Cyber Security Regulation in Nuclear Power Plants through Vital Digital Assets

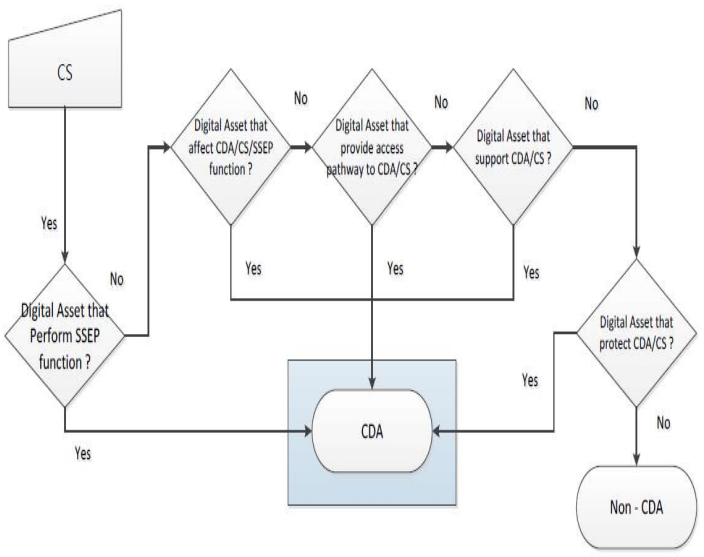
김승민, 권국희 / 이상 한국원자력통제기술원(KINAC)

본 논문은 원자력시설 내 초기사건(Initiating Event) 발생 이후 완화 실패에 의해 노심 손상(Core Damage)을 유발할 수 있는 핵심디지털자산에 대한 식별 방법론을 제시하였으며, 식별된 핵심디지털자산에 대한 사이버보안 규제방안을 제시하였다. 핵심디지털자산 식별은 크게 초기사건 및 예비초기사건을 유발할 수 있는 디지털자산에 대한 식별, 사고 완화를 위한 사고완화설비 작동에 영향을 줄 수 있는 디지털자산에 대한 식별로 나뉜다. 식별된 핵심디지털자산에 대한 사이버보안 규제로는 기존 사이버보안 보안조치의 강화, 취약점 분석을 통한 새로운 보안조치 적용, 강화된 심층방호전략 구축 등 이 있다. 본 논문에서 제시한 핵심디지털자산 식별 방법론과 새로운 규제방안을 통해 사이버공격에 의해 발생할 수 있는 노심 손상과 같은 중대사고를 예방할 수 있을 것으로 기대된다.

■ 배경

✓ **원자력시설에 대한 사이버공격 증가**

최근 원자력시설의 계측제어기기가 아날로그에서 디지털로 바뀜에 따라 사이버보안 이슈가 대두되고 있으며, 원자력시설을 대상으로 한 사이버공격 사례가 증가하고 있다. 한국원자력통제기술원은 “원자력시설 등의 컴퓨터 및 정보시스템 보안 기술기준”(KINAC/RS-015)에 따라, 원자력시설의 안전(Safety-related 및 Important-to-Safety), 보안(Security),비상대응(Emergency Preparedness) 기능 수행 및 침해시 해당 기능에 악영향을 줄 수 있는 디지털기기를 “필수디지털자산(Critical Digital Asset, CDA)”으로 식별하도록 요구하고 있으며, 적절한 보안조치를 적용하도록 규제하고 있다.



[필수디지털자산 식별 프로세스]

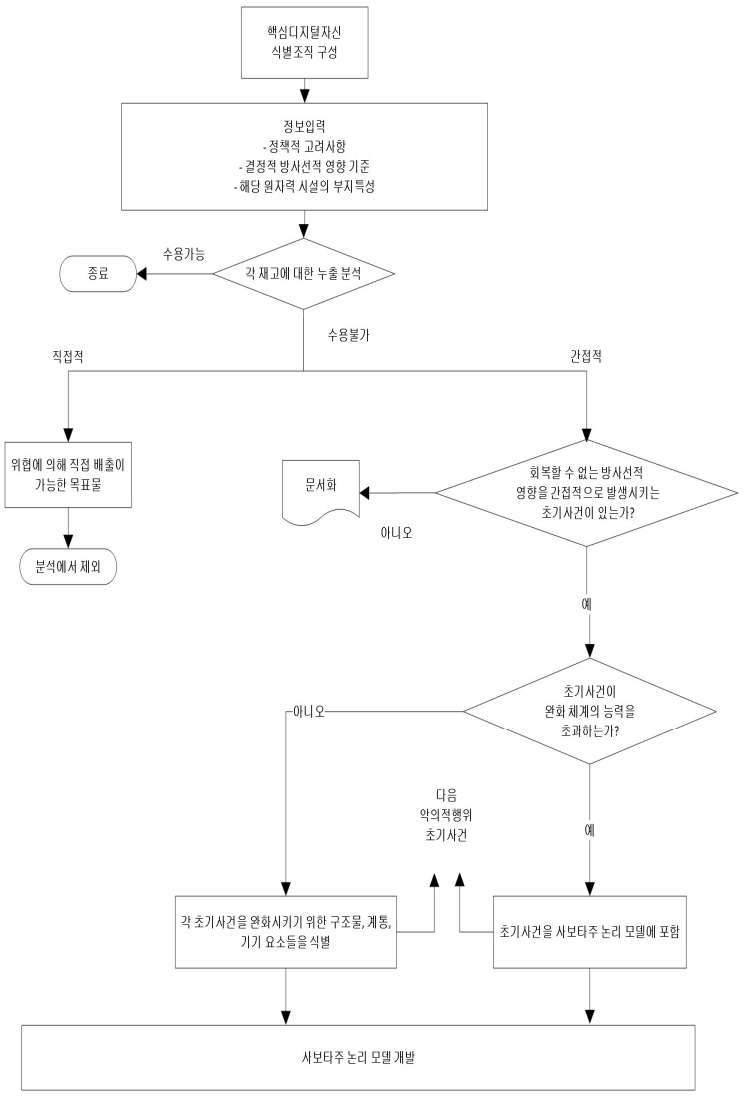
✓ **핵심디지털자산 식별 및 규제 필요성**

원자력시설 내 필수디지털자산은 디지털자산의 약 70%에 해당하며, 동일한 보안조치를 적용하기에는 경제적, 관리적으로 비효율적이다. 이를 위해, 사이버공격에 의해 악영향을 받을 시 원전의 노심손상(Core Damage) 를 유발할 수 있는 디지털자산인 핵심디지털자산에 대한 식별 방법론과 식별된 핵심디지털자산에 대한 규제방안을 제시함을 목적으로 한다.

■ 핵심디지털자산 식별을 위한 사보타주 논리 모델

✓ **핵심디지털자산 사보타주 논리 모델 개발 프로세스**

1. 핵심디지털자산 식별 조직 구성
2. 핵심디지털자산 식별을 위한 정보 수집 (정책적 고려사항, 부지특성, 확률론적안전성 분석 결과, 설계특성 등)
3. 방사능 재고 누출 분석 수용 여부 결정
4. 회복할 수 없는 방사선적 영향을 간접적으로 발생시키는 초기사건의 유무 판단
5. 초기사건의 완화 체계능력 초과 여부 판단
6. 초기사건을 완화시키기 위한 구조물, 계통, 기기요소 식별
7. 위협이 사보타주 사건을 수행할 능력 유무 판단
8. 확률론적안전성분석 기법을 통한 사보타주 논리 모델 개발
9. 논리모델에서 사건을 디지털자산으로 대체 하여 디지털 사보타주 논리모델 개발
10. 공격목표집합 및 핵심디지털자산 후보군 식별



[사보타주논리 모델 개발 프로세스]

■ 핵심디지털자산 식별을 위한 사보타주 논리 모델

✓ **기존 보안조치 보완**

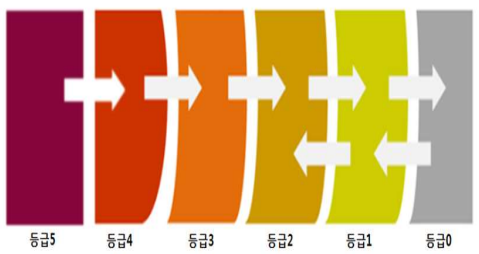
- RS-015 101가지 보안조치에 대해 새로운 기술적 보안조치 적용 혹은 더 강화된 운영적, 관리적 보안조치 적용

✓ **취약점 분석을 통한 새로운 보안조치 적용**

- 침투테스트 및 보안성 평가를 통해 취약점을 도출하고, 도출된 취약점에 대하여 새로운 보안조치 적용

✓ **강화된 심층방호전략 구축**

- 기존 4등급이 최고인 심층방호구조를 1단계 더 강화하여 핵심디지털자산에 해당하는 자산을 가장 높은 등급 5등급에 배치하여 강화된 심층방호전략 구축



[강화된 심층방호전략 구조 예시]

■ 기대 효과 및 향후 연구 목표

✓ **원자력시설 사이버보안 심·검사 규제이행에 활용**

- 핵심디지털자산에 대한 사이버보안 이행에 대한 심사 및 검사 이행에 활용
- 개발된 검증방안을 통해 현장 심·검사 규제이행 시 도출된 현안에 대한 규제기술 검증에 활용