원전 통신망 사이버보안 체계 연구

최영수*°,최유락, 이재철, 조재완, 구인수, 홍석붕

*°한국원자력연구원

Study on the Construction of Cyber Security for the Nuclear Power Plants

Choi, Young Soo, Choi, Yu Rak, Lee, Jai Chul, Cho Jai Wan, Ku, In Soo, Hong, Seok Boong

Korea Atomic Energy Research Institute

E-mail : yschoi1@kaeri.re.kr

요 약

원전 계측제어 시스템의 디지털화에 따라 개방형 시스템의 사용이 늘어나고 있으며, 개방형 시스템의 사용으로 인해 보안 취약성이 늘어나 통신망을 통한 해킹의 위험이 증가되고 있다. 원전은 다른 산업에 비해 경제, 사회적 영향이 크므로 원전의 운영중단 및 파손을 방지하기 위한 대책을 철저히 마련하여야 한다. 원전 통신망 사이버 보안을 위해서는 보안 환경의 정확한 분석을 통해 대책을 세우는 것이 필요하다. 사이버 보안에 대한 전체적인 틀은 보안정책의 수립, 보안 위험을 최소화하기 위한 인력, 장비 및 기술을 포함한 사이버 보안 기술의 구현, 그리고 지속적인 보안 감시 및 관리가 필요하다. 본 논문에서는 원전 통신망 사이버 보안 체계 구축을 위한 방법을 제안한다.

1. 서론

원전은 우리나라의 주요 에너지원으로 국가적인 차원의 기간시설 보호 대책이 요구된다. 과거 개인 및 사무망에 제한되었던 사이버 보안 문제가 최근 들어 원전 계측제어 시스템 같은 계측 제어 망에도 위협을 가하고 있다. 사이버 공격에 의해 원전 계측제어 시스템의 조작이 발생되면 원전의 운영중단 및 파손 등의 심각한 사태를 초래할 수 있다.

지금까지 원전 계측제어 시스템은 전용 통신망의 사용, 고유의 운영체제 사용 등으로 인하여 사이버 위협에 안전하다고 여겨져 왔다. 하지만 계측제어 시스템의 개방화·표준화에 의해 사이버보안 취약성이 증가하고 있으며, 최근 국외에서 수집된 사이버 침해사례를 보면 더 이상 해킹·사이버테러 등의 사이버 위협에 안전할 수 없다.

본 연구는 지경부 원전기술혁신사업의 연구비지원에 의하여 연구되었음

2. 본론

사이버 공간을 통한 공격 경로 및 방법들이 다양해지고 사용자의 사이버 환경이 변화하므로 사이버 보안 취약성을 완벽하게 제거할 수는 없다. 원전 사이버 보안을 위해서는 원전 사이버 환경의 정확한 분석을 통해 대책을 세우는 것이 필요하다. 사이버 보안에 대한 전체적인 틀은 보안정책의 수립, 보안 위험을 최소화하기 위한 사이버 보안 기술의 구현, 그리고 지속적인 보안 감사 및 관리가 필요하다.

본 논문에서는 보안체계 수립을 위한 설계 및 운영을 통한 검증모델을 제시하였다. 보안체계 설계 단계에서는 보안체계 요구사항, 보안정책 요구사항, 보안정책 설계, 보안모듈 요구사항, 보안모듈 설계의 순으로 보안 방안을 수립하고, 보안 검증 단계에서는 운영 및 감사를 통해 분석, 검증을 수행하도록 하였다. 보안 대책은 한 번의 설계 및 운영으로 종결되는 것이 아니므로 지속적인 분석 및

검증을 통해 보안체계를 수정, 보완하여야 한다.

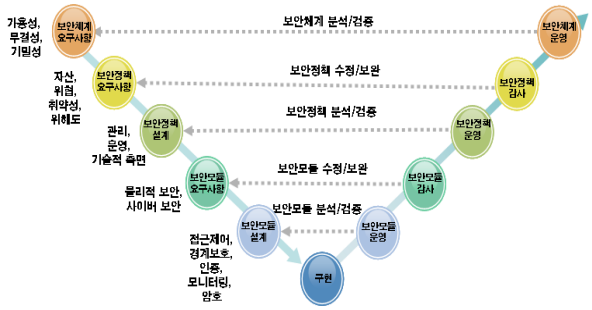

그림 1 보안체계 수립 및 운영 모델

원전의 사이버 보안체계 설계를 위해 자산 분석, 사이버 위협 및 취약성 분석, 위해도 분석, 그리고 대응방안의 과정을 거친다. 원전 사이버 보안 정책 및 모듈 설계의 단계는 다음과 같다.

① 자산 분석 : 자산의 잠재적 손실에 따른 영향을 고려하여 계측제어 시스템과 사무망을 등급화한 자산 모델로 설정한다.
안전망 : 등급 0, 비안전망 : 등급 1, 전용망 및 유지보수망 : 등급 2, 소내망 : 등급 3

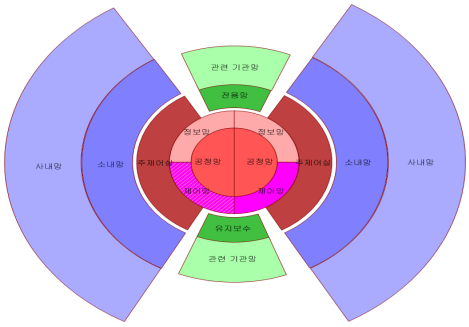

그림 2 원전 통신망 자산

② 위협 식별 : 원전 통신망의 사이버보안 위협원은 범죄조직, 외국 정보국, 해커, 테러리스트, 바이러스 제작자, 내부자 위협 등이 있다.
위협 유형은 통신 방해, 가로채기, 정보의 수정, 조작 등이 있다.

③ 취약성 분석 : 사이버보안 위반을 유발할 수 있는 약점으로 논리적, 물리적 사이버 보안 취약성이 있다. 원전 계측제어 시스템은 사무망과는 독립적인 망으로 구성되어 있으나, 물리적 연결로 인한 사이버 보안 취약성이 발생할 수 있다. 분리된 망의 물리적인 연결을 방지할 수 있는 물리적 보안 방안도 사이버 보안 설계시 중요하게 고려되어야 할 요소이다.

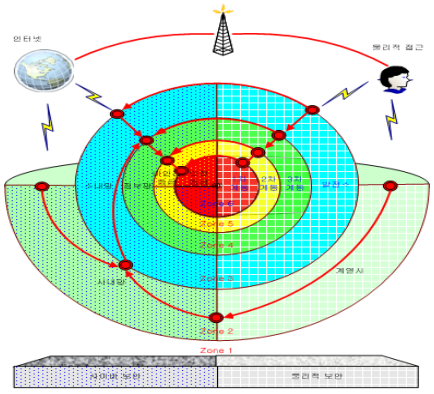

그림 3 공격 경로 및 취약성

④ 위해도 분석 : 위해도를 평가하고 자산 보호를 위한 우선순위를 결정해야 한다. 위해도 평가 단계에서는 자산에 대한 손실이나 손해의 잠재성을 검토한다. 손실이나 손해의 영향, 자산에 대한 위협 및 취약성을 평가함으로써 위해도 정도를 파악한다.

⑤ 대응 방안 : 위험을 줄이거나 제거하기 위한 대응책의 비용 및 장단점을 파악한다. IT 산업에서 개발된 기술을 비교 검토하여 원전 특성에 맞게 적용할 수 있다.

3. 결론

본 논문에서는 원전 사이버 보안체계 수립을 위한 설계 및 운영을 통한 검증모델을 제시하였다. 사이버 보안체계 설계를 위해 자산 분석, 위협 식별, 취약성 분석, 위해도 분석 및 보안 대응방안 과정을 거치며 원전 특성을 고려한 자산의 등급화 및 물리적 사이버보안 취약성을 분석하였다.

[참고문헌]

[1] Critical Infrastructure Protection : Challenges and Efforts to Secure Control Systems, GAO-04-354, 2004

[2] Framework for SCADA Security Policy, D. Kilman, J. Stamp, Tech. Rep. SAND2005-1002C, Sandia National Laboratories, 2005