Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.2.267

원전 계측제어계통의 안전 네트워크 설계 및 평가를 위한 보안 기준

김도연*

Security Criteria for Design and Evaluation of Secure Plant Data Network on Nuclear Power Plants

Do-Yeon Kim*

요 약

원자력발전소의 데이터 네트워크와 연관된 안전 계통들은 다양한 IT (information technology) 네트워크 및 응용프로그램들을 적용하여 현대화되고 있다. 발전소 데이터 네트워크의 출현과 더불어 원전 계측제어시스템들은 최신의 디지털화된 마이크로프로세서에 근간을 둔 시스템으로 진화하고 있는 반면에, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 이를 보완하기 위해 원전에 적용하는 데이터 네트워크는 신뢰성, 성능 및 보안요건을 충분히 고려해서 설계되어야 한다. 본 논문에서는 원전 계측제어계통에 적용되는 안전한 네트워크의 설계 및 평가 시 사용될 수 있는 기술적인 보안 기준들을 제시하였으며, 본 기준들을 적용하여 설계 및 운영되는 발전소 데이터 네트워크는 외부의 사이버 위협으로부터 효과적인 대처를 할 것으로 판단된다.

ABSTRACT

Nuclear power plant data networks and their associated safety systems are being modernized to include many information technology (IT) networks and applications. Along with the advancement of plant data networks (PDN), instrumentation and control systems are being upgraded with modern digital, microprocessor-based systems. However, nuclear PDN is confronted significant side-effects, which PDN is exposed to prevalent cyber threats typically found in IT environments. Therefore, cyber security vulnerabilities and possibilities of cyber incidents are dramatically increased in nuclear PDN. Consequently, it should be designed fully ensuring the PDN meet all reliability, performance and security requirements in order to overcome the disadvantages raised from adaption of IT technology. In this paper, we provide technical security criteria should be used in design and evaluation of secure PDN. It is believed PDN, which is designed and operated along with these technical security critera, effectively protect against possible outside cyber threats.

키워드

Nuclear Power Plant, Technical Security Criteria, Secure Plant Data Network
원자력발전소, 기술적인 보안 기준, 안전한 발전소 데이터 네트워크

* 교신저자(corresponding author) : 순천대학교 컴퓨터공학과(dykim@sunchon.ac.kr)
접수일자 : 2013. 11. 21 심사(수정)일자 : 2013. 12. 13 게재확정일자 : 2014. 02. 11

I. 서 론

원전은 우리나라 주요 에너지원으로 국가적인 차원의 기간시설 보호대책이 요구된다. 과거 개인 및 사무실에 제한되었던 사이버보안 문제가 최근 들어 원자력발전소 계측제어시스템에 운용되고 있는 네트워크에도 위협을 가하고 있다. 사이버 공격에 의해 원전 계측제어계통을 대상으로 임의 조작이 발생하면 원전의 운영중단 및 파손 등의 심각한 사태를 야기 시킬 수 있다. 지금까지 원전의 계측제어계통은 전용 통신망의 사용, 고유의 운영체제의 사용 등으로 인하여 사이버 위협에 안전하다고 여겨져 왔지만, 원전 계측제어시스템의 개방화 및 표준화에 의해 사이버 위협에 대한 취약점이 증가하고 있으며, 최근 국외에서 수집된 사이버 침해 사례를 보면 더 이상 해킹 및 사이버 테러 등의 사이버 위협에 안전 할 수 없는 현실이다 [1].

원자력발전소 계측제어계통은 일반 IT 시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있다. 폐쇄성은 인터넷과 같은 외부 네트워크와 분리된 내부의 필드 장비들만 연결하는 폐쇄적인 네트워크를 사용하면서 독자적인 설비 시설에서 개별적으로 운영되는 특징이 있으며, 특수성은 독자적인 프로토콜 및 임베디드 운영체제가 사용되고 하드웨어 역시 독자적인 변형을 가지는 장비가 사용되며, 가용성은 상시 작동할 수 있도록 운영되는 특징을 가진다 [2].

원전 계측제어시스템은 주요 기반시설로써 사이버 공격으로 인해 기능이 마비되면 국민의 생명, 생활, 재산, 국가 경제에 중대한 영향을 끼쳐 국가경제에 혼란 초래할 수 있다.

본 논문에서는 원전 계측제어계통을 구성하는 안전한 디지털 네트워크의 설계 및 평가 시 사용되는 기술적인 보안 기준에 대해 논하고자 한다. 2장에서 원자력설비 및 시설들에 대한 사이버침해 사례를 열거하고, 3장에서는 원전 계측제어계통의 안전한 네트워크의 구조에 대해 기술하며, 4장에서는 원전 계측제어계통의 안전한 네트워크 설계 및 평가 시 사용되는 기술적인 보안 기준에 대해 논하고자 한다.

II. 원자력설비에 대한 침해 사례

2.1 우라늄 농축시설에 대한 Stuxnet 침투 사고

스턱스넷은 SCADA 시스템 중 독일 지멘스(Siemens)사의 SIMATIC PCS7 시스템을 공격하도록 설계되어 있다. PCS7의 다양한 컴포넌트 중 SIMATIC WinCC7와 SIMATIC Step7이라 불리는 통합 관리도구를 공격 대상으로 삼고 있다. SIMATIC WinCC는 통제 및 모니터링 시스템으로서 PLCs(programmable logic controllers) 와 통신을 담당하는 소프트웨어인데, 스턱스넷은 WinCC의 존재하는 취약점을 이용하여 침투하게 된다. 또 다른 컴포넌트인 Step7은 제어 PC와 산업자동화 제어시스템 간에 블록(동작명령)파일 교환을 담당한다. 스턱스넷은 Step7의 일부 구성 요소를 자신이 생성한 파일로 교체시켜 산업자동화 제어 시스템을 모니터링 하거나 임의의 블록(악성 명령어 블록)을 생성시켜 제어하게 된다. 이렇게 장악된 시스템은 공격자가 제어하게 된다. 이렇게 장악된 시스템은 공격자가 의도한 명령으로 동작하게 되는데, 현재 발견된 스턱스넷은 모든 PLC의 영향을 주진 않고, PLC 타입 6ES7-315-2와 6ES7-417만 감염의 영향을 받는 것으로 알려졌다 [3].

2.2 Davis-Besse 원자력발전소 사고

2003년 SQL 슬래머 웜이 미국 오하이오에 위치한 Davis-Besse 원자력발전소의 감시계통 컴퓨터에 감염되어, 관련 설비의 작동이 5시간 이상 불능 상태로 유지되었으며, 여타 발전소 제어망 통신에도 영향을 미친 것으로 보고되었다 [4].

2.3 Browns Ferry 원자력발전소 정지사고

2006년 두 개의 원자로 재순환 펌프의 고장으로 수동 정지되는 사고가 발생했다. 발전소컴퓨터시스템 네트워크에 연결된 이중의 PLC에 의해 작동되도록 설계된 재순환펌프의 VFD (variable frequency drive) 제어기가 반응하지 않았다. 조사결과, 발전소컴퓨터시스템 네트워크의 과도한 트래픽으로 기인된 사고로 분석되었으나, PLC 자체의 고장인지, 아니면 과도한 네트워크 트래픽으로 인한 VFD 제어기의 미 반응 결과인지에 대한 확인은 이루어지지 않았다. 이는 확인되지 않은 네트워크의 취약점으로 인한 정지사고로 추측할 수 있다 [5].

III. 원전 계측제어계통의 안전 네트워크 구조

원자력발전소의 데이터 네트워크와 연관된 안전 계통들은 다양한 IT 네트워크 및 응용프로그램들을 적용하여 현대화되고 있다. 발전소 데이터 네트워크의 출현과 더불어 원전 계측제어시스템들은 최신의 디지털화된 마이크로프로세서에 근간을 둔 시스템으로 진화하고 있다. 고도로 발전된 IT 및 네트워크 관련 기술들이 원전 계측제어시스템에 적용되고 있는 관계로, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 위협[6-8], 보안취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 이러한 단점들을 보완하고자 원전에 적용하는 데이터 네트워크는 신뢰성, 성능 및 보안요건을 충분히 고려해야 하며, 사이버 위협에 안전한 네트워크의 설계 및 평가가 이루어져야 한다.

3.1 원전 계측제어계통의 운영 특성

원전에서 운영되었던 최초의 네트워킹된 시스템들은 특화된 하드웨어 및 소프트웨어의 사용 및 자체 제작된 제어프로토콜을 적용한 격리된 형태의 네트워크 시스템을 운용 하였으며 IT 시스템과의 유사성이 많지 않았다. 하지만, 최근에 들어 광범위하게 사용되는 저렴한 IP 기기들이 자체 제작된 솔루션들을 대체하여 원전에 적용되는 관계로, 사이보안 취약점 및 관련 사고가 증가하는 상황이다. 비록 현대화된 원전 계측계통 및 데이터 네트워크에 IP 프로토콜과 설계 경험을 적용하고 있지만, IT 시스템과 원전 네트워크망을 사용한 계측제어계통의 운영 환경은 상당히 큰 차이를 가진다. 이러한 차이점들이 사이버보안의 평가방법 및 보안통제 항목의 구현방법 등에 영향을 미칠 수 있다 [9].

다음은 원전 계측제어계통만이 가지는 운영 특성들이다.

- 필수자산의 보안 : 상업화된 IT 시스템에서 보호되어야만 되는 주된 자산은 일반적으로 서버에 저장되어 있는 정보이지만, 계통을 보호하고 제어하는 각각의 장비들이 서버에 저장된 정보 보다 중요한 관계로, 발전 데이터 네트워크를 구성하는 모든 보안 기능들은 시험되어야 한다.

- 위기관리 : 전형적인 IT시스템 보안은 데이터 기밀성 및 무결성에 초점을 맞추고 있지만, 원전에서는 각 개인이나 공공의 생명을 위협하는 안전성을 우선으로 한다.

- 가용성 및 신뢰성 : 최상의 가용성 및 신뢰성을 요구하는 원전의 운전 특성상, 일반적인 IT 시스템에서의 전략 (예, 리부팅)등은 허용되지 않는다.

- 소프트웨어 및 자원의 제약 : 원전의 특정 계통은 전형적인 IT 소프트웨어 및 경험이 적용될 수 없는 형태의 커스터마이징된 실시간 운영체제 또는 임베디드된 시스템을 포함하고 있다. 또한, 벤더 계약사항으로 인해 3자의 보안 솔루션을 적용할 수 없는 한계점도 존재한다.

- 반응시간 : IT 시스템과는 달리 원전에서는 운전원의 상호작용 및 자동화된 계통의 반응시간이 굉장히 중요한 요소로 작용한다.

3.2 안전 네트워크의 구조

현대화된 발전 데이터 네트워크는 다양한 IT 네트워크와 연결되어 있다. 아날로그 형태로 설계된 안전 네트워크는 컴퓨터기반의 네트워크로 개선되고 있다. 그림 1은 원전에 적용할 수 있는 가상의 현대화된 디지털 네트워크를 보여주고 있으며, 안전기능을 수행하는 네트워크 세그먼트, 공정제어, 데이터 획득, 운전 기능을 제공하는 제어실 세그먼트로 구성 된다 [10].

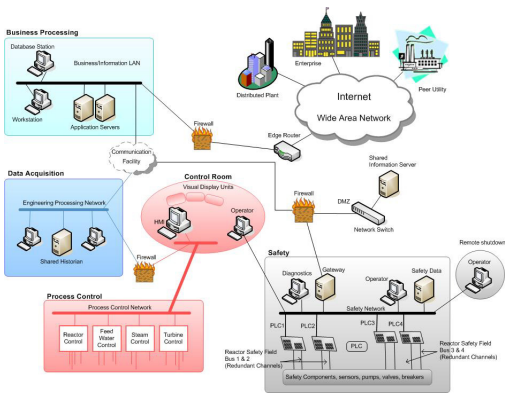

그림 1. 가상의 디지털 플랜트 네트워크 구조 [10]
Fig. 1 Hypothetical digital plant system network architecture [10]

Ⅳ. 안전 네트워크의 보안 기준

IT 네트워크 및 관련 신기술들을 적용한 원전 계측제어계통의 데이터 네트워크는 발전소의 운전 효율을 향상 시킬 수 있도록 자동화 정도를 극대화 할 수 있고, 운전원의 부담을 경감 시킬 수 있으며, 정상 및 비정상 운전 조건에 대한 상황인지력을 증가시킬 수 있는 장점을 가진다. 하지만 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 위협, 보안취약성 및 사고의 가능성이 원전 계측제어계통의 데이터 네트워크에도 그대로 존재한다는 단점을 가진다. 이러한 단점들을 극복하기 위해서는 데이터 네트워크의 신뢰성, 성능 및 보안요건을 충분히 고려해야 하며, 사이버 위협에 안전한 네트워크의 설계 및 평가가 이루어져야 한다. 다음은 원전에 적용하고자 하는 안전한 네트워크를 설계하고, 또한 설계평가를 수행할 시 충분히 고려되어야만 되는 보안관점의 기준들에 대해 기술 하고자 한다 [10].

4.1 보안정책 기준

필수 디지털 자산을 보호하기 위해 발전소 자체의 보안 정책 및 절차들에 대한 주기적인 검토가 요구되며, 기술발전 현황을 평가하고, 조직원들의 역할 및 책임사항과 관련된 위험요소를 확인해야 한다.

4.2 물리적 보안 기준

다중 레이어 및 중복성을 겸비한 제대로 설계된 물리적 방호시스템이 요구되며, 효율적인 물리적 방호시스템이 되기 위해서는 발견, 지연 및 대처 기능이 충분히 고려되어야 한다.

4.3 네트워크 구조 설계 및 위상 기준

네트워크의 위상은 문서화되고 검토되어야 하며, 각각의 네트워크 기기 및 경로들은 위치 기반으로 정확하게 확인되어야 한다. 네트워크의 분리를 위한 경계는 명확하게 정의되어야 한다. 또한, 네트워크의 위상은 가능한 간단한 계층구조를 갖도록 설계되어야 되며, 심층방어 개념을 지원 가능해야 한다.

4.4 네트워크 감시 기준

네트워크 트래픽을 포함한 네트워크 자원을 감시할 목적으로 보안관리 시스템을 적용해야 한다. 이와 더불어 네트워크 감시 목적으로 침입탐지시스템(IDS) 및 침입차단시스템(IPS)을 사용할 수 있다.

4.5 통신 매체 기준

통신 매체로 동선을 사용할 경우 물리적인 감사 및 검토를 통해 안전계통 네트워크가 전자파간섭(EMI)으로 자유롭다는 것을 확인해야 되고, 통신 매체 보호를 위해 물리적인 장벽이 온전히 유지되는지를 확인해야 한다. 안전기능을 수행하는 계통에 무선기기를 적용한 설계는 허용하지 않는다. 상대적으로 광섬유를 사용하는 것은 EMI 및 무선주파수간섭(RFI)으로부터 자유로워 잡음이 존재하는 환경에 적합하다.

4.6 데이터 흐름 기준

네트워크에 존재하는 필수 장비들 사이의 데이터 흐름을 파악할 수 있어야 한다. 가상랜(VLAN) 사용 시 네트워크에 생성되는 데이터 흐름의 영향을 확인해야 되며, 가상사설망(VPN)의 사용은 금지한다.

4.7 네트워크 접근제어 기준

발전소 데이터 네트워크에 접근제어 방법을 적용해야 하고, 네트워크의 모든 장비들은 주어진 필요한 기능만 수행할 수 있도록 보호되어야 한다. 흐름제어 메커니즘을 적용해야 되고, 데이터 흐름 필터링을 위해 방화벽의 필터링 룰을 제대로 구성해야 된다.

4.8 네트워크 정보 보증 기준

발전소 네트워크상에 전달되는 데이터를 보호해야 되며, 가용성, 신뢰성, 기밀성, 무결성 등을 유지해야 된다.

4.9 네트워크 기기 기준

발전소 데이터 네트워크에 일반적으로 사용되는 기기들의 보안 특성 및 기능들을 면밀히 검토하여야 한다. 이러한 네트워크기기 들은 이더넷장비, 제어기(PLC)장비, 게이트웨이 및 방화벽을 포함한다.

4.10 시스템 사용자 인터페이스 기준

의도적이거나 부주위로 인한 보안 위반 확률을 경감시키기 위해, 또한 계통의 보안을 전반적으로 향상시키기 위해 사용자 인터페이스 설계 제대로 이루어 져야 한다.

4.11 시스템 생명주기 기준

설계오류, 잘못된 구성 및 부적절한 운전 등으로 기인되는 보안 취약점들을 제거하기 계통의 생명주기 동안에 준수해야 되는 기준을 제시한다. 생명주기는 개념, 요건, 설계, 구현, 시험, 설치 및 운전 단계를 포함한다.

Ⅴ. 결 론

노후화, 유지보수 비용의 증가 및 좀 더 효율적인 운영 목적으로 원전 계측제어계통 및 데이터 네트워크는 최신의 마이크로프로세서 기반의 계통으로 대체되거나 일부분 개선되고 있는 상황이다 [11].

IT 및 네트워크 관련 기술들이 원전 계측제어시스템에 적용되고 있는 관계로, 일반적인 IT 환경에서의 각종 정보시스템이 가지는 사이버보안 위협, 보안 취약성 및 사고의 가능성이 증대되는 단점을 가지게 되었다. 이를 보완하기 위해 원전에 적용하는 데이터 네트워크는 신뢰성, 성능 및 보안요건을 충분히 고려해서 설계되어야 한다. 원전 계측제어계통에 적용되는 안전한 네트워크의 설계 및 평가 시 사용될 수 있는 기술적인 보안 기준들을 제시하였으며, 본 기준들을 적용하여 설계 및 운영되는 발전소 네트워크는 외부의 사이버 위협으로부터 효과적인 대처를 할 것으로 판단된다.

참고 문헌

[1] Y. Choi, Y. Choi, J. Lee, C. Wan, I. Koo, and S. Hong "Study on the Construction of Cyber Security for the Nuclear Power Plants," *Fall Conf. from Korea Society of IT Services*, 2009, pp. 537-538.

[2] Y. Cha, B. Cho, and J. Na, "Security Technology Trends and Prospective of Industrial Control System," *KEIT PD Issue Report*, vol. 13, no. 6, 2013, pp. 79-100.

[3] N. Falliere, L. O. Murchu, and E. Chien, *Win32.stuxnet Dossier.* Symantec Security Response, 2011.

[4] NRC Information Notice 2003-14, *Potential Vulnerability of Plant Computer Network to Worm Infection.* Nuclear Regulatory Commission, 2003.

[5] NRC Information Notice 2007-15, *Effects of Ethenet based, no-safety related controls on the safe and continued operation of nuclear power stations.* Nuclear Regulatory Commission, 2007.

[6] W. Seo and M. Jun, "A Direction of Convergence and Security of Smart Grid and Information Communication Network," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 5, no. 5, 2010, pp. 477-486.

[7] I. Koo, K. Kim, S. Hong, G. Park, and J. Park, "Digital Asset Analysis Methodology against Cyber Threat to I&C System in NPP," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 6, no. 6, 2011, pp. 839-847.

[8] C. Yoon, G. Kim, and C. Jang, "Embedded-based Power Monitoring Security Module Design," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 8, no. 10, 2013, pp. 1485-1490.

[9] C. K. Veitch, S. Wade, and J. T. Michalski, *Cyber Security Assessment Tools and Methodologies for the Evaluation of Secure Network Design at Nuclear Power Plants.* Sandia National Laboratories, 2012.

[10] NRC NUREG/CR-7117, *Secure Network Design.* Nuclear Regulatory Commission, 2012.

[11] J. T. Michalski, F. J. Wyant, and D. Duggan, *Secure Network Design Techniques for Safety System Applications at Nuclear Power Plants.* Sandia National Laboratories, 2010.

저자 소개

김도연(Do-Yeon Kim)

1986년 충남대학교 계산통계학과 졸업(이학사)

2000년 충남대학교 대학원 정보통신공학과 졸업(공학석사)

2003년 충남대학교 대학원 컴퓨터공학과 졸업(공학박사)

1986년～1996 한국원자력연구원 선임연구원

1997년～2008 한국전력기술(주) 책임연구원

2008년～현재 순천대학교 컴퓨터공학과 교수

※ 관심분야 : 영상보안, ICS 및 원전사이버보안