

Evaluation Procedures of Measures to Eliminate Further Consideration of Digital CCFs of NPP

Y. M. Kim and S. B. Park

Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338

Evaluation Procedures of Measures to Eliminate Further Consideration of Digital CCFs of NPP

2020. 12. 16 ~ 18

원자력안전연구원
김영미

KINS 한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY

개요

- 배경 및 필요성**
 - 미국 원자력 산업계에서는 원전에 최신 디지털 기술의 채택이 느린 주된 이유 중의 하나가 디지털 I&C S/W 공통원인고장(CCF)에 대한 현 미국 NRC의 규제 입장임을 제시
 - 미국 NRC에서는 2016년부터 IAP(Integrated Action Plan)을 통해 디지털 I&C 계통 CCF 대처와 관련된 기술적 규제 입장을 개선하기 위한 활동을 수행 중
- 현 디지털 CCF 규제 입장에 대한 미국 원자력 산업계의 의견**
 - 규제 입장이 너무 모호하고 복잡함
 - 디지털 업그레이드 시 상세한 규제 지침 부족함
 - Screening Criteria가 적용의 어려움 제시
 - 차등적 접근 방식의 요구
 - 리스크 정보 기반의, 결과 기반의 규제 인프라를 요구

Digital I&C CCF 규제 요건

- KINS/GE-N001, 경수로형 원전 안전심사지침**
 - 부록 7-16 디지털 컴퓨터 기반 계측제어계통의 심층방어 및 다양성 평가지침

- 공통원인고장에 따른 취약성들이 적절히 다루어졌는지를 입증하기 위한 심층방어 및 다양성을 평가
- 안전성분석보고서의 사고해석 절에서 평가된 각 사건에 대해서 최적평가기법(BE 기법; 현실적인 가정사항들을 이용한 기법)으로 각 가상된 공통원인고장을 분석
- 가상 CCF로 안전기능이 상실될 수 있다면, 고장으로 영향을 받지 않는 다양한 수단으로 안전계통의 기능을 수행하도록 하여야 함. 각 사고분석에서 필요한 기능을 수행할 수 있는 성능이 입증된다면, 비안전계통에서 다양성 기능이 수행될 수 있음
- 안전필수 기능을 수동으로 계통수준에서 수동 작동시킬 수 있어야 함. 상기 1~3에서 확인된 안전계통과 독립적이고 다양성을 가진, 계통 수준 수동 동작을 위한 지시와 제어가 주재어실에 제공되어야 함

NRC Digital I&C CCF 규제 개선 노력

- NRC Integrated Action Plan to Modernize Digital I&C**
 - MP #1 – Protection Against Common Cause Failures**
 - MP 1A:** 낮은 안전중요도(리스크)를 가지는 디지털 I&C 계통의 설비 교체, 수정 시 적용 가능한 지침 개발
 - Supplement 1 to RIS 2002-22 (2018.5)
 - Key words: sufficiently low likelihood of failure, likelihood of CCF failure, qualitative assessment
 - MP 1B:** 디지털 I&C 기술평가를 위한 NEI 16-16 지침 평가
 - Key words: defensive design measures, CCF likelihood, scope of D3 assessments of potential CCFs
 - MP 1C:** 현 NRC의 디지털 I&C CCF에 대한 입장 평가
 - SECY-18-0090 발간 완료 (2018.9)
 - Key words: five guiding principles
 - MP 1D:** BTP 7-19 개정
 - BTP 7-19, rev.8 draft (2019.8)
 - Key words: graded approach, qualitative assessment, defensive measure

NRC Digital I&C CCF 규제입장 명확화

- SECY 93-087과 SECY 08-0090**

SECY 93-087	SECY 08-0090
<ul style="list-style-type: none"> 4 Point Position <ul style="list-style-type: none"> P1: I&C 계통의 DID 평가 수행 P2: 가상의 CCF와 15장 SAR 사고에 대해 최적추정방법을 이용한 평가 P3: 필요시 다양성 수단 제공 P4: MCR에서 수동, 계통 수준의 작동을 위한 한 세트의 지시와 제어가 제공 	<ul style="list-style-type: none"> 5 Guiding Principles <ul style="list-style-type: none"> Graded approach 사용 가능 최적추정방법 혹은 설계기준분석(전통적 방식) 사용 가능 자동/수동 수단 모두 허용 필수안전기능 관리 제시된 안전계통 CCF와 관련이 없다면, D3의 다양성 수단으로 신뢰 가능

차등적 접근을 위한 안전중요도의 분류 및 평가

- 안전중요도에 따른 디지털 I&C 설비의 분류**

분류	구분	설명	예시
H (높은)	높은 안전중요도를 가지는 설비	발전소의 안전성에 주요한 기능을 하는 안전 계통 설비 (리스크정보기반) 안전성 측면에서 중요도가 높은 기능을 수행하는 설비	RSC1 설비 (보수시 설비)
	낮은 안전중요도를 가지는 설비	발전소의 안전성에 주요한 기능을 하는 안전 계통 설비 (리스크정보기반) 안전성 측면에서 중요도가 낮은 기능을 수행하는 설비	RSC2 설비 (보수시 설비)
M (중간)	높은 안전중요도를 가지는 설비	발전소의 안전성에 주요한 기능을 하는 안전 계통 설비 (리스크정보기반) 안전성 측면에서 중요도가 높은 기능을 수행하는 설비	RSC3 설비 (보수시 설비)
	낮은 안전중요도를 가지는 설비	발전소의 안전성에 주요한 기능을 하는 안전 계통 설비 (리스크정보기반) 안전성 측면에서 중요도가 낮은 기능을 수행하는 설비	RSC4 설비 (보수시 설비)
L (낮은)	비안전 설비	M-설비에 포함되지 않는 비안전 설비	RSC5 설비 (보수시 설비)

차등적 접근을 위한 안전중요도의 분류 및 평가

- 디지털 CCF 차등적 접근방안 분석**

- 높은 안전중요도를 가지는 H 설비의 CCF 대처 방안**
 - CCF 제거를 위한 수단 평가
 - CCF 대처 수단 평가
 - 설계기준분석 혹은 최적추정분석
 - 설계 특성 및 방어수단을 추가한 재설계의 절차로 수행
- 낮은 안전중요도를 가지는 설비의 CCF 대처 방안**
 - M 설비 → 정성적 평가 수행
 - L 설비
 - 통합된 설계 기능, 자원의 공유, 다른 계통-기기와 네트워크 연결로 인해 분석되지 않은 조건을 야기할 수 있는 가능성이 있는 경우 정성적 평가를 수행
 - 정성적 평가를 수행하지 않을 경우 근거에 대한 문서화

디지털 CCF 추가고려 배제를 위한 수단 평가 절차

- 디지털 계측제어 및 전력설비 CCF의 기술적 평가 절차 개발**

- 충분한 다양성 평가**
 - 안전기능 식별 및 다양성 설계 확인
 - 다양성 속성 확인
 - 공통/공유자원 여부 확인
 - 요구되는 다양성 기능의 운영 가능성 확인
 - 주기적 감시기준 및 운영기술지침서와의 일관성 유지 확인
- 충분한 시험성 평가**
 - 단순성 평가
 - 운영환경 평가
 - 필수 시험항목의 수행
 - 모든 입력 조건에 대한 출력 시험 수행
 - 모든 타이밍 순서에 대한 입출력 시험 수행
 - 이전 데이터의 상태에 대한 입출력 시험 수행 (메모리 포함 시)
 - 사용하지 않는 로직(회로)의 처리
- 충분한 방어수단 평가**
 - 위험요소의 식별
 - 방어수단들의 적용을 고려한 해당 디지털 계통 및 기기의 취약성이나 위험 식별
 - 방어수단들에 대한 선별 및 적용
 - 식별된 취약점이나 위험을 다루기 위해 보증되는 방어수단들에 대한 설명 제시
 - 방어수단들의 동작원리 이해
 - 제안된 방어수단들의 검증 및 평가
 - 방어수단들의 제원 및 성능이 제시
 - 해당 디지털 계통 및 기기에서 식별된 취약점이나 위험을 예방 및 제한하기 위해 적용된 방어수단들이 허용 가능한 이유에 대한 기술적인 기준 제시
 - 적용된 방어수단들의 효과가 어떻게 검증될 수 있는지에 대한 분석 제시
 - 다른 위험요인에 대한 평가
 - CCF로 인해 나타날 수 있는 다른 잠재 위험요인(residual risk)에 대한 평가 수행

차등적 접근을 위한 안전중요도의 분류 및 평가

- 디지털 계측제어 및 전력설비 CCF의 기술적 평가 절차 개발**

국내 Digital I&C CCF 심사지침(안) 제안

- CCF 분석 대상의 확대**
 - 디지털 기반의 안전등급 보조지원설비, 기타보조설비
 - 공통원인고장 발생 시 발전소 운전에도 영향을 미칠 수 있는 디지털 비안전설비 포함
- 안전중요도에 따른 차등적 접근**
 - 설비의 안전중요도 분류 및 안전 중요도에 비례하는 D3 평가 요건 제시
- 추가적 방어수단의 신뢰**
 - 예상되는 CCF에 대한 예방수단, 제한수단 등의 방어수단 적용여부에 대한 평가 결과 활용
- 정성적 평가의 활용**
 - 안전중요도가 낮은 설비에 대한 정성적 평가 결과 신뢰
- 오동작(Spurious Operation) 평가**
 - CCF에 기인한 분석되지 않은 오동작 식별 및 발전소 영향 평가

국내 Digital I&C CCF 심사지침(안) 제안

- 디지털 계측제어 및 전력설비 CCF 평가 심사지침 개발**

- 특징**
 - 충분한 내부 다양성과 충분한 시험성에 대한 명확화
 - 방어수단의 사용 기준 추가
 - 안전중요도에 따라 차등적으로 CCF 평가를 수행
- 전문가 의견 수렴**
 - 차등적 CCF 접근 방안의 필요성
 - 차등적 CCF 접근 방안의 적절성
 - 안전등급 분류 방법
 - 정성적 평가 방법의 사용
 - 충분한 시험성 및 방어수단 사용에 대한 의견 등
 - 대표적 수렴 의견

원자력 안전 KINS가 만들어 갑니다!

감사합니다

KINS 한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY

글로벌 원자력안전의 중심

KINS 한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY