원전 다양성보호계통 사이버보안 테스트베드 설계

정성민*
*한국원자력연구원
smjung@kaeri.re.kr

The Design of a Cybersecurity Testbed for Diverse Protection System in NPPs

Sungmin Jung*
*Korea Atomic Energy Research Institute

요 약

원자력 발전소의 계측제어시스템에 디지털 관련 기술이 적용되면서 사이버보안 위협이 증가하였고, 이에 따라 사이버보안 위협의 대응은 중요한 현안이 되었다. 하지만, 실제 운영중인 원자력 발전소에 침투 시험은 불가능하기 때문에 테스트베드를 구축 및 활용하여 사이버보안 위협을 분석해야 한다. 계측제어시스템의 비안전계통은 디지털 기반의 제어기기와 통신망이 사용되기 때문에 안전계통보다 많은 사이버보안 취약점이 존재한다. 본 연구에서는 비안전계통인 다양성보호계통을 위한 테스트베드의 구성과 취약점 확인을 위한 공격, 그리고 대처 방안에 대해 논의한다.

1. 서론

원자력 발전소의 계측제어시스템은 보수적인 특성에 따라 아날로그 기술이 일반적으로 사용되었지만, 최근 디지털 기술이 사용되면서 사이버보안 위협이 증가하였다[1]. 사이버보안 위협에 대한 취약점을 확인하기 위해 계측제어시스템을 대상으로 침투 시험이 필요하지만 운영중인 원자력 발전소에서는 잘못된 결과에 대한 위험이 크기 때문에 직접적인 침투 시험은 불가능하다. 따라서 위협을 분석하기 위해 테스트베드를 이용해야 한다. 테스트베드를 통해 사이버보안 공격의 영향을 간접적으로 확인하고 방화벽이나 암호화 장비와 같은 보안 도구들의 적합성을 평가하여야 한다. 테스트베드를 구축하기 위해 안전과 관련 사항, 설치 비용 및 규모, 그리고 시험의 용이성을 고려하여 비안전계통인 다양성보호계통에 대해 테스트베드의 구성과 시험 및 사이버보안 대응 방안에 대해 논의한다.

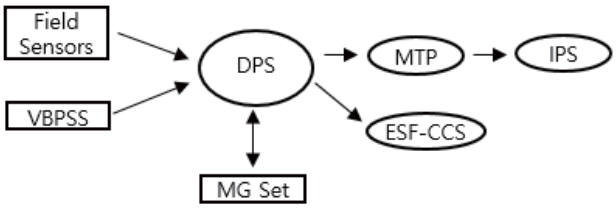
2. 다양성보호계통 테스트베드 구성

원자력 발전소 계측제어시스템은 기능과 규제 등급에 따라 안전계통과 비안전계통으로 나눌 수 있다[2]. 안전계통은 원자력 발전소의 사고를 방지하고 사고 결과를 완화하기 위한 계통이고, 비안전계통은 원자력 발전소 운전을 위해 계측, 감시, 제어 기능을 수행하는 계통이다. 다양성보호계통(DPS, Diverse Protection System)은 비안전계통으로 원자로가 정지되어야 할 조건임에도 정지되지 않는 과도상태의 위험을 줄이기 위해, 원자력 발전소의 상태 정보를 입력 받아 설정치와 비교하여 원자로 정지, 터빈 정지, 그리고 보조급수 작동 기능을 수행한다[3].

다양성보호계통은 디지털 기반의 제어기기와 통신망이 사용되기 때문에 사이버보안 위협에 취약하고, 안전계통인 원자로보호계통(RPS, Reactor Protection System)과 다양성을 위하여 설계된 계통이기 때문에 사이버보안 공격으로 인한 오작동 또는 간단히 조작된 정보의 입력만으로 원자로 정지와 같은 잘못된 결과를 가져올 수 있다. 따라서 다양성보호계통에 대한 사이버보안의 위협을 분석하여 대응 방안을 마련하는 것은 중요하고 침투 시험이 불가능한 원자력 발전소는 테스트베드를 활용하는 것이 최선의 방법이다. 테스트베드를 이용한 침투 시험을 수행하기 위해 먼저 다양성보호계통의 연계 사항을 파악해야 한다. 그리고 취약한 구간을 선정하여 가능한 취약점을 확인하기 위한 시험을 수행하고 분석된 결과를 바탕으로 사이버보안 위협에 대한 대응을 마련해야 한다.

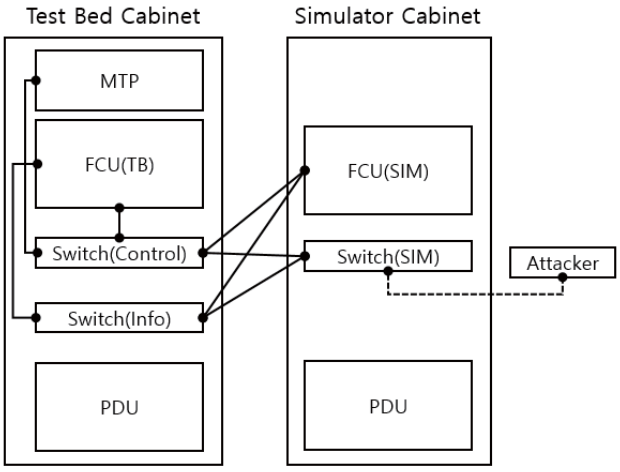
(그림 1)은 다양성보호계통과 다른 계통과의 주요한 연계 사항을 보여준다[4]. 여러 계통과 단방향 또

는 양방향으로 데이터를 송수신 하는데, 일부 구간은 독자적인 통신망이나 아날로그 실배선을 사용하기 때문에 보안상 영향이 거의 없지만 정보처리계통(IPS, Information Processing System)같은 일부 시스템 사이에 디지털 기반의 통신망을 사용하기 때문에 시스템의 취약점이 될 수 있으므로 해당 구간에서 사이버보안 위협을 분석해야 한다.



(그림 1) 다양성보호계통 주요 연계 사항

(그림 2)는 다양성보호계통의 테스트베드 구성을 보여준다. 테스트베드는 테스트베드 캐비닛과 시뮬레이터 캐비닛으로 구성될 수 있다. 다양성보호계통은 센서 데이터 수집과 공정제어 수행을 위해 비안전 제어기인 FCU(Field Control Unit)를 사용한다. 테스트베드 캐비닛에는 MTP(Maintenance and test panel), FCU(Field Control Unit), PDU(Power Distribution Unit), 그리고 제어망, 정보망을 위한 스위치로 구성된다. 시뮬레이터 캐비닛은 타 계통 및 현장 센서의 입력신호를 모사하기 위한 FCU 와 PDU, 그리고 로깅과 시험을 위한 스위치로 구성된다.



(그림 2) 다양성보호계통 테스트베드 구성안

3. 다양성보호계통 취약점 분석

테스트베드를 통해 예상되는 취약점을 확인하여 다양성보호계통의 사이버보안 위협을 분석할 수 있다.

먼저 테스트베드에서 스위치 장비의 취약점을 확인해야 한다. 테스트베드에 정보망과 제어망을 위한 스위치에 보안 기능이 없거나 기본적인 설정만 적용되어 있는 경우에 취약점이 될 수 있다. 스위치 장비에 대해 MAC 플러딩(Flooding)이나 ICMP 리다이렉트(Redirect) 공격을 확인한다. MAC 플러딩의 경우에 변조된 대량의 ARP relay 패킷을 발생시켜 공격 목표인 정보망 또는 제어망 스위치의 MAC 테이블에 오버플로우(Overflow) 공격을 수행하여 패킷을 강제로 플러딩(Flooding)한다. 이후 스위치의 Fail Open 정책에 따라 허브(Hub)와 같은 방식으로 동작하게 된다. 이 취약점은 네트워크에서 스니핑(Sniffing)이 가능하게 하여 운영과 관련한 패킷 정보가 노출될 수 있다. 또한, ICMP 리다이렉트는 공격 목표 IP 주소를 획득하고 이를 공격자의 IP 주소로 변조된 ICMP 리다이렉트 메시지를 브로드캐스트한다. 이 취약점에 의해 다른 네트워크의 제어기기 사이에 송수신 되는 패킷이 노출될 수 있다.

스위치 장비 이외에 디지털 기반의 통신망을 사용하는 FCU(TB)와 FCU(SIM), MTP 와 FCU(TB), 그리고 MTP 와 FCU(SIM) 구간에서 취약점을 확인해야 한다. 즉, 제어기기와 제어기기 간, 그리고 제어기기와 MTP 사이의 데이터 송수신시 해당 구간에서 ARP 스푸핑(Spoofing)과 스니핑(Sniffing)과 같은 취약점을 확인한다. ARP 스푸핑의 경우에 공격 목표인 FCU 또는 MTP 의 IP 와 MAC 주소를 파악한다. MAC 주소가 변조된 ARP relay 패킷을 지속적으로 네트워크에 브로드캐스트 하면 공격 대상이 되는 FCU 나 MTP 는 변조된 정보를 이용하여 내부의 ARP 캐쉬를 업데이트 한다. 이후 해당 정보는 공격자에게 전송되기 때문에 공격 목표의 송수신 패킷을 가로채거나 중간자(MITM) 공격을 통하여 FCU 제어명령 등이 노출될 수 있다. 그리고, 스니핑의 경우에는 무차별(Promiscuous) 모드 혹은 ARP 스푸핑이나 MAC 플러딩을 이용하여 스위치 장비를 오버플로우시켜 패킷을 강제로 플러딩시킬 수 있다. 이 취약점을 이용하여 제어 명령 등 중요 정보를 습득할 수 있다.

4. 결론

원자력 발전소 계측제어시스템의 사이버보안 위협의 분석과 대응을 위해 테스트베드의 구축은 중요하다. 본 논문에서는 비안전계통인 다양성보호계통에서 테스트베드의 구성과 취약한 구간과 대상 및 취약점 확인이 필요한 공격을 알아보았다. 다양성보호계통에서 사이버보안 위협에 대응하기 위해 네트워크 장비에 대한 접근권한 관리, 송수신 데이터의 암호화, 정

적 ARP 테이블 관리, 스위치의 동작상태 확인, VLAN을 이용한 네트워크 분리, 스위치 보안 설정, ICMP 리다이렉트 기능의 비활성화 등이 사이버보안 위협에 대한 대응 방법이 될 수 있다. 추후 침투 시험 결과와 해당 대응 방법을 분석하여 단방향 통신과 같은 기본적인 보안 대응 방안과 함께 계통에 최적화된 선별적 사이버보안 대응 방안을 마련하고자 한다.

참고문헌

[1] Seungmin Kim, Gyunyoung Heo, EnricoZio, Jinsoo Shin, Jae-gu Song, “Cyber attack taxonomy for digital environment in nuclear power plants,” Nuclear Engineering and Technology, Volume 52, Issue 5, pp.995-1001, 2020.

[2] 이철권, “원전 계측제어시스템 사이버보안 기술동향,” 한국정보보호학회, 정보보호학회지, 제 22권, 제 5 호, 2012, pp.28-34.

[3] 원자력안전위원회규칙 제 24 호, “원자로시설 등의 기술기준에 관한 규칙,” 2020.

[4] Oh, Y.G., Jeong, J.K., Lee, J.J., Lee, Y.H., Baek, S.M., Lee, S.J., “Fault-tolerant design for advanced diverse protection system,” Nuclear Engineering and Technology, Volume 45, Issue 6, pp.795–802, 2013.