기타 원자력시설의 필수디지털자산 식별 현황과 그에 대한 검사 결과 고찰

김시원*, 김현두
한국원자력통제기술원, 대전광역시 유성구 유성대로 1534
*swkim@kinac.re.kr

1. 서론

원자력시설의 주요 시스템들이 디지털로 변화해감에 따라, 독일 그룬트레밍엔 원전 내 일부 단말 컴퓨터가 악성코드에 감염된 사례와 같이 원자력시설에서도 사이버위협의 가능성이 점차 높아지고 있는 상황이다[1]. 사이버위협으로부터 원자력시설을 보호하기 위해 국내에서는 관련 지침에 따라 사업자가 사이버보안계획을 작성하고 이를 7단계로 나누어 단계별로 이행하고 있다.

이러한 사이버보안계획의 2단계로 사이버위협으로부터의 보호 대상이 되는 필수디지털자산을 식별하여야 하며, 사업자의 식별 결과에 대한 적정성 확인을 위해 한국원자력통제기술원(KINAC)에서는 사이버보안계획 2단계 특별검사를 수행하였다. 그 과정에서 몇 가지 문제가 도출되었고, 본 논문에서는 이에 대해 고찰해보고자 한다.

2. 필수디지털자산 식별 절차 및 현황

2.1 필수디지털자산 식별 절차

KINAC/RS-019에 따르면, 필수디지털자산을 식별하기 위하여 사업자는 우선 필수시스템을 식별하여야 한다. 이러한 필수시스템은 반드시 디지털 시스템일 필요는 없으며, 원자력시설의 SSEP (Safety, Security, and Emergency Preparedness) 기능에 악영향을 미치는지의 여부 등을 통해서 식별된다. 구체적으로는 SSEP 기능을 수행하는 시스템 혹은 필수시스템에 악영향을 미칠 수 있는 시스템을 말하며, 필수시스템으로의 접근경로를 제공하거나 필수시스템을 지원하는 시스템도 포함한다[2].

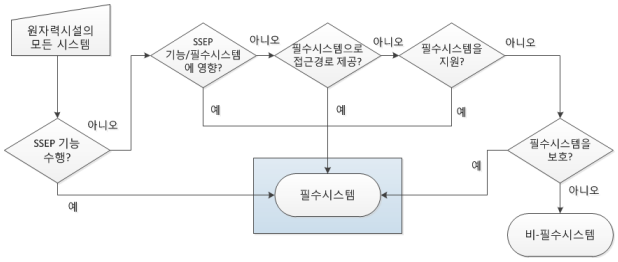

Fig. 1. Process for identifying critical systems.

필수시스템을 식별한 후, 사업자는 필수시스템 내부의 어떤 자산들이 필수디지털자산에 포함되는지 식별하게 된다. 먼저, SSEP 기능을 수행하거나 SSEP 기능에 악영향을 줄 수 있는 디지털자산을 필수디지털자산으로 식별하며, 필수시스템 또는 필수디지털자산에 악영향을 줄 수 있거나, 접근경로를 제공하는 디지털자산도 필수디지털자산에 포함된다[2].

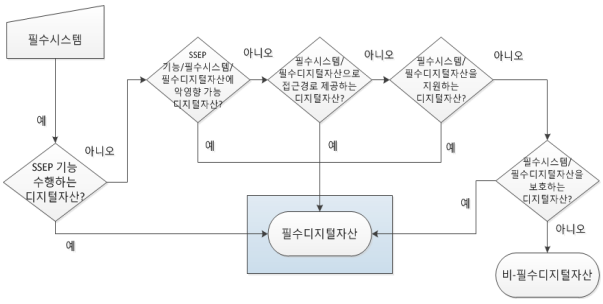

Fig. 2. Process for identifying critical digital assets.

2.2 필수디지털자산 식별 현황

위의 필수디지털자산 식별 절차에 따라 기타 원자력시설 사업자는 필수디지털자산을 식별하였으며, 그 결과를 KINAC으로 제출하였다. 원전과 연구로를 제외한 기타 원자력시설 5개에서 총 78개의 필수시스템이 식별되었으며, 그 중에서 32개의 필수시스템이 내부에 필수디지털자산을 보유하고 있는 것으로 확인되었다. 해당 시스템 내부의 전체 자산 중에서 총 584개의 필수디지털자산이 식별되었으며, 필수디지털자산의 종류는 총 128개였다.

3. 특별검사에서 도출된 문제점 고찰

KINAC에서는 사이버보안계획 2단계 특별검사를 통해 위의 필수디지털자산 식별 절차에 따라 수행된 사업자별 식별 결과의 적정성을 확인하였다. 이러한 검사 과정에서 몇 가지 문제들이 발견되어 이에 대해 공유하고, 규제 측면에서 어떠한 개선 요구사항이 있는지에 대해서 서술해보도록 하겠다.

3.1 필수디지털자산 추가 식별 절차 부재

위의 필수디지털자산 식별 현황에 따르면, 상당수의 필수시스템은 디지털자산을 포함하고 있지 않아 필수디지털자산 식별 절차를 적용할 필요가 없었다. 하지만, 향후에 이러한 시스템이 설비 개선 등을 통해 디지털화된다면 추가로 필수디지털자산 식별이 필요하므로, 이를 위한 절차 수립이 필요하다. 이와 더불어, 향후에 추가적인 시스템이나 설비가 도입되는 경우에도 마찬가지로 필수디지털자산을 추가 식별하는 절차가 요구된다.

3.2 검사 이후 식별 결과에 대한 검토의견 발생

검사가 종료된 이후 검사 결과에 대한 보고서를 작성하는 과정에서 필수디지털자산 식별 결과에 대한 검토의견이 추가로 발생한 사례가 있었는데, 필수시스템 내부의 자산 중 디지털인 자산을 비디지털로 잘못 기술하여 필수디지털자산에서 제외되었다가 해당 자산을 디지털로 변경하고 필수디지털자산으로 재선정한 경우였다. 향후 원전에서의 식별 작업 시에 이러한 오류가 발생할 가능성이 더 많아질 것이라고 판단되며, 이러한 문제가 검사 기간 내에 최대한 걸러지도록 하기 위해 현재 수행 중인 시설별 검사팀 내부의 상호 검토 외에 별도의 팀에 의한 2차 검토 등과 같은 추가적인 검토 절차를 마련하는 것에 대한 고민이 필요하다.

3.3 필수디지털자산 관련 효율적 관리방안 부재

기타 원자력시설 전체의 필수디지털자산은 총 584개이며, 원전에서는 그보다 훨씬 많은 수의 필수디지털자산이 식별될 것으로 예상된다. 이로 인해 필수디지털자산을 식별하는 과정에서 많은 수의 관련된 문서나 근거자료 등이 제출되어 자료 보관 및 문서화 작업 등 관리에 어려움이 있었다. 또한, 식별 이후 각 시설에서 필수디지털자산을 검사하고 관리하기 위해 많은 행정 소요가 예상된다. 이러한 문제를 해결하기 위해, 문서나 작업 등에 대해 시스템별로 관리할 것인지 아니면 자산별로 관리할 것인지에 대한 기준을 선정하는 등 효율적인 관리 방안을 마련하는 것이 필요하다.

3.4 많은 검사 자원 소모

미국원자력협회(NEI)에서는 원전 한 호기당 1천여개의 필수디지털자산을 식별했다고 발표했으며 [3], 국내에서도 비슷한 숫자의 필수디지털자산이 식별된다고 가정한다면, 원전 한 호기의 필수디지털자산은 기타 원자력시설 전체 대비 2배 정도의 규모가 예상된다. 기타 원자력시설 2단계 검사에서 총 4 MM의 자원이 투입되었는데, 이의 2배인 8 MM가 원전 한 호기에 필요하다면, 원전 26개 호기에 총 208 MM의 자원이 요구된다. 이러한 많은 자원을 정해진 검사 기한 내에 투입하는 것은 쉽지 않을 것으로 판단되며, 이에 투입되는 자원을 줄일 수 있도록 검사 효율화 방안을 마련하는 것이 요구된다.

4. 결론

사이버 위협의 대상이 되는 시스템들을 보호하기 위해 KINAC에서는 사이버보안계획 2단계 특별검사를 통해 각 시설에서 정확히 보호 대상을 식별했는지 확인하였다. 본 논문에서는 이러한 검사 과정을 통해 확인된 규제 측면에서의 몇 가지 문제들을 정리하고 앞으로의 개선 방향을 제시하였다. 향후 연구에서는 이러한 문제들에 대한 구체적인 개선방안 및 절차를 마련하고 이를 적용한 결과에 대해 분석할 계획이다.

5. 참고문헌

[1] 연합뉴스, "독일 바이에른주 원전 IT 악성코드 감염으로 가동 중단", 2016.4.

[2] 한국원자력통제기술원, "원자력시설등의 필수디지털자산 식별 기술기준", KINAC/RS-019, 2015.

[3] William Gross, "NEI 13-10 - Overview, Results, and Need for Consistency", NEI Cyber Security Implementation Workshop, 2016.