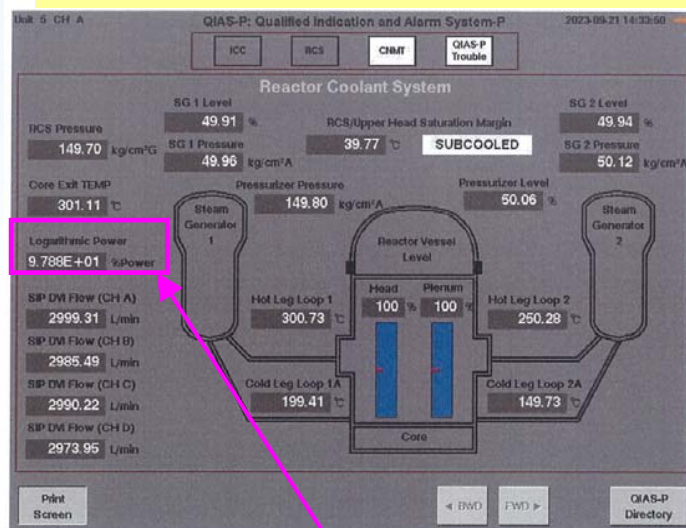
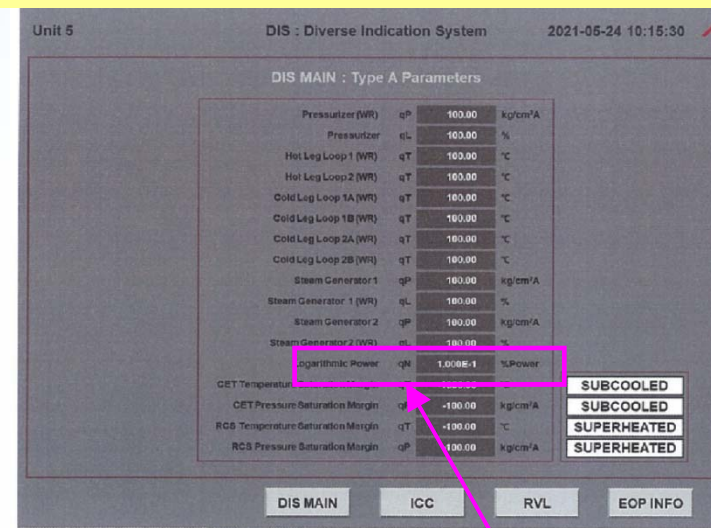


Figure 7. Reactor Coolant System Display (Channel A Only)

QIAS-P 화면 (w/ CCF)
→ ENFMS Log Power 지시



DIS 화면 (w/o CCF)
→ ENFMS Log Power 지시

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

❖ 신한울3,4: CCF 부분-오작동 및 오지시 가능성에 대한 평가 (계속)

● CCF에 의한 원자로정지 오작동 + 오지시 대응 (계속)

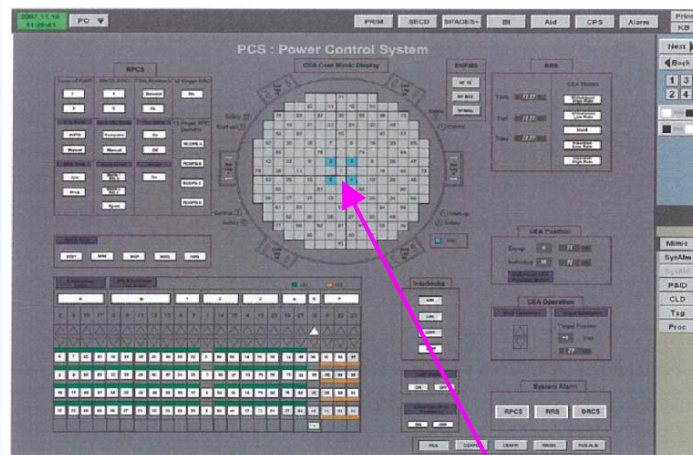


FIGURE 1 Power Control System Main Display

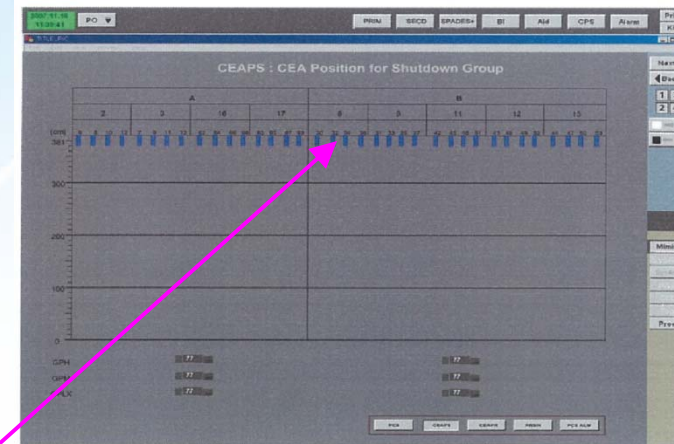


FIGURE 2 DRCS CEA Position Display for Shutdown Group

IPS – PCS 화면
(w/o CCF)

QIAS-P 화면
(w/ CCF)

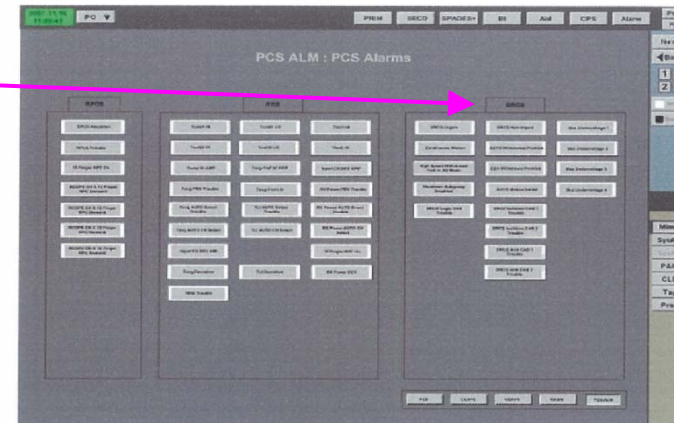


FIGURE 5 PCS Alarms Display

II. BTP 7-19, Rev.8 CCF/D3 요건 및 적용

[3] 신한울3,4호기 CCF에 의한 다수 안전기능의 동시-오작동 평가

- RPS 및 ESFAS의 동시-다발적인 오작동은 → 핵연료 건전성 및 원자로냉각재계통(RCS) 압력 경계의 건전성에 영향을 미칠 수 있음.
- 핵연료 건전성이 악화되는 경우는 → 정상 운전에 비해 노심 출력의 상승, RCS 온도 상승, 또는 압력이 감소하는 경우임.
- PPS 오작동 항목 중에서 노심 출력을 증가시키는 경우는 보조급수주입-오작동이며, 이에 대한 평가결과는 발전소 안전을 위협하는 상황을 초래하지 않음. 상세 내용은 PSAR 15.1.1(급수온도 감소) 및 15.1.2(급수유량 증가)를 참조.
- 그러므로 RPS/ESFAS 동시-다발적 오작동에 따른 핵연료 안전성은 보장됨.
- RCS 압력경계의 건전성이 악화되는 경우는 → 정상 운전에 비해 노심 출력의 상승, RCS 온도 상승, 또는 압력이 증가하는 경우임.
- PPS 오작동 항목 중에서 RCS 압력을 증가시키는 경우는 주증기격리-오작동이며, 이에 대한 평가 결과는 고압력에 의한 원자로정지와 POSRV와 MSSV의 여닫힘으로 발전소는 안정상태 유지가 가능함.
- RPS/ESFAS 동시-다발적 오작동에 따른 RCS 압력경계의 안전성은 보장됨.

III. BTP 7-19, Rev.9 CCF/D3 요건 및 대응

❖ BTP 7-19, Rev.9에서 변경된 주요 CCF 및 D3 요건

- P1/P2/P3: 기존 D3 평가방식 + 리스크정보접근(RIA)을 확장하여 적용 가능
- RIA 사용시: CCF 모델링, PRA, 리스크-중요도, 안전-중요도 등의 적용이 필요
- SRM-SECY-22-0076 기반으로 확장된 4 Point 요건을 설명 (기존 4P 요건 w/ RIA)

(SRM-SECY-22-0076) & (BTP 7-19, Rev.9) → 신규 D3 요건의 Couple!

❖ 참조: 리스크정보접근(RIA) 개념 (NRC Executive Director, Dec. 2018)

- 리스크정보접근(RIA) → 설계-운전 현안이 건강과 안전 중요성에 상응하도록 리스크 정보(통찰력)를 다른 요소와 함께 고려하여 요건을 정립하는 철학 (파-면허자와 규제-주의사항이 건강과 안전 중요성에 상응하는 설계와 운전-현안에 좀 더 집중이 목적임)



Application of the Concept of Graded
Approach in Core Regulatory Functions:
Risk-Informed Decision Making (RIDM)

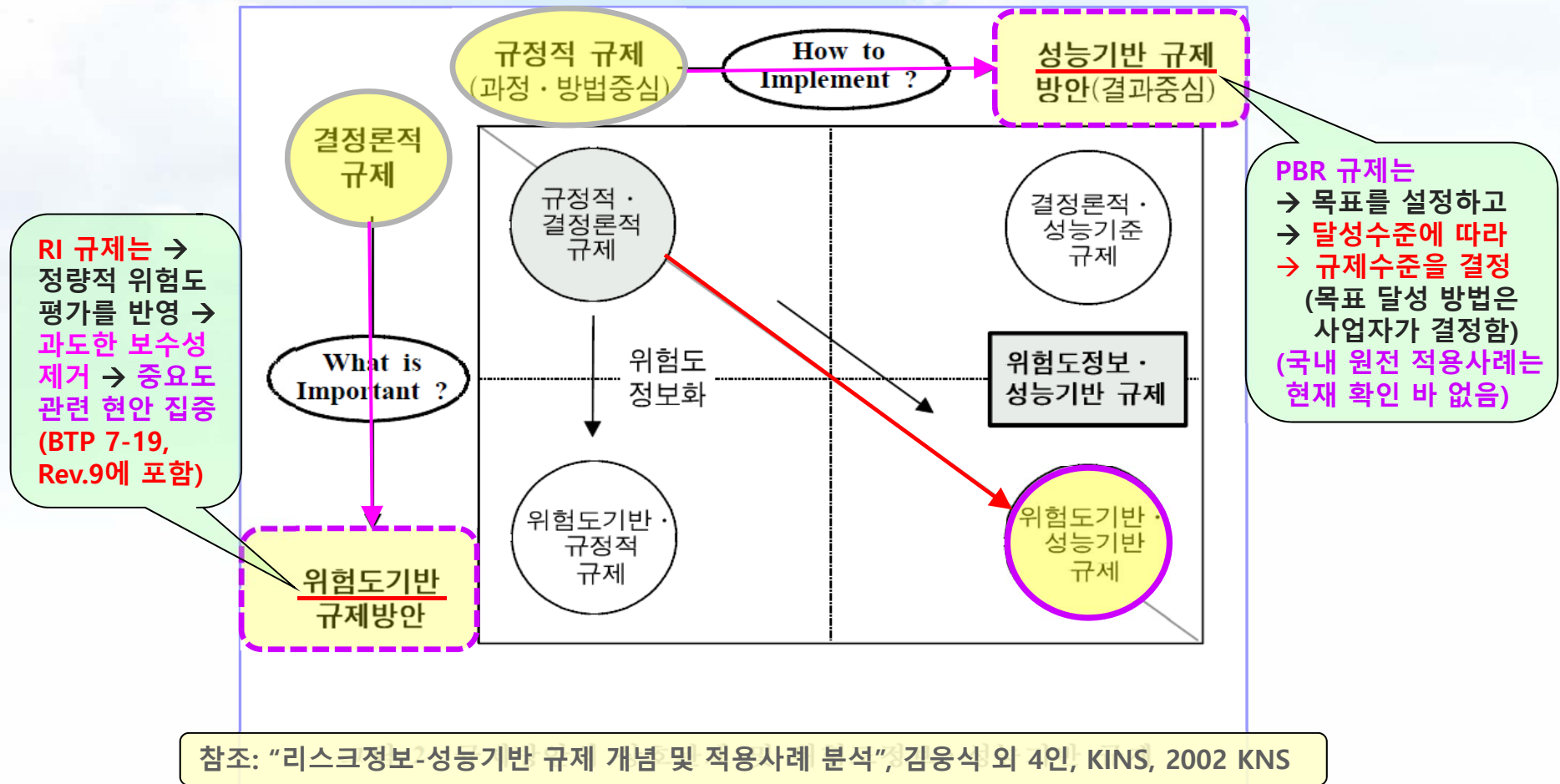
Executive Director of Operations
U.S. Nuclear Regulatory Commission

Risk-Informed Approach*

A "risk-informed" approach to regulatory decision-making represents a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to health and safety.

III. BTP 7-19, Rev.9의 CCF/D3 요건 및 대응

❖ 리스크-정보(RI) vs. 성능-기반-규제(PBR)의 개념



❖ 참조: BTP 7-19, R8~R9 개정과정 및 결과

- BTP 7-19, Rev.8 → January 2021 → PRA/RIA: 1회씩, Risk: 13회 기술
- SECY-22-0076 → August 10, 2022 → CCF 정책-확장을 요구 (w/ RIA)
- SRM-SECY-22-0076 → May 25, 2023 → Risk/RIA/RIDM 등 14회 기술
- BTP 7-19, Rev.9 → May 2024 → Risk-Informed: 60회 이상, Risk: 170회 이상 기술

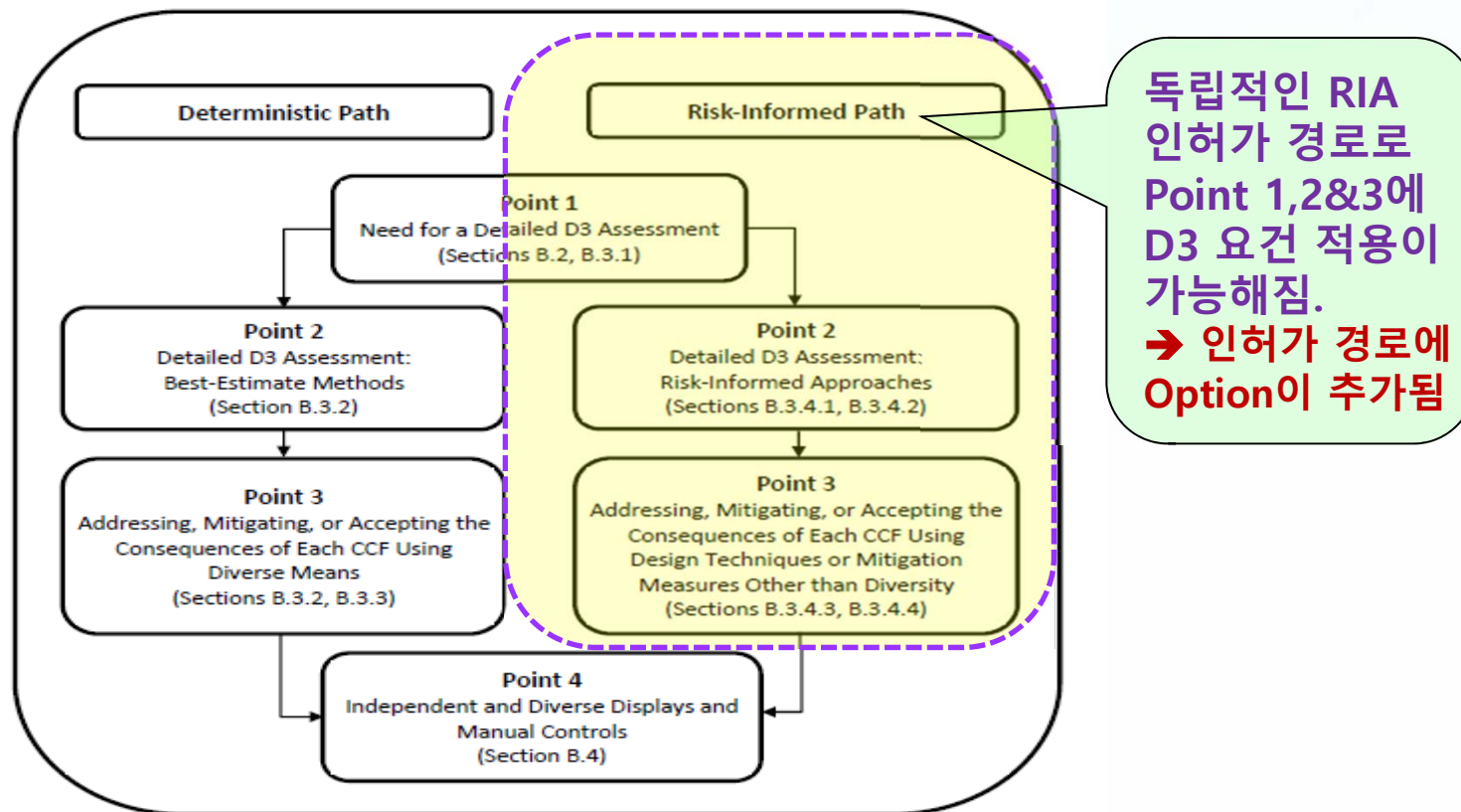
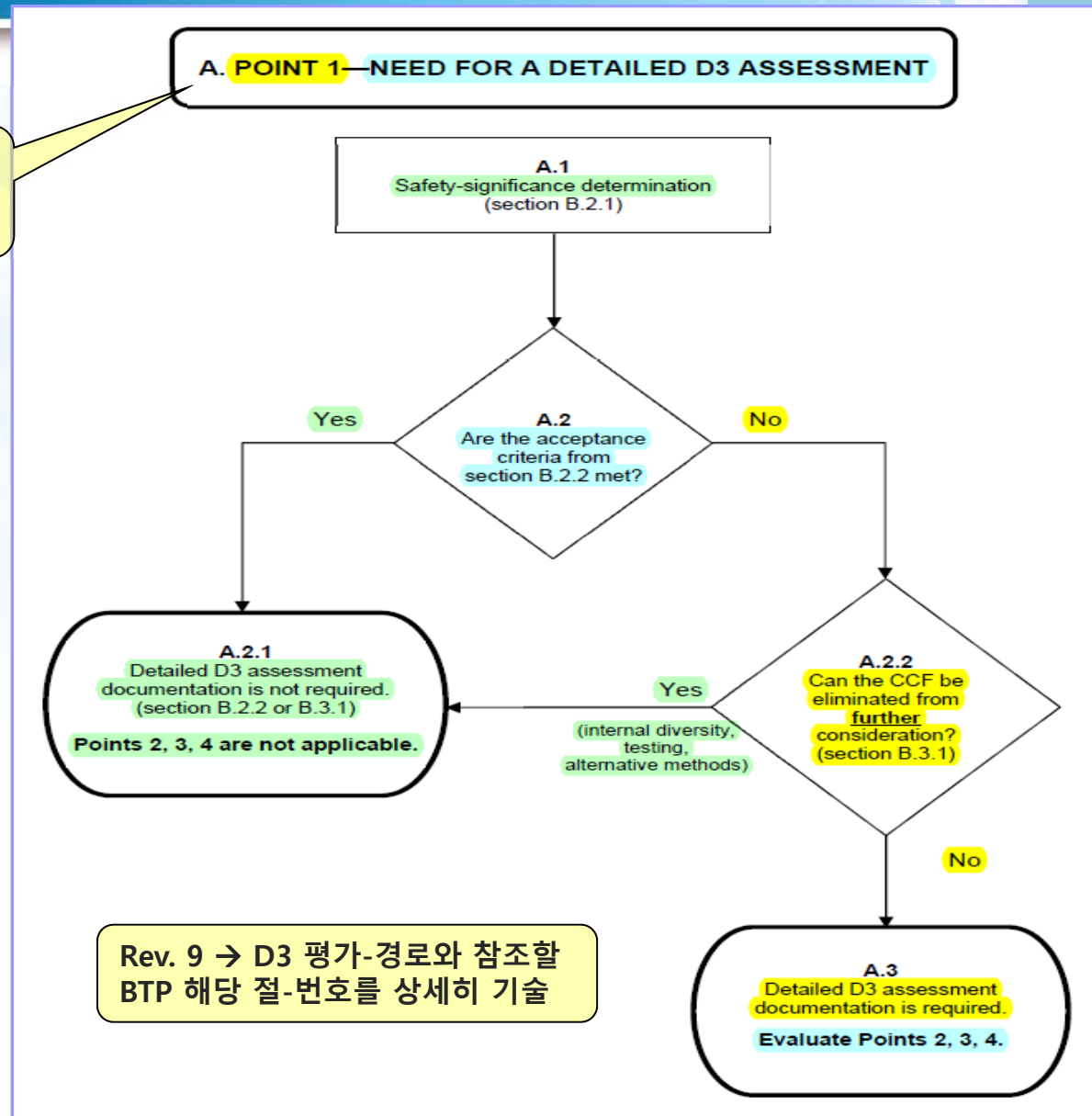


Figure 7-19-1 Four points of SRM-SECY-22-0076 and applicable BTP 7-19 sections

III. BTP 7-19, Rev.9의 CCF/D3 요건 및 대응

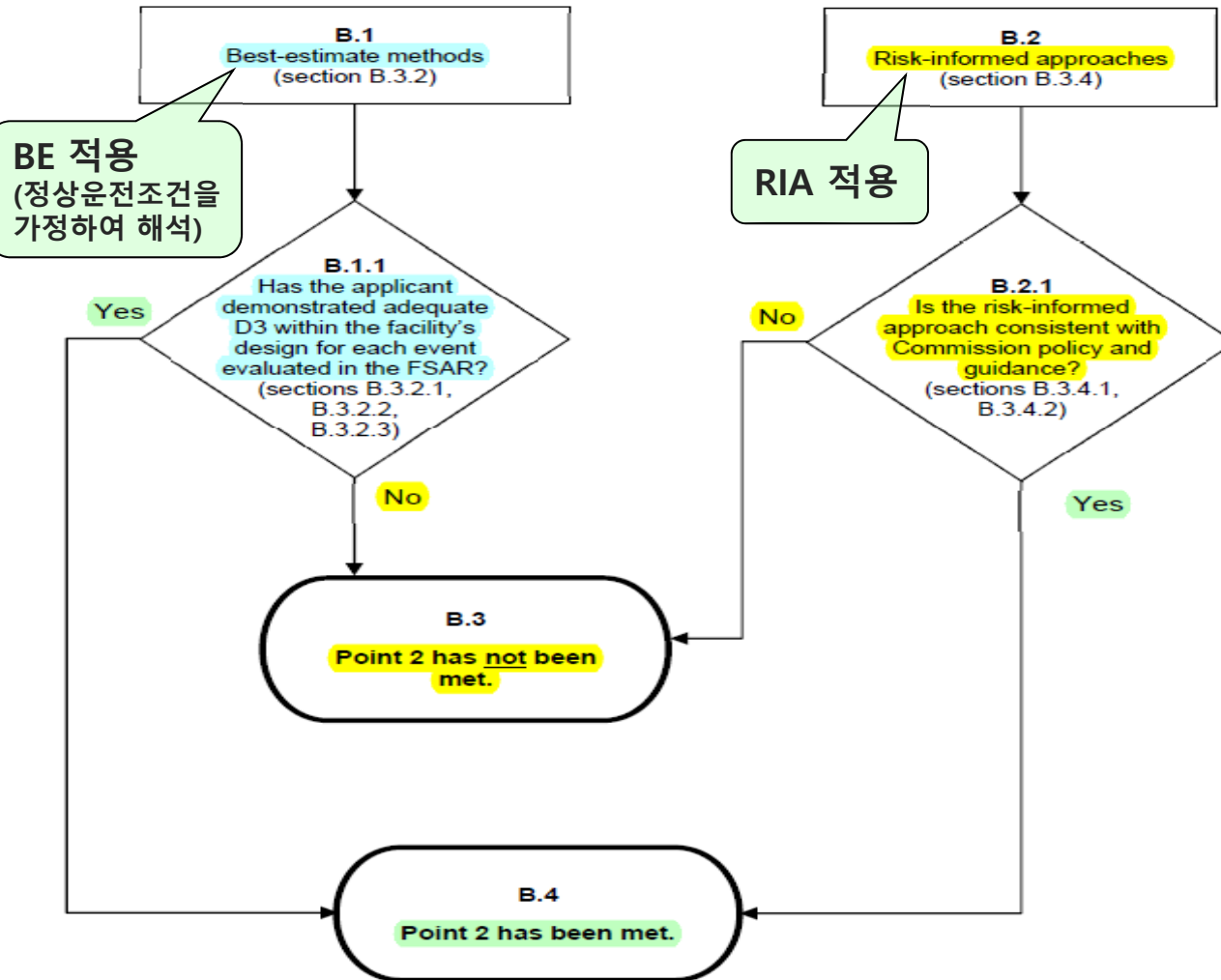
Point 1 요건:
D3 상세-평가의
필요-여부를 판단



III. BTP 7-19, Rev.9의 CCF/D3 요건 및 대응

Point 2 요건:
D3 상세-평가 수행

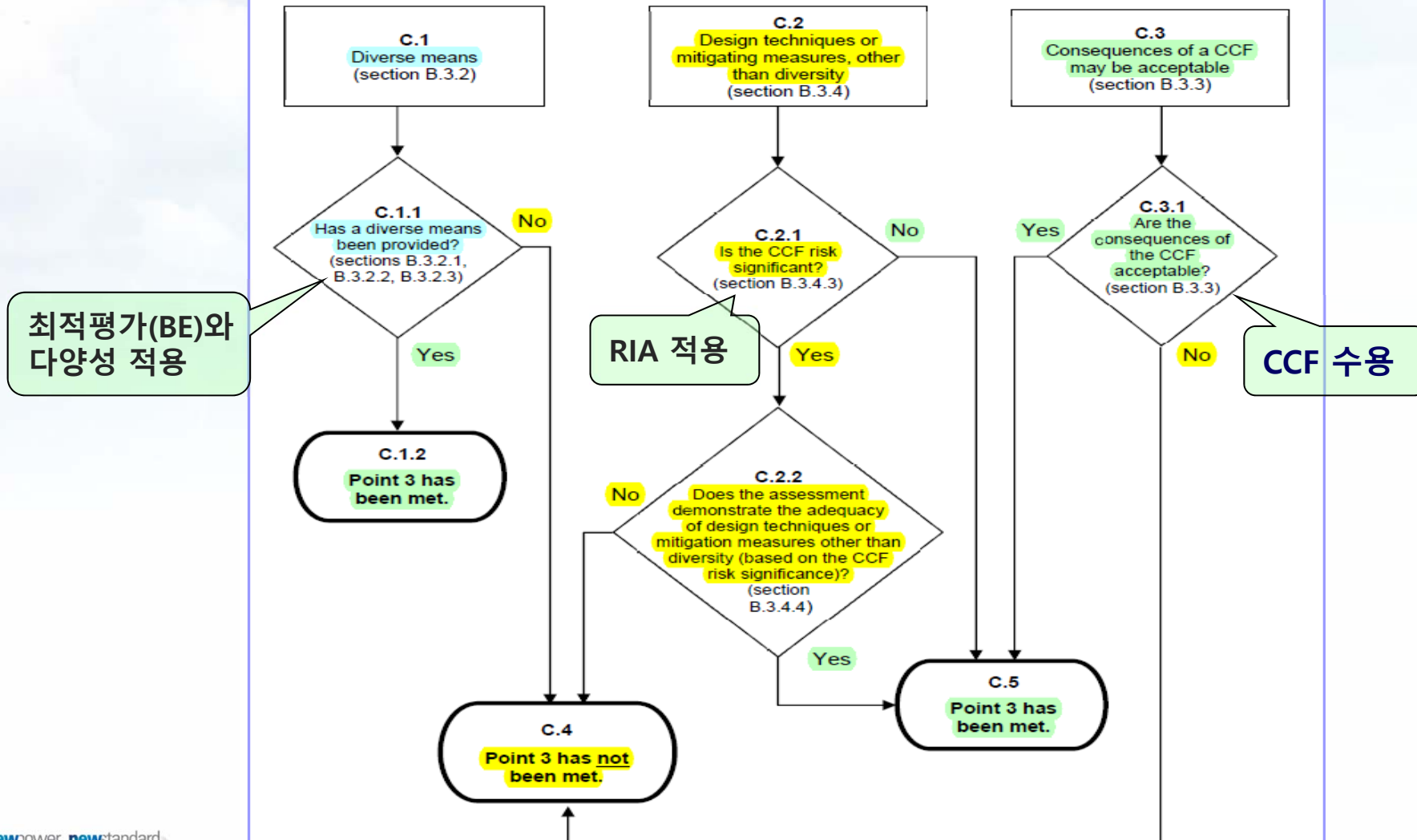
B. POINT 2—DETAILED D3 ASSESSMENT



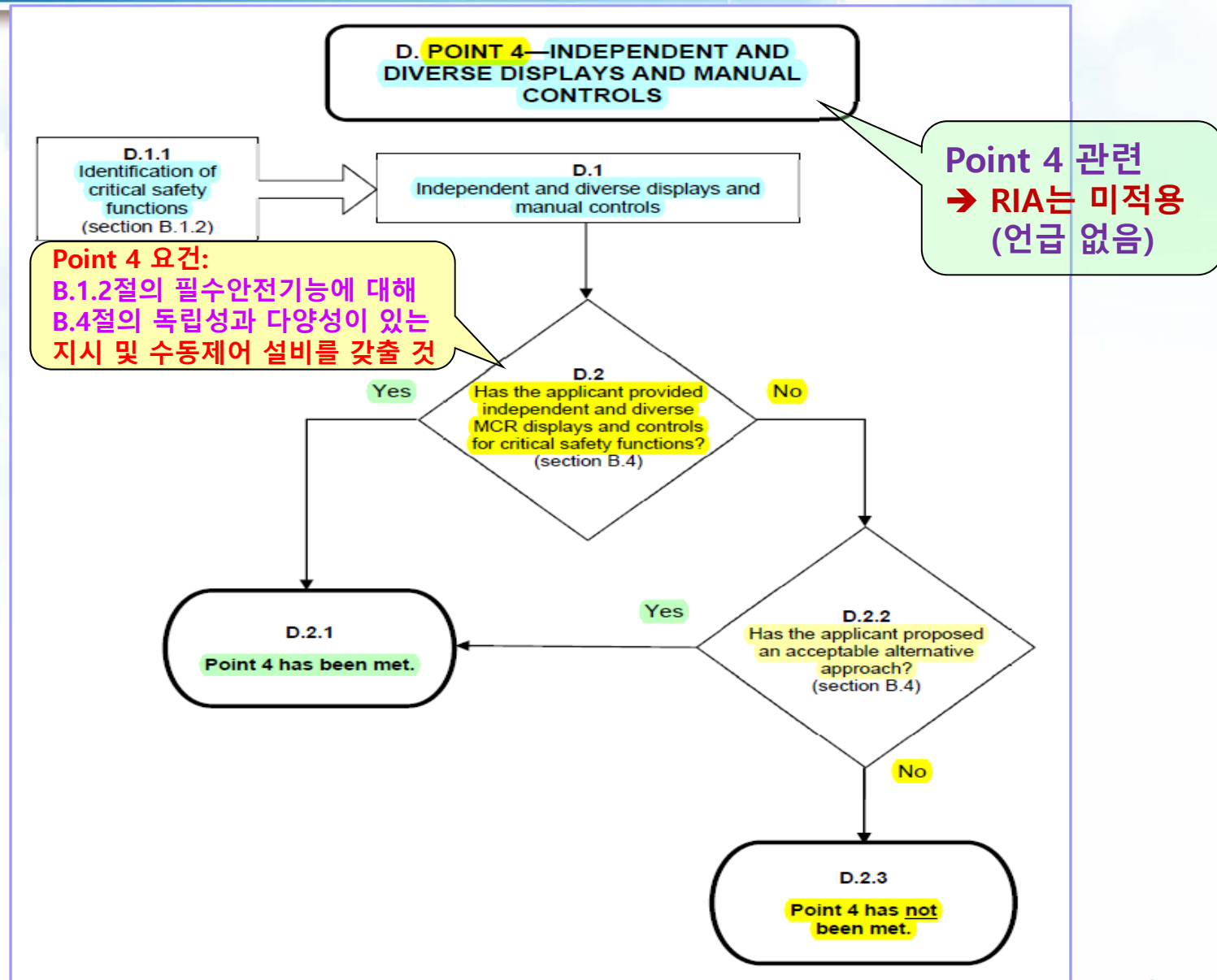
III. BTP 7-19, Rev.9의 CCF/D3 요건 및 대응

Point 3 요건:
각 CCF 결과에 대해
대응/감축/수용여부를 결정

C. POINT 3—ADDRESSING, MITIGATING, OR
ACCEPTING THE CONSEQUENCES OF EACH
CCF



III. BTP 7-19, Rev.9의 CCF/D3 요건 및 대응



IV. CCF/D3 요건의 변화추세 및 설계

❖ CCF/D3 평가 및 대응 위한 접근방법의 변화 추세

- 1) CCF 대응-주안점: Diverse I&C로 CCF 감축 → 안전계통 내부에서 CCF 제거
→ SRM-SECY-22-0076 → BTP 7-19, Rev.9 → CCF 제거 관련 RIA 평가를 도입
- 2) 다양성 I&C 설비(DPS/DIS/DMA SW)의 공급: 기본 설비 → 평가 후 필요하면 공급
→ P1: D3 평가 → CCF 취약성 확인 → RIA 적용 → SSC 변경-여부 결정
- 3) D3 평가/분석/구현 요건-변화: 결정론적 접근 → RIA를 선택적 적용 가능 (P4는 예외)
 - RIA를 D3 방법으로 공인하여 추가 → 설계자와 Utility의 선택-범위가 확장됨
 - 2000년대에 연구된 위험도정보-성능기반규제(RI-PBR)가 D3 요건에 일부 반영됨
 - RIA는 결정론적-규제에서 → 위험도-정보 규제로 변화를 반영 (RI-PBR의 RI 구현)
(규제-입장: CDF/LERF 관련 안전성을 확보한다면 → 규제 방식은 확장성 가능)
 - D3 평가 시 정성적-평가 대상을 명시 → [저/최저-안전 중요도 SSC]에 적용
- 3) 설계 반영 → 호기 별 계약-요건을 적용 → i-SMR 경우 (필요 시) RIA 적용을 고려
 - RIA 적용사례: NuScale → ATWS 관련 설비는 면제됨 (안전계통 내부에 충분한 다양성을 갖춰서 CCF 제거한 점 외에도, ATWS 상황을 고려한 PRA 결과를 제시)

V. 후속연구 및 Q&A

❖ 후속연구 필요

- [합리적인 수준으로] 안전등급 **디지털 I&C 계통의 내부-다양성을 구축**
- [RIA가 제한되는] 다양성 지시/수동제어 관련 **최적화된 P4 요건 구현**
- [디지털 I&C 설비 D3 요건 만족을 위해] 설계 **적용 가능한 RIA 방법**

❖ Q&A

문의: ygoh@kepco-enc.com (오양균)

❖ 소감

You've got to find what you love.

- Steve Jobs' 2005 Stanford Commencement Address -