원전 디지털 계측제어계통 사이버보안 방안 고찰

최유락*°, 이재철*, 최영수*, 홍석붕*

*한국원자력연구원 융합기술개발부

Cyber Security Considerations for the NPP Digital I&C

Choi, Yoo Rark, Lee, Jae-Cheol, Choi, Young-Soo, Hong, Seok-Boong

Korea Atomic Energy Research Institute

E-mail : yrchoi@kaeri.re.kr, jclee2@kaeri.re.kr, yschoi1@kaeri.re.kr, boong@kaeri.re.kr

요 약

원전 디지털 계측제어계통 통신망에서는 일반 산업체의 사이버보안과는 달리 안전성과 가용성, 그리고 경성실시간 조건을 매우 중시하면서도 일반 IT 분야에서 사용하고 있는 사이버보안 기술의 대부분을 수용할 것을 요구받고 있다. 사이버보안 활동은 원전 디지털 계측제어계통 통신망에서 요구하는 통신망의 성능 조건을 저해하지 않아야만 하는데, 이러한 요구 조건들은 서로 상충되는 측면들이 있다. 원전 디지털 계측제어계통 사이버보안을 위한 보안기술들이 계측제어시스템 및 이와 관련된 통신망에 적용될수록 이들의 성능은 저하될 수밖에 없기 때문이다. 사이버보안에 대한 위협이 일반 산업계는 물론 국가 핵심 기반시설까지 확대되고 있는 현실에서 안전성이 가장 우선시되는 원전의 핵심 제어계통인 원전 디지털 계측제어계통에 대한 사이버보안 활동은 매우 주요하다. 본 논문에서는 원전 디지털 계측제어계통 사이버보안에 활동 수행에 필요한 고려사항들에 대하여 기술한다.

1. 서론

원자력발전소의 제어시스템이 아날로그에서 디지털로 업그레이드되고, 발전소 상태의 실시간 데이터 획득을 위한 통신 접속이 늘어남에 따라 발전소에 대한 사이버공격 취약성이 지속적으로 증가하고 있다.

원전 디지털 계측제어시스템과 통신망은 최초 설계 단계에서부터 사이버 공격에 대한 대비책을 포함하지 않았다. 특히 최근 들어 원자력발전소 디지털 계측제어계통에서 발전소 운전에 심각한 위해를 가한 사례를 분석해 볼 때 가장 많은 사이버 공격 유형은 바이러스 소프트웨어에 의한 제어시스템들의 오작동으로 밝혀지고 있다. 이러한 원인은 원자력발전소의 디지털 계측제어계통에 사용되는 제어시스템들 중 바이러스 침투 가능성이 매우 높은 윈도우즈 OS를 사용하는 제어시스템들이 바이러스에 대한 대비책을 갖고 있지 못함에 기인하는데, 이는 일반적으로 사용되는 바이러스 백신 제품들이 작동하거나 새로 업그레이드하는데 소요되는 컴퓨팅 파워가 Hard-Realtime 요건을 필수적으로 요구하는 제어시스템에 영향을 주기 때문이다.

2003년 9월 미국 데이비드 베쎄 원전 통신망에 발전소 공급자가 발전소의 한 계통에 접속하면서 유포한 슬램 웜 바이러스에 의해 비안전계통 쪽에 이상 신호를 지속적으로 발생시킴으로써 발전소 가동 중간을 야기한 사건이 있었다. 이는 원자력발전소 디지털 계측제어계통 통신망을 구성하는 안전계통 통신망과 비안전계통 통신망에 대한 외부 통신망의 접속이 완전히 차단되어 있어야 하는 원전 통신망 요구 조건이 지켜지지 않았음을 의미하

는데, NRC에서는 비안전계통을 제외한 원전의 노심과 기타 안전계통은 사이버 공격으로부터의 확실한 보호를 위해 외부 통신망과 완벽하게 단절되어 있다고 보고한 바 있다. 그러나 비안전계통에서 수집되는 계측 신호들도 원전 가동에 중요한 영향을 미치고 있으며, 결국 비안전계통에 대한 외부 통신망에서의 비인가된 접속은 원전 전체의 안전성 붕괴와 직결된다.

결국 원전 디지털계측제어계통 통신망에 대한 사이버보안은 완벽한 단방향 통신으로 다른 통신망과 단절되어 있는 안전계통 통신망을 제외한 비안전계통 통신망에 대해서 반드시 수행되어야만 한다.

본 연구는 지식경제부 원전기술혁신 연구과제의 연구비지원에 의하여 연구되었음

2. 원전 디지털계측제어계통 통신망 요구 조건

한국형 원전 디지털 계측제어계통에서는 통신과 관련된 통신망 성능 요구 조건은 다음과 같다.

① 자료처리 계통의 성능에 지장을 주지 않도록 충분한 입출력 장치를 마련해야한다. 자료수집, 처리, 분배를 위한 다양한 입출력 장치를 설치하여 타 계통과의 접속에 지장이 없도록 해야 한다.

② 모든 신호에는 신호 식별 정보를 포함하도록 설계해야 한다. 신호 식별 장보는 신호처리과정에서 발생되는 제반정보와 발생 가능한 오류 등을 확인할 수 있어 신호의 건전성을 확인할 수 있도록 한다.

③ 자료통신 선로는 이중화되고, 충분한 성능 여유를 가져야한다.

④ 자료의 전송지연시간이 여타 계통의 성능을 저해시키지 않도록 해야 한다.

⑤ 자료의 처리 과정에서 신호의 건전성을 유지할 수 있는 능력을 가져야하며, 전송 자료의 건전성을 점검하고, 오류가 있을 때 오류 정정 기능 등의 대책이 마련되어야 한다.

원전 디지털 계측제어계통의 통신망에서는 계측자료 수집이 Hard-Realtime 요건을 만족시키면서 신호와 전송 자료의 건전성을 유지할 것을 요구하고 있다.

이러한 요구 조건을 반영하기 위해 원전 디지털 계측제어계통 통신망에 사용되는 통신 프로토콜은 Shake-hand 기법을 사용하지 못하도록 규정하고 있으며, 자료 통신 선로의 Redundancy를 중요시한다. 따라서 IT 산업에서 일반적으로 사용되는 TCP/IP 프로토콜은 원전 통신망에 사용될 수 없으며 통신 선로는 이중화 되어있다.

다음 표는 원전 계측제어계통 통신망 구성과 데이터 길이, 요구 전송속도, 그리고 전송지연시간 등에 대하여 기술하고 있다.

표1. 원전 계측제어계통 통신망 구성

통신망	총 노드 / 외부 노드 수	데이터 길이 (Byte)	전체 데이터 송수신 1회 완료 전송지연시간 (msec)	요구 통신 용량	망 이용률 (%)	전송지연시간 제한 (msec) / 전체 망에서의 이용률 (%)	통신망
정보처리망	85 / 37	46~1,500	55.83	14.52 Mbps	14.52	500 / 20	100Mbps Fast Ethernet
지시 및 경보망	25 / 16	1~246	22.88	178.43 Kbps	5.95	500 / 40	Profibus-FMS
제어망	35 / 0	72 이상	15.19	19.75 Mbps	19.75	100 / 40	Token-Ethernet
보호-A/B연계망) (3 Mbps 기준)	8 / 0	1~246	8.76	341.89 Kbps	11.4	100 / 40	Profibus-FMS
보호-C/D연계망 (3 Mbps 기준)	6 / 0	1~246	22.88	238.72 Kbps	7.96	100 / 40	Profibus-FMS

원전 계측제어계통 통신망에 대한 사이버보안 활동을 수행하기 위해서는 표1에 정의된 요구조건들을 충분히 반영할 수 있는 보안 기술의 도입이

필요하다.

제어시스템의 경우 소프트웨어의 바이러스에 대비한 감염 및 치료 대책을 세우도록 요구하고 있으나, 이는 차후 건설되는 디지털 기반의 원전에 적용될 수 있을 것으로 예상된다.

이 외에 특별히 원전 디지털 계측제어계통 통신망과 관련된 요구조건들은 없는 것으로 파악되며, 바이러스 문제 외에 사이버보안과 관련된 요건에 대해서는 그 내용이 미약하다.

표2. IT와 I&C에서 요구하는 사이버보안의 관점

	IT 산업(기능성, 개방성, 확장성)	원전디지털I&C(기밀성, 무결성, 가용성)
성능과 기능요건	. High throughput . 시간 지연에 관대	. 실시간 특성요구 . 필수 응답 시간 요구
요구에 대한 응답	. 일정시간 후 정보 제공가능(또는 허용)	. 운전원에게 정보를 즉시 제공 . 패스워드 오류로 인한 시스템 잠금 금지
보안 구조의 관점	. 집중화된 시스템의 접근통제/정보보호	. 분산된 제어시스템의 접근통제 / 가용성유지
가용성과 신뢰성 요건	. 기능상실 방지	. 더욱 필요한 기능상실 방지(지나칠 정도의 시운전 필요)
안전성 요건	. 성능강조 . 정보노출 / 무결성 중시	. 정보의 노출보다는 무결성과 가용성에 중시

원전 디지털 계측제어 통신망의 사이버보안에 대한 필요성이 제기되기 시작하면서 KINS에서는 KINS/GT-N27을 통해 원전 계측제어계통 사이버보안 기술지침을 발표하였다. 이 기술지침에 따르면 원자력 시설의 안전관련 계측제어계통이 사이버 침해로부터 영향을 받지 않도록 하는 것을 원전 디지털 계측제어계통의 사이버보안의 목표로 정의하고 있다. 이 지침서에서는 원전 디지털 계측제어계통에 IT 분야에서 사용되는 모든 사이버보안 기술들이 적용될 것을 권고하고 있는데, IT 분야와 원전 디지털 계측제어계통에서 요구하는 사이버보안의 관점은 표2와 같이 그 성격이 다른 부분이 있다.

IT 분야에서는 빠른 통신을 요구하기는 하지만 실시간 개념의 통신 속도 보다는 클라이언트의 접속이 원활할 정도로만 수행될 수 있는 조건을 요구함에 반해, 원전 디지털 계측제어계통에서는 응답 속도에 대하여 매우 철저하다. 이는 IT 분야에서 연속적인 인터넷 서비스의 제공을 통한 기업 이윤 추구에 주목적을 두는 반면 원전 디지털 계측제어계통에서는 계측 신호의 발생 시간과 순서, 그리고 주어진 시간 내에 수집되어짐을 강조하고 있는 것을 의미한다. 이에 따라 원전 디지털 계측제어계통 통신망에서는 통신과 관련된 장비들이 반드시 지정된 시간 내에 지정된 임무를 완벽하게 수행할 것을 강조한다.

3. 원전 디지털계측제어계통 통신망 사이버보안 방안

최근 들어 가장 이슈가 된 사이버침해 사례는 DDOS 공격에 의한 산업계 주요 웹 사이트의 작동 불능 사태였다. 이 사건을 주도한 해커는 인터넷에 접속된 불특정 다수의 컴퓨터에 DDOS 공격에 사용되는 악성 코드를 심어 놓았으며, 특정 시간을 기준으로 이 코드들이 특정 사이트에 대해 대량의 트래픽을 발생시키는 방식을 취하였다. 이러한 공격은 악성코드에 감염된 pSet 작업자의PC에서의 PLC에 대한 대량 트래픽 유발과 같은 형태로 원전 계측제어계통 통신망에서도 발생할 수 있다.

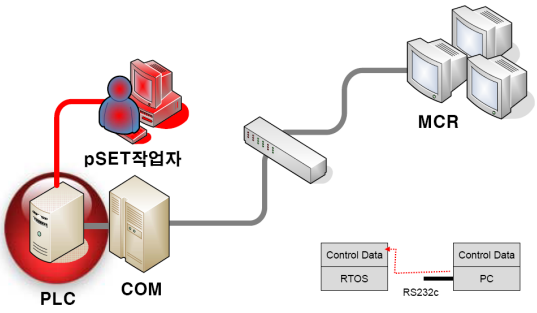

그림 1. PC-PLC 구간의 DDOS 공격 유형

IT 분야에서는 접근제어, 시스템 무결성, 암호기법, 침해 조사 및 감지, 그리고 망 구성관리 등 다양한 분야에 대한 사이버침해 방어 기술들을 개발하여 적용하고 있다. DDOS 공격은 시스템 무결성과 관련된 일부의 사례일 뿐이며, 매우 다양한 사이버 공격이 발생될 수 있다.

IT 분야에서 발생되었던 사이버공격 사례를 바탕으로 원전 계측제어계통 통신망에서 발생할 수 있는 사이버공격에 대한 유형을 분류해보면 다음과 같다.

① 외부망을 이용한 제어시스템에 대한 접근 권한 획득 : 외부와 연결된 비안전계통 통신망 컴퓨터 장비에 대한 해킹 및 제어시스템의 관리자 권한 획득

② 비인가자에 의한 제어시스템 운용 : 비인가된 내부 직원에 의한 제어시스템 관리 노출

③ 통신망 데이터의 불법 조작 : 통신망 전송 데이터의 불법 수집 및 데이터 변조

④ 컴퓨터 기반 장비에 대한 악성코드 유포 : 컴퓨터 작동 불능, 대량 트래픽 유발과 같은 악성코드를 이용한 통신망 및 컴퓨터 성능 저하 및 Back-Door를 이용한 컴퓨터 사용권한 불법 취득

⑤ 통신망에 대한 물리적 침해 : 물리적 침입자에 의한 통신망 관련 장비의 훼손 및 비인가 사용

①~④번 까지는 사이버보안 측면에서 발생할 수 있는 대표적인 침해 사례이고, ⑤번은 물리적보안 측면에서 기술한 사항이다.

①~④번 항목을 보면 각각의 항목이 독립적 사안이 아니라 사이버공격에 있어 서로가 밀접하게 연관되어 있음을 알 수 있다. 사이버공격의 유형을 크게 두 가지로 나누어 보면 공격 대상 컴퓨터나 통신망의 동작을 방해함으로써 원래의 기능을 발휘하지 못하게 하는 유형과 공격 대상 컴퓨터의 사용권을 취득하여 대상 컴퓨터를 해커가 원하는 대로 조작하는 유형으로 분류될 수 있다.

이러한 사이버공격을 감행하기 위해서는 기본적으로 공격 대상 컴퓨터에 위협을 가할 수 있는 공격 기법을 사용해야하는데, 이 방법에는 네트워크 트래픽 및 내용 분석 기술, 악성 코드 유포 기술, Back-Door를 이용한 공격 대상 컴퓨터 접근 권한 분석 및 획득 기술이 가장 많이 사용된다. 2000년대 들어 두 차례 발생했던 전 세계적인 사이버테러는 바이러스를 이용한 불특정 다수의 컴퓨터 기능 마비와 감염 컴퓨터를 좀비 컴퓨터로 만드는 악성코드를 이용한 무차별 대량 트래픽 유발을 통한 특정 컴퓨터 시스템에 대한 DDOS 공격이었다. 원전에서도 악성코드로 인한 가동 중단 사고가 수차례 발생한 바 있으며, 공격자가 목표로 하지 않았던 불특정 다수의 컴퓨터 시스템에 위해를 가하는 사례가 지속적으로 증가하고 있어 원전 계측제어통신망도 사이버공격의 안전지대는 아님을 알 수 있다.

IT분야에서는 이러한 사이버공격에 대응하기 위해 다음과 같은 기술들을 개발하여 적용하고 있다.

표3. IT분야의 사이버보안 기술 유형

범주		기술
접근 제어	경계 보호	방화벽
		컨텐츠 관리
	인증	생체 인식
		스마트 토큰
	인가	사용자 권리 및 특권
시스템 무결성		바이러스 백신 SW
		무결성 검사기
암호화		전자서명 및 인증서
		VPN
조사 및 감시		침입탐지시스템(IDS)
		침입방지시스템(IPS)
		보안사건 상관 분석
		컴퓨터 수사지원도구
구성 관리 및 보증		정책집행 응용 프로그램
		네트워크 관리
		운영도구의 연속성
		스캐너
		패치관리

IT분야에서 개발된 다양한 사이버보안 기술을 원전 계측제어 통신망에 적용하는 것은 매우 필요하고도 중요한 일이다. 그러나 IT와 원전 계측제어 통신망에서 요구하는 사이버보안의 관점 중 통신망에 연결된 컴퓨터 기반 장비의 동작 및 응답 시간과 관련된 요구 조건이 매우 달라 IT분야의 사이버보안 기술을 원전 계측제어 통신망에 모두 적용하기는 불가능하다. 이는 원전 계측제어 통신망에서 요구하는 통신망과 컴퓨터 기반 장비의 절대

적인 성능을 사이버보안 기술이 저하시킬 가능성이 매우 높기 때문이다. 예를 들어 전자인증의 경우 PKI와 관련하여 암호화와 관련된 부가적인 프로세싱 요구 시간이 필요한데, 이는 암호화와 관련된 키의 길이가 클수록 프로세싱 시간이 늘어나는 문제가 있다. 백신 소프트웨어의 경우 원전 계측제어통신망에 연결된 컴퓨터 장비들에 대한 가동 중 백실 설치 및 업그레이드가 매우 곤란하며, 네트워크 접속 제어를 위한 기술들도 네트워크에 전송되는 데이터들을 분석해야하는 프로세싱 시간을 요구하므로 전체적인 성능 저하를 야기한다.

Hard-Realtime 스펙을 요구하는 원전 디지털 계측제어계통과 같은 통신망에서는 이러한 부가적인 프로세싱 시간이 Hard-Realtime 조건을 해칠 가능성이 많으며, 향후 건설될 원전의 경우 아날로그 계측제어 장비가 디지털 장비로 계속 전환됨으로 인해 통신망에 부가되는 통신량이 크게 늘어날 것으로 예상되어 Hard-Realtime 제약을 더욱 크게 받을 것이다. 그러나 이러한 문제는 통신망과 컴퓨팅 파워에 관련된 기술 발전의 속도와 매우 밀접하게 관련된다.

최근 들어 NAC(Network Access Control)가 사이버보안의 중요한 기술로 부각되고 있다. NAC가 우회공격을 차단하고 네트워크의 무결성을 구현하는 진보된 보안 기술이지만 NAC는 다른 보안 기술들과 반드시 연동되어야만 하는데, 이들 자체가 원전 디지털 계측제어계통에서 요구하는 Hard-Realtime 조건을 해칠 가능성이 있다.

따라서 IT 분야의 매우 발전된 사이버보안 기술들을 원전 계측제어 통신망에 적용하기 위해서는 이 통신망이 가진 특성을 유지할 수 있는 방안들이 함께 개발되어야 한다.

KINS/GT-N27을 보면 정보의 노출 보다는 정보 및 시스템의 무결성과 가용성을 중시하고 있다. 원전 계측제어계통 통신망에서 사용되는 데이터 프레임을 살펴보면 데이터 사이즈가 1~1,500 Byte이면서 데이터 패딩 기법을 적용하고 있다. 이는 데이터가 노출되었을 때 분석이 매우 쉽다는 것을 의미하며, 계측제어 통신망이 침입자에 의해 스캐닝 될 경우 데이터 분석을 통한 데이터 변조는 물론 제어시스템의 제어 명령까지 쉽게 변조할 수 있는 빌미를 제공하게 된다. 통신망에 전송되는 데이터에 대한 스캐닝 기술은 해커에게 아주 유용하게 사용될 수 있다. 요즘의 웹을 이용한 통신이나 전자 금융 거래와 같은 대부분의 인터넷 통신은 암호화와 인증 기술을 이용하여 사이버보안을 수행하고 있지만, 원전 계측제어통신망과 같이 암호화와 인증기술이 전혀 적용되지 않고 있는 통신망에서는 man-in-the-middle-attack 공격에 대해서 적절한 대처를 취하기가 매우 곤란하다.

사이버보안을 방어적 입장에서 살펴볼 때, 보안은 언젠가 뚫리게 되어 있고 방어하는 쪽에서는 무너진 보안 대책을 다시 설정하기 위한 기술을 개발하고 적용하는 활동을 지속할 수밖에 없다. 원전과 같이 제어시스템의 잘못된 명령으로 인한 피해가 매우 막중한 경우에 사이버공격에 의해 보안체제가 무너졌을 경우에도 제어시스템에서 잘못된 명령이 수행되는 경우가 없어야만 한다. 이를 위해서는 기본적으로 제어시스템의 원격제어가 원천적으로 차단되어야하며, 스마트카드와 생체인식기술 등을 이용한 제어시스템 사용자 인증을 철저히 수행해야만 한다. 그러나 제어시스템이 아닌 네트워크에서 스캐닝에 의한 데이터 변조 공격을 받게 될 경우 현재의 원전 계측제어통신망에서는 이를 차단할 수 있는 방법이 없다. 이러한 공격은 외부 침입자가 원전 계측제어 통신망에 접속하였을 때 언제든지 가능한 공격 패턴으로 이를 방어하기 위해서는 데이터의 암호화와 메시지 인증 기술을 적용하는 것이 필요하다.

원전계측제어 통신망에 전송되는 데이터의 암호화와 메시지 인증을 통하여 데이터의 변조를 구별해낼 수 있다하여도 근본적으로는 스캐닝에 사용되는 컴퓨터 장비를 찾아내거나, 혹은 침입자의 접속 경로를 파악하여 이를 원천적으로 차단해야한다. 이를 위해서는 NAC 기술의 적용이 요구된다. 따라서 NAC를 구축하기 위해 연동이 필요한 여타 보안기술들이 원전 계측제어 통신망의 제약조건들에 위해를 주지 않도록 통신망 관련 장비들과 연

계성능평가를 수행해야 한다.

4. 결론

원전 디지털 계측제어 계통 통신망의 사이버보안을 위해서는 기존 IT 분야의 사이버보안 기술을 적용하는 것이 타당하다고 판단된다. 다만, 기존 IT 분야의 사이버보안 기술을 원전 디지털 계측제어 계통 통신망에 적용하기 위해서는 이 통신망에서 요구하는 Hard-Realtime 조건과 같은 특정한 요구 조건들을 만족시켜야만 한다. 이를 위해서는 컴퓨터 기반 장비와 통신망의 성능 대비 IT 분야의 사이버보안 기술이 소비하는 프로세싱 시간을 비교 분석하여야 한다. 기존 원전에 사용되고 있는 컴퓨터 기반 장비들에 대해서는 현재 사용되고 있는 IT 분야의 사이버보안 기술의 적용 가능 여부를 장비의 스펙 비교와 성능 실험을 통하여 결정할 수 있으나, 향후 변화되는 컴퓨팅 파워와 사이버보안 기술에 대해서는 적용 가능 여부에 대한 정확한 비교 분석이 매우 어렵다.

사이버보안은 언젠가는 붕괴될 수 있으며, 이것이 붕괴될 때 심각한 피해를 입지 않기 위해서 가장 기본적으로 필요한 조치가 무엇인지를 파악해야하는데, 현재의 원전 계측제어통신망은 해킹에 의한 통신망 외부 접속 시 모든 계측 관련 데이터와 제어명령이 그대로 노출되는 문제점을 가지고 있다. 따라서 이러한 문제를 해결하기 위해서는 원전 계측제어 통신망에 전송되는 모든 데이터에 대한 암호화와 메시지 인증이 필요하며, 외부 침입자나 내부 불법 접속자에 대한 방어 및 처리 기술이 요구된다. 이러한 보안 기술들의 원전 계측제어 통신망으로의 적용을 위해서는 적용하고자 하는 보안 기술들이 표1에 명시된 통신망의 조건들을 수용할 수 있는지에 대한 철저한 검증이 반드시 선행되어야만 한다.

[참고문헌]

[1] 이철권 외, I&C 총괄 시스템 설계, KAERI/RR-2495, 2003.

[2] ANSI X9.63(Draft), “Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Key Cryptography.”

[3] 2008 Information Security All Guide v.3

[4] IEEE Regulatory guide 1.152, “Criteria for use of computers in safety systems of nuclear power plants”, DG-1130, 2004.

[5] NRC Draft final Regulatory guide 5.71, “Cyber security programs for nuclear facilities”, The Advisory Committee on Reactor Safeguards, 2009