물리적 단방향 시스템의 도입 확대 방안에 관한 연구

A Study on the Expansion of Physical Unidirectional System

심 영 복*, 박명노*, 이 종 연**1)
(주)위런텍*, 충북대학교**

Shim, Young Bok*, Park Myung No*, Lee Jong Yun**
Weruntech Co., Ltd..*,
Chungbuk National Univ.**

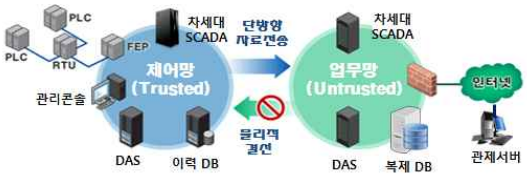
요약

물리적 단방향 자료전달 시스템은 산업제어시스템에 적용하여 보안등급이 높은 안전영역에서 보안등급이 낮은 비안전영역으로의 데이터 전송을 물리적으로 한방향으로만 전달하는 보안 시스템으로, 최근 사이버테러에 대한 사회적, 경제적 피해가 날로 증가함에 따라 다양한 산업제어시스템에서 단방향 자료전달 시스템에 대한 기술 개발 및 적용 요구가 증가하므로 본 연구에서는 단방향 통신 기술의 현 주소를 짚어보고 앞으로의 발전 방향과 저변 확대를 위한 방안을 제안한다.

Ⅰ. 서론

최근 원전, 정부기관, 금융, 통신사 등 정부기관 뿐 아니라 민간 기간망 등에 대한 사이버테러 혹은 개인정보 유출 사고가 심심치 않게 발생하고 있으며 국방, 원전과 같은 국민 안전과 직결된 분야에 대한 보안 위협이 현실화되고 있다. 이와 같은 외부로부터의 해킹, 보안 사고에 의한 피해를 방지하기 위한 기술을 망간 자료전송 기술이라고 하며, 최근 제어시스템에 이 기술을 도입하여 보안을 강화하고 있다[1].

물리적 단방향 자료전달 시스템[1][2]은 그림 1과 같이 망간 자료전달 시스템의 일종으로 비안전 영역에서 안전 영역으로 데이터를 보낼 수 있는 회선을 물리적으로 차단함으로써 외부로부터의 침입을 원천적으로 차단하는 장치이다.



▶▶ 그림 1. 물리적 단방향자료전달시스템 구성도

본 연구에서는 이러한 물리적 단방향 자료전달 시스템에 대한 국내·외 현황을 고찰하고, 향후 산업 분야에 적용 확대를 위한 방안을 제안한다.

Ⅱ. 본론

1. 단방향자료전달시스템의 국내 기술 동향

국내 망간 자료전송 기술은 크게 스토리지 방식, 소켓 방식, 시리얼인터페이스 방식 등의 소프트웨어에 기반하여 개발되었으나 최근에는 보안 최고 레벨인 물리적 단방향자료전달시스템이 제어시스템에 적용되고 있는 추세이다.

1.1 단방향자료전달시스템의 국내 현황

아래 표 1은 기존 소프트웨어 기반의 망분리 시스템 기술 현황이며, 표 2는 최근 개발 및 산업제어시스템에 적용이 활발하게 진행되고 있는 물리적 단방향자료전달 시스템의 기술 현황이다.

표 1. 국내 망분리 시스템 기술 현황

제조사	모델명	CC인증	OS/DBMS	프로토콜
휴네시온	i-oneNet V2.0	EAL3	RHEL/ MySQL,Oracle	전용 암호화 프로토콜
시큐에버	reverseWall -MDS 3.0	EAL4	공개 안됨	전용 암호화 프로토콜 / FCP
엘케이 컴즈	i-Connect V3.0	EAL3	CentOS / MySQL	전용 암호화 프로토콜
지온 공작소	CoreBridge 2.0	EAL2	RHEL, IBM AIX,	FCP
에스큐 아이 소프트	ssBridge 3.0	EAL2	RHEL, Mysql	FCP

1) 교신저자, jongyun@chungbuk.ac.kr

표 2. 국내 물리적 단방향자료전달시스템 기술 현황

제조사	모델명	CC 인증	지원프로토콜
한전 KDN	NIMA-1000	국정원보안 적합성만족	UDP, TCP, FTP, 파일전송, OPC, DAS, SCADA, PI Redundancy
휴네시온	i-oneNet DD	-	UDP, TCP, 파일전송
NNSP	nNetDiode	EAL2	OPC, Modbus, Syslog, SNMP, SQL

1.2 단방향자료전달시스템의 국내 적용 사례

기존 소프트웨어 기반의 망분리 시스템의 경우 공공기관, 금융기관 등을 주 고객으로 시장을 형성하고 있으나 여전히 악의적인 외부의 공격을 완벽하게 차단하지 못하므로 그 대안으로 물리적 단방향자료전달시스템이 대두되었다. 물리적 단방향자료전달시스템은 최근 본격 개발되어 한전, 발전사, 수자원공사, 지역난방공사 등의 산업제어시스템에 적용, 확산되고 있는 추세이며 주로 TCP 스트리밍, File Transfer, FTP, OPC-DA, DAS[3], SCADA 등의 서비스 프로토콜을 사용하는 구간에 적용하여 운영되고 있다.

2. 단방향자료전달시스템의 해외 기술 동향

2.1 단방향자료전달시스템의 해외 기술 현황

물리적 단방향자료전달시스템은 최초로 이스라엘의 Waterfall社에서 개발되었으며 국내보다 관련 기술 개발 및 현장 도입이 월등히 앞서 있다. 아래 표 3은 해외의 대표적인 물리적 단방향자료전달시스템의 기술 현황이다.

표 3. 해외 물리적 단방향자료전달시스템 기술 현황

제조사	모델명	평가기준	지원프로토콜
Water-Fall [4]	UnidirectionalSecurityGateWay	EAL4+	ICCP, Modbus, DNP3 등의 표준 SCADA, DB, OPC, PI, Syslog, HTTP, PLC 등 다양한 서비스 지원
Owl [5]	Data Diode Cybersecurity Solutions	-	Syslog, PI, OPC, DB, Modbus, File transfer, TCP, UDP 등 다양한 서비스 지원

2.2 단방향자료전달시스템의 국외 적용 사례

해외의 물리적 단방향자료전달시스템은 오래된 역사만큼 다양한 분양에 적용하여 운용되고 있다. Waterfall社의 제품의 경우 주요 H/W 벤더별로 대부분의 제어장치의 프로토콜(Historian, DB, IEC 60870-104, Modbus, OPC-DA, OPC-HDA, OPC-AE, OPC-UA, DNP3, ICCP, SNMP, Syslog, SMTP, TFTP, FTP, etc.)을 지원하며 다양한 산업제어시스템에 적용하여 운영되고 있다.

3. 단방향자료전달시스템의 도입 확대 방안

국내에서 단방향자료전달시스템이 활발하게 개발되고 있으나 아직 저변확대를 위해 넘어야할 산이 많은 것이 현실이며 이를 극복하기 위한 방안을 제시한다.

- 첫째, 해당 제어시스템에 단방향자료전달시스템을 적용하려면 서비스 프로토콜에 대한 단방향 전송 방식에 맞는 에이전트를 별도로 개발해야만 한다. 따라서 단방향자료전달시스템의 저변 확대를 위해서는 제어시스템의 다양한 서비스 프로토콜의 개발이 선행되어야 한다.
- 둘째, 특정 프로토콜의 경우 양방향으로 통신해야만 정상적으로 운영이 가능한 서비스가 있는데, 이 경우 단방향 전송으로 서비스 지원이 가능하드록 기존 서비스의 프로토콜 변경이 요구된다.
- 셋째, 국가 기간망, 금융, 국방 등 국민 재산과 안전에 직결된 망에 대한 사이버테러를 원천 차단을 위해 단방향자료전달시스템의 도입을 범정부적 차원에서 촉진하고, 더불어 핵심 기간망에 대한 단방향자료전달시스템의 의무 적용을 확대해 나갈 필요가 있다.

Ⅲ. 결론

본 논문에서는 산업제어시스템에 적용된 국내·외 주요 단방향자료전달시스템의 기술 동향과 적용 사례들을 살펴보았다. 또한, 최근 사회 이슈로 부각되는 사이버테러로부터 시민 안전과 재산권 보호를 위해 단방향자료전달시스템의 도입 촉진과 저변 확대를 위한 방안으로, ▲다양한 산업제언시스템에 적용할 수 있는 서비스 에이전트 확충 ▲단방향자료전달시스템의 적용이 가능하도록 양방향성의 기존 프로토콜을 단방향성으로 변경 요구 ▲시스템 도입 촉진을 위한 범정부적 지원과 투자 확대를 제시하였다.

향후 과제로 산업제어시스템에서 수요 프로토콜의 우선순위가 높은 서비스를 선별하여 그 개발 방안을 제시하고 개발 서비스의 신뢰성을 확보할 수 있는 방법에 대한 연구가 요구된다.

■ 참 고 문 헌 ■

[1] 김경호, “제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계”, 정보과학회논문지 정보통신 제40권 제2호, pp. 126~130, 2013.
[2] Pascal Sitbon, “Enabling Secure Information Exchange from a Less Secure Zone to a Control System Zone in a Critical Infrastructure,” Proceedings of the SCADA Security Scientific Symposium, Digital Bond Press, pp.10, 2003.
[3] 김지희, “배전DAS-업무망 보안 이슈 및 물리적 일방향 자료전달 시스템 적용 방안,” 정보보호학회지 제24권 제5호, 2014.
[4] http://www.owlcti.com
[5] http://www.waterfallsecurity.com