Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 4 pp. 664-673, 2018

https://doi.org/10.5762/KAIS.2018.19.4.664
ISSN 1975-4701 / eISSN 2288-4688

산업제어시스템 환경에서 효과적인 네트워크 보안 관리 모델

김일용[1], 임희택[1], 지대범[1], 박재표[2*]
[1]숭실대학교 대학원 IT정책경영학과, [2]숭실대학교 정보과학대학원

A Efficient Network Security Management Model in Industrial Control System Environments

Il-Yong Kim[1], Hee-Teag Lim[1], Dae-Bum Ji[1], Jae-Pyo Park[2*]
[1]**Department of IT Policy Management, Soongsil University**
[2]**Graduate School of Information Science, Soongsil University**

요 약 산업제어시스템(ICS, Industrial Control System)은 과거에는 폐쇄 네트워크로 운영되었으나 최근에는 정보통신 서비스와 연결되어 운영되면서 사이버 공격으로 인한 피해로 이어지고 있다. 이에 대한 대책으로 정보통신기반보호법이 제정되고 보안가이드라인이 배포되고 있지만 제어망에서 업무망으로의 일방향 정책만 있어 다양한 실제 제어 환경에 대한 보안가이드가 필요하며 국제 표준으로 IEC 62443의 경우 산업제어시스템 참조 모델을 정의하고 침입 차단 시스템을 이용한 영역 보안 모델을 제시하고 있으나 폐쇄 네트워크로 운영되는 산업제어망을 침입 차단 시스템만으로 외부 네트워크와과 연계하기에는 부담이 있다. 본 논문에서는 국내외 산업제어시스템 보안 모델 및 연구 동향을 분석하고 다양한 국내 산업제어망의 실제 연동 환경에 적용할 수 있는 산업제어시스템 보안 모델을 제안한다. 또한 현재 상용 경계 보안 제품들인 침입 차단 시스템, 산업용 침입 차단 시스템, 망 연계 장비, 일방향 전송 시스템 등의 보안성을 분석하였다. 이를 통하여 국내 구축 사례와 정책에 대한 비교를 통해 보안성이 향상되는 것을 확인하였다. 4차 산업혁명 시대를 맞이하여 스마트 팩토리, 스마트 자동차, 스마트 플랜트 등 다양한 산업제어 분야에 대한 보안 관리 방안에 적용할 수 있을 것이다.

Abstract The industrial control system (ICS) has operated as a closed network in the past, but it has recently been linked to information and communications services and has been causing damage due to cyber attacks. As a countermeasure, the Information Communication Infrastructure Protection Act was enacted, but it cannot be applied to various real control environments because there is only a one-way policy-from a control network to a business network. In addition, IEC62443 defines an industrial control system reference model as an international standard, and suggests an area security model using a firewall. However, there is a limit to linking an industrial control network, operating as a closed network, to an external network only through a firewall. In this paper, we analyze the security model and research trends of the industrial control system at home and abroad, and propose an industrial control system security model that can be applied to the actual interworking environments of various domestic industrial control networks. Also, we analyze the security of firewalls, industrial firewalls, network connection equipment, and one-way transmission systems. Through a domestic case and policy comparison, it is confirmed that security is improved. In the era of the fourth industrial revolution, the proposed security model can be applied to security management measures for various industrial control fields, such as smart factories, smart cars, and smart plants.

Keywords : Industrial Security, ICS Security, SCADA Security, ICS Reference Model, Industrial Control System

*Corresponding Author : Jae-Pyo Park(Soongsil Univ.)
Tel: +82-2-820-0270 email: pjerry@ssu.ac.kr
Received January 24, 2018 Revised February 19, 2018
Accepted April 6, 2018 Published April 30, 2018

1. 서론

산업제어시스템(ICS, Industrial Control System)은 과거에는 폐쇄망으로 운영되어 물리적인 공격이나 조작 실수가 대부분이었으나 최근에는 정보통신 서비스와 연결되어 운영되면서 사이버 공격으로 인한 피해로 이어지고 있다[1].

이에 대한 국가 차원의 대책으로 정부는 2001년 국가적으로 중요한 정보통신기반시설을 보호하기 위해 「정보통신기반보호법」을 제정하였으며 “주요 정보통신 기반시설 취약점 분석·평가 기준”을 고시하고 “산업제어시스템 보안요구사항”[2]을 마련하고 있다.

국내의 경우, 제어시스템은 업무망, 인터넷망과 물리적으로 분리하여 폐쇄망을 구성하고 제어 네트워크와 외부와 자료연계 시 물리적 일방향 환경을 구축하도록 되어 있다[2-3]. 국내 제어망 보안모델은 제어망과 업무망으로 이분화하고 물리적 일방향 장비(One-Way System, Data Diode)를 적용하도록 만 권고하고 있어 다양한 제어망 연계에 대한 보안과 제어망 내부 네트워크에 대한 보안 대책이 추가적으로 필요하다.

ISA/IEC 62443[4-5]등에서는 제어망을 영역별로 분류하고 방화벽(Firewall)을 이용한 제어망 영역(Zone)간 경계 보안 모델을 제시하고 있다. 방화벽은 네트워크 경계 보안의 기본이지만 보안정책이 느슨하면 제어망을 보호할 수 없고 업무망 시스템과 제어망 시스템이 방화벽으로 연결되어 있어 업무망 시스템이 해킹될 경우 제어망에 영향을 미칠 수 있다. 또한 제어망이 해킹되면 기업 경쟁력에 막대한 영향을 미칠 수 있어 방화벽만으로 산업제어망을 외부망과 연계하기는 어렵다.

본 논문의 2장에서는 국내외 산업제어시스템 보안 모델 및 연구 동향을 분석하고 3장에서는 다양한 국내 산업제어망의 실제 연동 환경에 적용할 수 있는 산업제어시스템 보안 모델을 제안하고 4장에서는 제안한 산업제어망 보안 모델을 현재 시장에서 출시되어 있는 경계 보안 제품을 통해서 검증하고 5장에서 결론을 제시한다.

2. 관련 연구

본장에서는 국내외 산업제어시스템 보안 모델 및 연구 동향을 분석하고 산업제어만의 경계 보안 모델로 적용할 수 있는 보안 제품들을 분석한다.

2.1 국내외 산업제어시스템 보안 모델

산업제어시스템 보안 모델로는 국외 모델로 NIST SP 800-82[6], ISA/IEC 62443[4-5]을 분석하고 국내 모델로 “산업제어시스템 보안요구사항”[2]에 있는 제어시스템 운영환경 모델을 분석한다.

2.1.1 NIST SP 800-82

NIST SP 800-82[6]는 산업제어시스템을 안전하게 수립하기 위한 공식적인 지침서로 산업제어시스템에 대한 일반적인 구성과 개념을 제시하고 산업제어시스템의 관리적, 운영적, 기술적 보안 통제를 분류하고 산업 제어시스템이 가지고 있는 취약성과 위험요소를 도출하여 산업제어시스템을 보호하기 위한 기술과 대응책을 제공한다[7-8].

NIST SP 800-82에서 제시하는 ICS 보안 구조에서는 기업 네트워크와 ICS 네트워크를 분리하는 것을 권고하고 있으며 네트워크가 연결되어야 한다면 최소의 연결만 허용되어야 하고 그 연결은 방화벽(Firewall)과 비무장지대(De-Military Zone)를 구성하도록 권고하고 있다.

NIST SP800-82에서 권장하는 네트워크 구성은 다음과 같다.

- o 기업네트워크와 제어 네트워크 사이에 침입차단시스템 또는 라우터와 침입차단시스템 조합 구성
- o 기업 네트워크와 제어 네트워크 사이에 침입차단시스템을 설치하고 DMZ 영역 구성
- o 기업 네트워크와 제어 네트워크 사이의 침입차단시스템을 쌍으로 구성하고 침입차단시스템들 사이에 DMZ 영역 구성

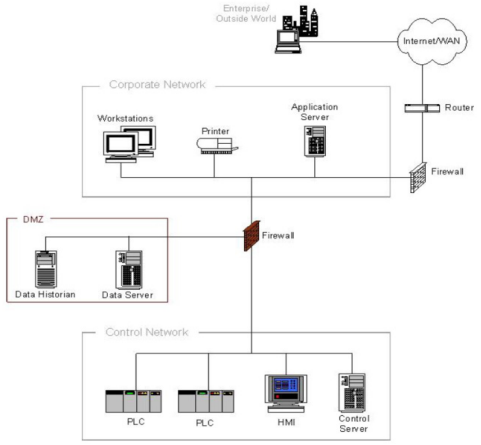

Fig. 1. Firewall with DMZ between Corp. and ICS Networks

2.1.2 ISA/IEC 62443

ISA/IEC 62443[4-5]은 미국 ISA(International Society of Automation)가 산업제어시스템(ICS)에 대한 보안이슈를 다루기 위해 제정한 표준으로 ISO/IEC 62443 시리즈의 보안요구사항 및 보안대책은 산업제어시스템 환경에 적합하도록 특성화하여 제정되었으며 ISA/IEC 62443 시리즈는 일반, 정책 및 절차, 시스템, 컴포넌트의 4가지 범주로 나누어져 있다[7, 9].

ISA/IEC 62443은 IACS(Industrial Automation and Control System) 보안에 대한 정의, 모델 등을 포괄하고 있으며 ANSI/ISA-95.00.01[9]의 산업제어시스템 참조 모델을 사용하고 있다.

산업제어시스템 영역으로 Level 0 Process, Level 1 Local or Basic Control, Level 2 Site Monitoring & Local Display, Level 3 Operations/Systems Management로 구분하고 있으며 엔터프라이즈 영역으로 Level 4를 두고 있다.

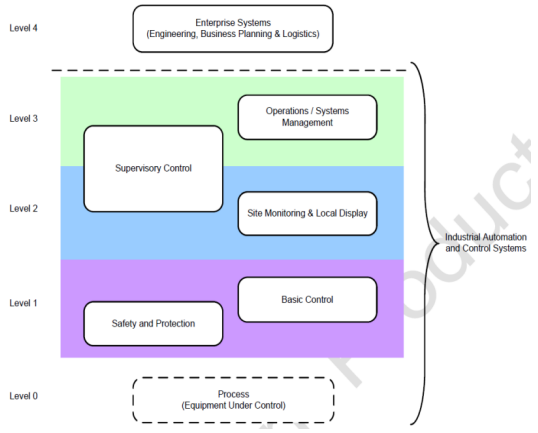

Fig. 2. ICS Reference Model

또한 산업제어시스템 보호를 위해 공통된 보안이 요구되는 논리적, 물리적 자산 그룹을 Zone으로 두고 영역의 경계를 명확하게 정의하고 있으며 두 영역 사이의 정보 흐름 통로로 통신 채널을 보호하기 위한 논리적 통신 자산 그룹을 Conduit으로 정의하고 있다.

Zone과 Conduit 개념을 SCADA 참조 모델의 실제 제어망에 적용하면 figure3과 같이 구성된다.

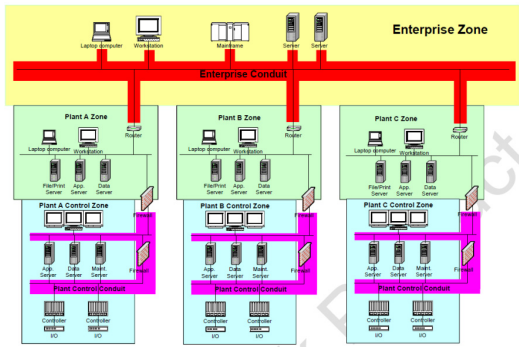

Fig. 3. Zone and Conduit Example

2.1.3 국내 제어시스템 기본 구성 모델

국내 산업제어시스템에 대한 정책적 보안 모델은“산업제어시스템 보안요구사항”[2]에 정의되어 있다.

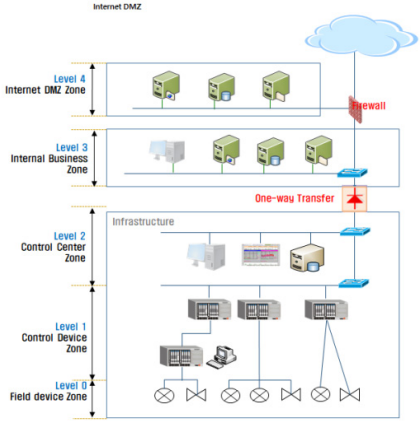

Fig. 4. Industrial Control System Example

제어시스템의 일반적인 구성을 제어시스템 외부망 영역으로 Level 4 인터넷 DMZ 영영과 Level 3 내부 업무망 영역을 두고, 제어시스템 영역을 Level 2 제어센터 영역, Level 1 제어기기 영역, Level 0 현장장치 영역으로 구분하며 제어시스템 영역에서 외부망(내부 업무망) 영역으로의 일방향 전송만 규정되어 있다.

2.2 영역 분리를 위한 적용 시스템 유형

네트워크 영역 분리를 위한 적용 시스템 유형으로는 IT 방화벽, 산업용 방화벽, 데이터 다이오드, 망연계 장비 등이 있다.

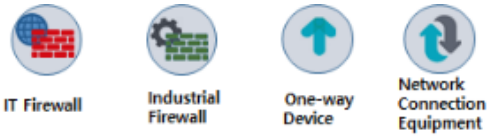

Fig. 5. Boundary Protection Systems

2.2.1 IT 방화벽을 이용한 영역 분리

방화벽을 이용한 영역 분리는 인터넷과 기관망을 분리하기 위해 가장 많이 사용하는 방식이다. NIST SP 800-82, ISA/IEC 62443 등에서 제어망과 업무망, 제어망 내부에서의 영역분리 등을 위해 사용하고 있다. 방화벽 보안정책은 내부 네트워크에서 외부 네트워크로 접근할 수 있지만 외부 네트워크에서 내부 네트워크로의 접근은 허용하지 않아 보안성이 강화되지만 실질적으로 보안정책의 적용 및 관리의 어려움이 있다. 또한 내부 네트워크의 시스템에서 외부 네트워크의 시스템으로 네트워크 접속이 발생하므로 외부 시스템의 직접적인 영향을 받을 수 있다.

2.2.2 산업용 방화벽을 이용한 영역 분리

산업용 방화벽은 IT 방화벽 기능에 산업제어프로토콜에 대한 필터링 기능을 제공한다[9-11]. ISA/IEC 62443를 적용한 사례[12-13]에서는 업무망과 외부망, 제어망과 업무망 경계에는 IT 방화벽을 적용하지만 제어망 내부에서의 영역분리를 위해서는 산업용 방화벽을 사용하고 있다.

산업용 방화벽은 산업제어프로토콜 명령어에 대한 필터링 기능을 제공하므로 제어센터에서 제어기기 및 현장장치로의 불법적인 접근이나 명령을 차단할 수 있지만 보안정책의 적용 및 관리는 IT 방화벽보다 복잡하다. 이로 인하여 제어망 내부에서 산업용 방화벽보다 IT 방화벽을 사용하는 경우가 많다.

2.2.3 데이터 다이오드를 이용한 영역 분리

데이터 다이오드는 단방향으로만 정보가 전달되도록 송신/수신 회선의 한쪽을 물리적으로 차단한 연결선을 사용한다. 보안등급이 높은 제어망에서 보안등급이 낮은 업무망으로 운영정보를 단방향으로 전송하기 위해 사용되며 폐쇄망을 요구하는 기반시설에서 많이 사용된다[14-16].

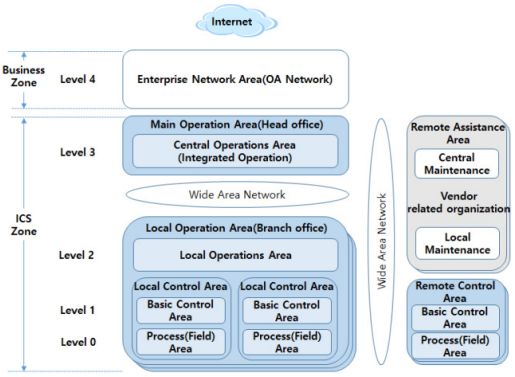

Fig. 6. Industrial Control System Configuration Model

데이터 다이오드는 내부 네트워크의 시스템과 외부 네트워크의 시스템이 직접 연결되지 않고 정해진 데이터만 단방향으로 전달하므로 보안성이 강화되며 외부 네트워크에서 내부 네트워크로의 회선이 물리적으로 단절되어 있어 외부 해킹을 100% 차단하고 제어망을 폐쇄망으로 유지할 수 있다.

2.2.4 망연계 장비를 이용한 영역 분리

망연계 장비는 서로 다른 영역(보안영역과 비-보안영역) 간 사용자 PC 및 서버 스트림을 보안 정책에 따라 안전하게 전송해 주는 망간 자료전송 제품이다[17].

망연계 장비는 물리적으로 업무망과 인터넷망을 분리했을 경우 원활한 업무수행을 위해 업무망과 인터넷망 간 자료교환을 위해 사용되며, 기반시설에서 양방향 통신이 요구될 경우 사용되는 경우도 있다[18-20].

망연계 장비는 보안영역 전송통제서버와 비-보안영역 전송통제서버로 구성되어 방화벽 보다 보안성이 높지만 망연계 장비의 허용 정책에 따라 내부 네트워크의 시스템과 외부 네트워크의 시스템이 응용 레벨에서의 세션 연결이 발생하므로 외부 시스템의 직접적인 영향을 받을 수 있다.

3. 산업제어망 보안 모델 제안

3.1 산업제어망 분리 모델

본 논문에서는 ISA/IEC 62443의 SCADA 참조 모델을 기반으로 국내 제어시스템 운영 기관들의 환경을 다음과 같이 산업제어망 영역(Zone) 분리 모델을 구성하였다.

본 논문에서는 산업제어망을 ISA/IEC 62443에서와 같이 영역(Zone) 개념을 사용하여 영역을 분리하고 크게 비즈니스 영역과 제어시스템 영역으로 구분한다.

비즈니스 영역은 국내 망분리 정책에 따라 인터넷 DMZ망, 인터넷연결망, 업무망으로 분리하고 있으나 본 논문에서는 제어시스템과 연결되는 업무망을 중심으로 비즈니스망을 정의한다.

Table 1. Industrial Control System Components

Assortment	Level	Domain	Component
Enterprise	Level 4	Enterprise Network Area	PC, Server Etc.
Control system	Level 3	Central Operations Area	PI, Historian, DB Server Etc.
	Level 2	Local Operations Area	DCS, HMI, DB Server Etc.
	Level 1	Basic Control Area	RTU, RLC, IED, HMI Etc.
	Level 0	Field Device Area	Pump, Motor, Valve Etc.

산업제어시스템 영역은 중앙 운영 영역(본사)과 로컬 운영 영역(지사)으로 구분하고 중앙 운영 영역을 Level 3로, 로컬 운영 영역을 Level 2, 1, 0로 구분하고 있다.

로컬 운영 영역은 로컬 운영관리 영역을 Level 2로, 실질적인 제어 영역은 기본제어영역 Level 1과 현장장치 영역 Level 0로 분류하였다. 여기서 제어 영역은 지사에 있는 로컬 제어 영역과 지사에서 원격으로 운영하는 원격 제어 영역을 별도로 분리하였다.

또한 원격 사이트로 원격 운영 영역과 원격 지원 영역을 구분하였다. 원격 운영영역은 지사의 로컬 운영망에서 원격으로 운영하는 제어 영역으로 Level 1, 0로 구성되며 원격 지원 영역은 벤더 영역으로 원격 유지보수 업무를 수행하며 중앙운영 원격지원 Level 3, 로컬운영 원격지원 Level 2로 구성하였다.

Table 2. Remote Site Component

Assortment	Level	Domain	Component
Remote Assistance Area	Level 3	Central Remote Assistance	Remote maintenance of central operation network
	Level 2	Local Remote Assistance	Remote maintenance of local operation network
Remote Control Area	Level 1	Remote Basic Control	RTU, RLC, IED, HMI Etc.
	Level 0	Remote Field Control	Pump, Motor, Valve, Button Etc.

제안한 산업제어망 분리 모델에 대하여 위에서 정의한 제어망 영역별 구성 요소를 포함시키면 산업제어망은 다음과 같이 구성된다.

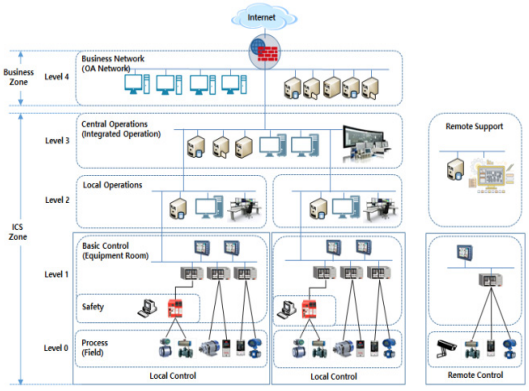

Fig. 7. Basic configuration model of industrial control network

3.2 산업제어망 보안 적용 모델

본 장에서는 제안된 산업제어망 기본 구성 모델을 기반으로 산업제어망 보안 적용 모델을 정의한다.

산업제어망 보안적용 모델은 Level 3까지를 제어망으로 관리하는 경우, Level 2까지를 제어망으로 관리하는 경우, Level 1까지를 제어망으로 관리하는 경우에 대하여 산업제어망 보안 적용 모델을 제시하고 부가적으로 원격 제어망과 원격 지원망에 대해서도 보안 적용 모델을 제시한다.

3.2.1 Level 3 기반 제어망 보안 관리 모델

기관망을 OA망과 FA망으로 분리하고 FA망 전체를 제어망으로 관리하는 보안 관리 모델은 다음과 같다.

이는 본사 통합운영과 지사 로컬 운영망을 모두 제어영역으로 보고 OA 업무망만을 비즈니스 영역으로 보는 것으로 국내 제어망 보안정책을 고려하면 제어망에서 로컬 운영망으로 단방향 전송장비를 적용해야 한다.

또한 본사 통합운영 영역과 지사별 로컬 운영 영역, 로컬 운영 영역 내 영역별 제어망을 분리하고 방화벽을 사용하는 것이 좋으며 제어망의 특성에 따라 IT 방화벽보다는 산업용 방화벽을 사용하는 것이 효율적이다. 또한 중앙 운영망과 로컬 운영망 사이에 인터넷 구간이 있는 경우 VPN을 추가로 사용해야 한다.

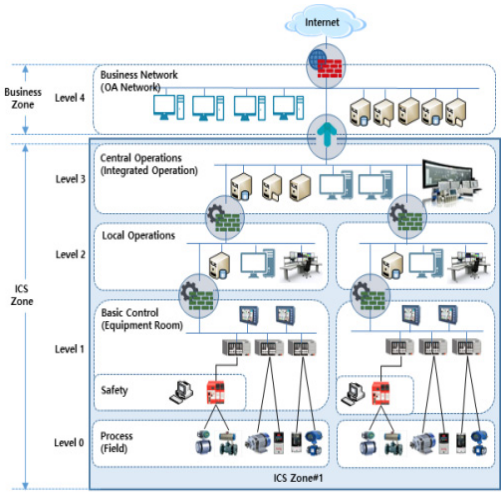

Fig. 8. Level 3 based control network security magn. model

3.2.2 Level 2 기반 제어망 보안 관리 모델

본사 운영 영역과 지사 운영 영역을 분리하고 제어시스템이 있는 지사 운영 영역을 제어망으로 관리하는 경우 보안 관리 모델은 다음과 같다.

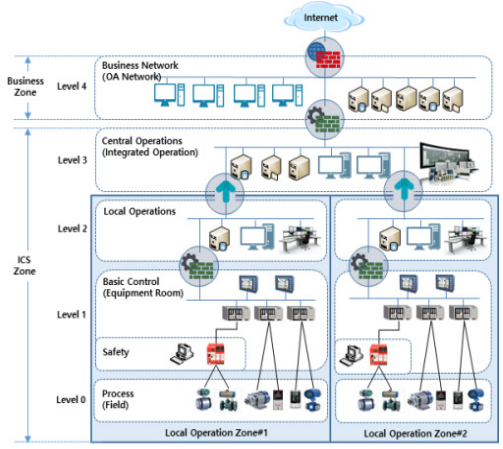

Fig. 9. Level 2 based control network security management model

이는 지사의 로컬 운영망을 실질적인 제어 영역으로 보고 중앙 운영망을 FA 업무망으로 보는 것으로 국내 제어망 보안정책을 고려하면 로컬 제어망에서 로컬 운영망으로 단방향 전송장비를 적용해야 한다.

중앙 운영망은 FA 업무망으로 비즈니스 영역인 OA 업무망과 성격이 다르므로 방화벽을 사용하여 영역을 분리할 필요가 있으며 제어망 내부인 로컬 제어망에 대해서도 영역별로 분리하고 방화벽을 사용하는 것이 좋다.

FA 업무망과 제어망의 특성에 따라 IT 방화벽보다는 산업용 방화벽을 사용하는 것이 효율적이다. 또한 중앙 운영망과 로컬 운영망 사이에 인터넷 구간이 있는 경우 VPN을 추가해야 한다.

3.2.3 Level 1 기반 제어망 보안 관리 모델

지사 운영 영역에서 실질적인 제어시스템 영역별로 제어망을 관리하는 경우 보안 관리 모델은 다음과 같다.

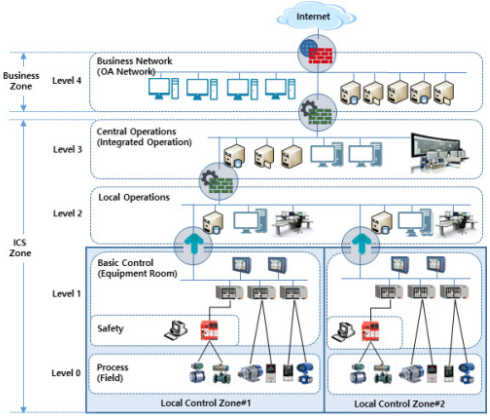

Fig. 10. Level 1 based control network security magn. model

이는 로컬 제어망을 실질적인 제어 영역으로 보고 로컬 운영망을 FA 업무망으로 보는 것으로 국내 제어망 보안정책을 고려하면 로컬 제어망에서 로컬 운영망으로 단방향 전송장비를 적용해야 한다.

중앙 운영망과 로컬 운영망은 FA 업무망으로 OA 업무망과 영역이 다르므로 방화벽을 사용하여 영역을 분리할 필요가 있으며 FA 업무망의 특성에 따라 산업용 방화벽을 사용하는 것이 효율적이다. 또한 중앙 운영망과 로컬 운영망 사이에 인터넷 구간이 있는 경우 VPN을 추가로 사용해야 한다.

3.2.4 원격 제어망 보안 관리 모델

지사 로컬 운영센터에서 원격으로 제어망을 관리하는 경우 보안 관리 모델은 다음과 같다.

지사 로컬 운영센터에서 원격제어망을 관리하기 위해

양방향 통신이 필요한 경우 산업용 방화벽을 적용해야 하며 CCTV와 같이 정보 수집만 필요한 경우 단방향 장비가 효율적이다. 또한 로컬 운영망과 원격제어망 사이에 인터넷 구간이 있는 경우 VPN을 추가로 사용해야 한다.

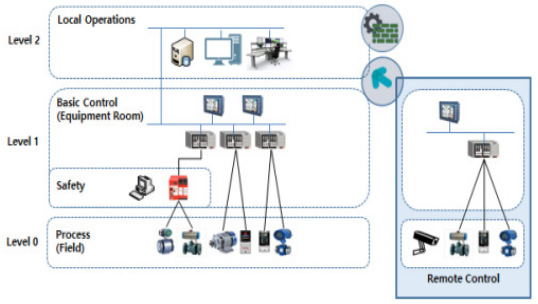

Fig. 11. Remote control network security management model

3.2.5 원격 지원망 보안 관리 모델

원격으로 유지보수를 수행하는 벤더들에 대한 보안 관리 모델은 다음과 같다.

대부분의 벤더들은 RMS(Remote Management Service)를 제공하며 이를 위해 중앙 또는 로컬 운영 영역에서 제어망 운영 정보를 벤더로 전달해야 하는데 국내 제어망 보안정책을 고려하면 단방향으로 전달해야 한다. 제어망과 원격지원망 사이에 인터넷 구간이 있는 경우 VPN을 추가로 사용해야 한다.

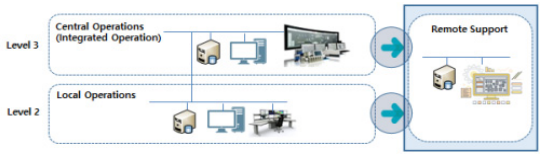

Fig. 12. Remote Assistance network security management model

4. 산업제어망 보안 모델 검증

4.1 국내외 제어망 보안 모델 비교 분석

본 논문에서 제안하는 제어망 보안 모델은 국내 제어망 보안정책을 준수하면서 국제 표준 모델을 만족하는 것이다.

이를 위해 ICS 영역을 ISA/IEC 62443과 같이 레벨 0에서 레벨 3까지 구분하고 있으며 업무망과 ICS망 경계 보안을 위해 국내 보안정책을 고려하여 단방향 장비를 권고하고 있다. 또한 국내 보안정책에서 제어망 내부 네트워크 보안에 대한 내용이 없어 ISA/IEC 63443의 Zone과 Conduit 개념을 적용하여 제어망 내부 네트워크 영역 간 방화벽을 권고하고 있으며 제어망 특성을 고려하여 IT 방화벽보다는 산업용 방화벽을 권고하고 있다.

Table 3. Remote Assistance Network Security Magm. Model

Type / Assortment	Proposal	NIST SP 800-82	ISA/IEC 62443	Domestic Security Policy
ICS Area classification	Level 0 to level 2 distinction	Classification of control network by area	Level 0 to level 3 distinction	Level 0 to level 2 distinction
Business area classification	Level 4	Classification of business network by area	Level 4	Level 3
Business network / ICS network separation type	physical	Logical	Logical	physical
Business network / ICS network boundary type	One-way	Firewall (Two-way)	Firewall (Two-way)	One-way
ICS Internal network security	Industrial firewall	Not Defined	Firewall	Not Defined
Advantages	No hacking from business network to control network (One-way)	Two-way communication on from business network to control network (Limit)	Two-way communication from business network to control network (Limit)	No hacking from business network to control network (One-way)
Dis-advantages	No two-way communication on from business network to control network	Hacking from business network to control network (Two-way)	Hacking from business network to control network(Two-way)	No two-way communication from business network to control network

4.2 국내 단방향 장비 구축 사례를 통한 모델 비교 분석

국내 제어망 보안정책이 제어망에서 업무망으로 단방향으로 데이터를 전송하는 것으로 큰 맥락은 있지만 실제 사이트에서 구성된 형태는 다음과 같이 여러 상황들이 있다.

Table 4. Examples of domestic one-way equipment

Type	Description
Case 1	One-way from Central Operation Network(Integrated Management) to Head Office Operation Network
Case 2	One-way from the local operation network (branch office) to the central operation network (head office)
Case 3	One-way from local control network (per unit) to local operating network
Case 4	One-way communication of remote CCTV information to local operating network
Case 5	One-way to vendor for remote management services(RMS)

국내 단방향 장비 구축 사례는 대부분 보안성 검증을 거쳐 구축된 사례들이지만 국내 정책과 비교하면 레벨 2(제어망)와 레벨 3(업무망) 해석이 유동적이다. 반면 본 논문에서는 5가지 경우에 대해 명확한 기준을 제시하고 있다.

Table 5. Comparison of Domestic Case and Policy

Type / Assortment	Proposal	Domestic Security Policy Standard
Case 1	One-way between level 4 and level 3	One-way between level 2 (control center) and level 3(business network)
Case 2	One-way between level 3 and level 2	One-way between local network to level 2 and center network to level 3
Case 3	One-way between level 2 and level 1(Local)	One-way between local control network to level 2 and local operation network to level 3
Case 4	One-way/firewall between level 2 and level 1(remote access)	One-way/firewall application to control network to internal network
Case 5	One-way between level 2 or level 3 and remote support	One-way between central/ local operation network to level 2 and external network to level 3

국내 단방향 장비 구축 사례를 통해 국제 표준과 비교하면 5가지 경우 모두 각 레벨과 일치하며 국제 표준에서는 방화벽을 권고하고 있지만 단방향 장비도 가능하며 본 논문에서는 국내 정책을 고려하여 단방향 장비를 기준으로 권고하고 있다.

Table 6. Cmpsn. of dom. case and international standard

Type / Assortment	Proposal	ISA/IEC 62443
Case 1	One-way between level 4 and level 3	Firewall between level 4 and level 3
Case 2	One-way between level 3 and level 2	Firewall between level 3 and level 2
Case 3	One-way between level 2 and level 1(Local)	Firewall between level 2 and level 1
Case 4	One-way/firewall between level 2 and level 1 (Remote access)	Firewall between level 2 and level 1
Case 5	One-way between level 2 or level 3 and remote support	Firewall application to external network to level 4

4.3 경계보안제품 해킹가능성 보안성 분석

인터넷망 분리에 사용되는 망연계 장비를 제외한 방화벽, 산업용 방화벽, 단방향 전송장비의 일반적인 공격차단 기능과 허용 기능은 다음과 같다.

해커가 업무망의 인가된 시스템을 해킹하여 장악하고 다시 인가된 서비스의 취약성을 이용하여 제어망의 인가된 HMI를 장악하여 제어 명령을 내릴 수 있다 이 경우 국내외 제어시스템 보안 모델의 보안성은 다음과 같다.

Table 7. Block and allow hacking of perimeter security products

Type / Assortment	Blocking function	Allow function
Firewall	Block unauthorized systems/services (Control command can not be controlled)	Allow authorized systems/ services Allow all control commands
Industrial firewall	Block unauthorized systems/services Block unauthorized control commands	Allow authorized systems/ services Allow authorized control command
One-way transmission equipment	All connections from the business network to the control network Physical blocking	Authorized data one-way transmission from the control network to the business network

국내외 제어시스템 보안 모델의 보안성을 비교하면 국제 표준 모델들은 업무망에서 제어망으로의 해킹이 가능하지만 국내 정책 및 본 제안은 업무망에서 제어망으로의 해킹이 불가능하다. 또한 본 논문에서는 국내 정책

에서 빠져있는 제어망 내부 네트워크 보안을 정의함으로써 보안성을 향상시키고 있다.

Table 8. Comparison of Domestic Case and Policy

Type / Assortment	Proposal	NISTSP 800-82	ISA/IEC 62443	Domestic Policy
Connection from the unauthorized system of the business network to the control network system	O One-way	O Firewall	O Firewall	O One-way
Connection from the authorized system of the business network to the control network system	O One-way	X	X	O One-way
Network packet attacks on the control network using authorized services in the business network	O One-way	X	X	O One-way
Connection from the unauthorized system of the control network to the control device	O Industrial firewall	△ Router	O Firewall	△ Router
Unauthorized control command attack in the authorization system in the control network	O Industrial firewall	X	X	X
An abuse attack using an authorized control command in an authorized system in the control network	X	X	X	X
	Industrial IDS/IPS required			

※O: Attack defense(Controled), X: Defensive failure(Hackable)

5. 결론

본 논문에서는 국외 산업제어시스템 보안 모델로 NIST SP 800-82와 ISA/IEC62443을 분석하고 국내 제어망 보안 모델로 “산업제어시스템 보안요구사항”을 분석하였다. 또한 네트워크 경계 보안을 위해 현재 시장에서 출시되어 있는 경계 보안 제품들로 IT 방화벽, 산업용 방화벽, 데이터 다이오드, 망연계 장비 등의 특징을 살펴보았다.

본 논문에서는 국내외 산업제어시스템 보안 모델 분석을 통해 제어시스템 참조 모델을 제안하고 산업제어망 보안관리 모델을 제시하였다.

산업제어시스템 참조 모델은 ISA/IEC 62443와 마찬가지로 비즈니스 영역을 레벨 4로 두고 제어망 영역을 레벨 3에서 레벨 0까지 두고 있으며 ISA/IEC 62443과 각 레벨의 의미는 차이를 두고 있다. 레벨 3는 본사 중앙 운영 영역, 레벨 2는 지사 로컬 운영 영역, 레벨 1/0은 각각의 로컬 제어 영역으로 레벨 1은 기본제어 영역, 레벨 0은 현장장치 영역으로 정의하고 있으며 원격 제어 영역과 원격 지원 영역을 별도로 정의하고 있다. 또한 제안된 산업제어시스템 참조 모델을 기반으로 산업제어망 보안관리 모델을 제안하고 있다. 산업제어망 보안적용 모델은 Level 3까지를 제어망으로 관리하는 경우, Level 2까지를 제어망으로 관리하는 경우, Levle 1까지를 제어망으로 관리하는 경우에 대하여 산업제어망 보안 적용 모델을 제시하고 부가적으로 원격 제어망과 원격 지원망에 대해서도 보안 적용 모델을 제시하였다.

산업제어망 보안관리 모델에서는 방화벽을 기본으로 하는 국제 표준과 달리 국내 정책을 고려하여 업무 영역과 제어 영역 사이 경계 보안은 단방향 장비를 권고하고 있으며 제어망 내부 네트워크 보호를 위해서는 산업용 방화벽을 권고하고 있다.

본 논문에서 제안된 산업제어망 보안관리 모델은 국내 정책 모델과 국제 표준 모델을 준수하도록 구성되어 있음을 검증하고 국내 단방향 장비 구축 사례를 통하여 국내 정책 준수 여부와 국제 표준 모델 준수 여부를 검증하였다.

또한 경계 보안 제품들의 해킹 가능성에 분석하여 산업제어시스템 보안 모델에서 권고하는 경계 보안제품의 구성 측면에서 가장 보안성이 뛰어남을 확인하였다.

본 논문에서는 산업제어시스템 중 기반시설에 해당되는 제어시스템을 기반으로 보안 모델이 제시되어 다양한 산업제어시스템 분야로의 확장이 필요하다. 향후 4차 산업혁명 시대 스마트 팩토리, 스마트 자동차, 스마트 플랜트 등 다양한 산업제어 분야에 대한 보안 관리 방안에 대한 연구가 필요하다.

References

[1] National Intelligence Service, Ministry of Science, ICT and Future Planning, Korea Communications Commission, Ministry of the Interior and Safety, Financial Service Commission, 2017 National information Security White Paper, 04. 2017.

[2] Ministry of Science, ICT and Future Planning Announcement 2013-37, Baseline for Vulnerability Analysis and Evaluation in the Critical Information Communication Infrastructure, 08. 2013.

[3] National Security Research Institute, Requirements for Industrial Control System, 2017. 11.

[4] IEC TS 62443-1-1:2009, Industrial communication

networks - Network and system security - Part 1-1: Terminology, concepts and models, Jul. 2009.

[5] ISA-62443-1-1, Security for Industrial Automation and Control System, Mar. 2017.

[6] NIST SP 800-82, Guide to Industrial Control System Security, May. 2015.

[7] Jun-Hyeong Oh, Young-In You, Kyung-Ho Lee, “Computer Emergency in Infrastructure and ICS Standards Trends”, Review of KIISC vol. 27, no. 2, pp. 5-11. 04. 2017.

[8] David Kuipers, Mark Fabro, Control Systems Cyber Security : Defense in Depth Strategies, INL/EXT-06-11478, May 2006.

[9] ISA-95.00.01-CDV3, Enterprise-Control System Integration, Part 1: Models and Terminology, 2008.

[10] Belden Inc., Tofino Security Appliance. https://www.tofinosecurity.com

[11] Moxa Inc., https://www.moxa.com/

[12] Crystal Group Inc., https://www.crystalrugged.com/

[13] Tofino Security White paper. Using ANSI/ISA-99 Standards to Improve Control System Security, May. 2012.

[14] NNSP Co. Ltd., http://nnsp.co.kr

[15] Waterfall Security Solutions Ltd., https://waterfall-security.com/

[16] Owl Cyber Defence Solution, https://www.owlcyberdefense.com/

[17] IT Security Certification Center, Requirements for Government IT Security Products, 2014.

[18] Hanssak Co. Ltd., http://www.hanssak.co.kr

[19] SQLsoft Co. Ltd., http://www.sqisoft.com

[20] Hunesion Co. Lted., http://www.hunesion.com/

김 일 용(Il-Yong Kim) **[정회원]**

- 2013년 8월 : 숭실대학교 정보과학대학원 (공학석사)
- 20018년 2월 : 숭실대학교 IT정책경영학과 박사 수료
- 2002년 12월 ~ 현재 : ㈜앤앤에스피 대표

<관심분야>
정보통신, 정보보안

임 희 택(Hee-Teag, Lim) **[정회원]**

- 2002년 8월 : 한양대학교 행정대학원(행정학석사)
- 20018년 2월 : 숭실대학교 IT정책경영학과 박사 수료
- 2015년 2월 ~ 2017년 2월 : 사회보장정보원 기획이사
- 2017년 9월 ~ 현재 : 우송대학교 보건의료경영학과 초빙교수

<관심분야>
정보경영, 정보통신

지 대 범(Dae-Bum Ji) **[정회원]**

- 2012년 2월 : 연세대학교 공학대학원 공학경영학과 (공학석사)
- 2018년 2월 : 숭실대학교 IT정책경영학과 박사 수료
- 2015년 2월 ~ 2017년 2월 : 사회보장정보원 정보이사
- 2017년 9월 ~ 현재 : 호서대학교 디지털기술경영학과 교수

<관심분야>
S/W공학, 정보보안, Big-Data 분석

박 재 표(Jae-Pyo Park) **[종신회원]**

- 1998년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
네트워크 보안, 디지털포렌식, 금융IT