Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.3, Jun. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.3.463

발전제어시스템에 적용 가능한 사이버 보안 정보공유 모델 연구

민 호 기,[1†] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on Cyber Security Information Sharing Model Applicable to Power Generation Control System

Hogi Min,[1†] Junghee Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

발전제어시스템의 보안 취약점 개선을 위한 선행 연구의 한계점을 분석하고 그 대안으로 사이버 보안 정보공유모델을 제안하였다. 발전제어시스템의 운영 특성을 파악하고 사이버 보안 정보공유 개념과 정책, 실제 구현사례들을 분석하여 발전제어시스템에 효과적으로 적용할 수 있는 정책과 기술방안을 제시하고 모델평가를 시행하였다.

ABSTRACT

The limitations of previous research on improving security vulnerabilities in power generation control systems were analyzed, and as an alternative, a cyber security information sharing model is proposed. Understanding the operational characteristics of power generation control systems, we examined the concepts and policies of cyber security information sharing, analyzing practical implementation cases. We presented effective policies and technological approaches that can be applied to power generation control systems, and their efficacy was verified through a model evaluation to validate their impact.

Key words: power generation control systems, cyber security, information sharing

I. 서 론

발전제어시스템은 전기를 생산하는 발전소에서 시스템의 제어 및 감시를 위해 사용되는 컴퓨터 기반의 시스템을 말한다. 발전제어시스템은 제작사 고유의 통신 프로토콜을 기반으로 한 단독망으로 보안에 안전하다는 인식이 지배적이었다. 그러나 발전제어시스템에 윈도우 OS와 TCP/IP 통신 프로토콜의 적용이 확대되고 기반시설을 대상으로 한 국내외 다수의 사이버 침해사고가 발생하면서 발전제어시스템도 더 이상 보안에 안전하지 않게 되었다. 2013년부터 산업부 취약점 분석평가가 시행되는 등 국가 차원에서 발전제어시스템의 정보보안 관리가 이루어지면서 보안 취약점들이 많이 개선되었고 보안 수준과 인식도 크게 향상되었다. 그러나 발전소 운영 특성상 보안 취약점 조치로 인한 시스템 안정성이 입증되지 않는 경우 조치하지 못하고 고질적인 취약점으로 남아 발전제어시스템의 보안을 위협하고 있다.

발전소 현장 및 논문들에서도 이러한 문제를 해결하기 위해 테스트베드 구축 등의 기술적 시도와 개선 방안을 제시하고 있으나 발전제어시스템 담당자들이 IT관련 기술과 정보가 부족하고 시스템 운영 시 제작사에 대한 의존도가 높아 개선 시도가 싶지 않고 지속적이고 효과적인 대응에도 한계가 있었다.

Received(04. 22. 2024), Modified(05. 31. 2024), Accepted(05. 31. 2024)
† 주저자, onion818@naver.com
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

본 연구에서는 발전제어시스템의 보안 취약점 개선을 위한 대안으로 발전제어시스템의 보안 취약점과 개선사례 등에 대한 사이버보안 정보공유 모델을 제안하였다. 발전제어시스템의 사이버 보안 정보공유가 활성화된다면 발전소 보안 담당자들의 기술역량이 강화되고 보안 취약점에 대한 대응능력 향상으로 발전제어시스템의 보안 수준 향상에 기여할 것이다.

II. 연구설계 및 방법

본 논문에서는 발전제어시스템 사이버보안 정보공유 모델을 개발하여 발전제어시스템의 보안 취약점을 개선하고 사이버 위협에 효과적이고 능동적으로 대응하는 것을 목표로 다음 연구방법을 수행하였다.

첫째, 발전소 현장의 보안 취약점 개선 관련 선행연구를 분석하고 한계점과 개선 방향을 모색하였다.

둘째, 사이버 보안 정보공유 관련 국내외 법규 및 선행 연구를 통해 정보공유의 효과와 한계점 및 활성화 방안 등을 분석하였다.

셋째, 실제 운영 중인 다양한 정보공유 시스템을 조사하고 기존 시스템의 운영 현황과 장단점을 파악하고 개선 방향을 제시하였다.

넷째, 정보공유에 대한 문헌 및 사례연구 결과를 바탕으로 발전제어시스템의 특성을 고려한 정보공유 정책 수립과 시스템 개발 방향을 제안하였다.

다섯째, 기존 방법론 대비 제안모델의 효과를 비교평가하고 발전제어시스템 운영자들을 대상으로 설문조사를 실시하여 정보공유 효과를 예측하고 제안 시스템에 대한 실효성을 검증하였다.

III. 발전제어시스템 취약점 개선 선행연구

3.1 발전제어시스템 개요

3.1.1 발전제어시스템 개념

발전제어시스템은 전기를 생산하는 발전소에서 현장 설비의 제어 및 원격감시를 위해 사용되는 컴퓨터 기반의 시스템을 말한다. 현장 설비의 상태 및 동작 데이터를 콘트롤러가 수집·변환하여 네트워크 통신을 통해 서버 및 PC와 연결되어 현장 설비의 감시 및 운전을 수행한다. 아래 〔그림 1〕과 〔표 1〕은 발전제어시스템의 구성요소 및 기능을 보여준다.

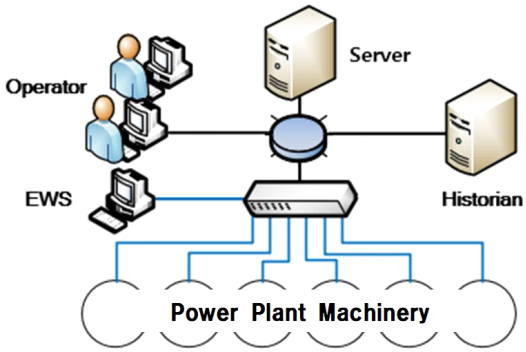

Fig. 1. Basic configuration diagram of power generation control system

Table 1. Main functions of each component in power generation control system

Component	Main function
Server	Overall operation control and management of power generation control system
Operator	Monitoring and operation control of machinery
Historian	Storage of operating rercords of machinery and trend analysis
Network Switch	Comunication linkage between components of power generation control system
Controller	Collention of analog/digital input/output signals fron power plant machinery
Power plant machinery	Boiler, turbine and other's status and operation sensors

3.1.2 발전제어시스템 보안동향 및 취약요소

발전제어시스템은 제작사 및 모델별로 고유의 통신 프로토콜을 사용하는 단독망으로 구성되어 있었으나 IT 기술의 발달에 따른 운영 편의성 및 구현 용이성 등의 이유로 점차 범용 네트워크 통신기술이 적용되고 있다. 이에 따라 발전제어시스템의 고유 취약점 외에 IT 보안 취약점이 더해져 사이버 보안에 취약할 수 있으며 주요 취약요소는 아래와 같다.

첫째, 발전제어시스템은 제작사 고유의 프로토콜을 사용하기 때문에 기술이 잘 공개되지 않아 보안 대응 방안을 수립하기에 한계가 있다.

둘째, 발전제어시스템은 정지 없이 장기간 운영되고 가용성을 우선시 하기 때문에 운영 중에 시스템

정지 등을 감수한 보안 취약 패치 적용이 어렵다.

셋째, 최신 보안패치가 발전제어시스템 프로토콜을 지원하지 않거나 오류를 야기 할 우려가 있어 시스템에 바로 적용하기 어렵다.

넷째, 회사 업무망에 발전제어시스템의 운전정보를 제공하기 위하여 망연계가 늘어나고 있어 발전제어시스템의 단독망 구성의 안정성을 위협하고 있다.

3.2 발전제어시스템 보안 취약점 관리현황

3.2.1 취약점분석평가 취약점 관리 현황

정보통신기반보호법 제9조(취약점 분석평가)에 의하여 국가안전보장, 행정, 국방, 통신, 에너지 등의 업무와 관련된 전기통신설비 및 컴퓨터 이용기술을 활용하는 전자적 제어 관리시스템의 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신시설에 대하여 매년 취약점 분석 평가를 실시하고 있다.

Table 2. Detailed vulnerability analysis and assessment criteria

Evaluation criteria	Specific Details
Manage -ment	Vulnerabilities in information security policy establishment and management
	Vulnerabilities in information security organization and personnel security
	Check on information security awareness and training
Physical	Monitoring and access control of critical information and communication infrastructure
	Physical inspection of support facilities (Power supply units, fire safety systems, etc.)
Technical	Vulnerabilities in unauthorized access by unauthorized users
	Vulnerabilities in information leakage and tampering
	Technical inspection for potential service delays and outages
	Windows and Linux Servers, PCs, Security Devices, Network Equipment, DBMS, Web, and Control Systems

과학기술정보통신부 고시 제2021-103호에 의해 발전소는 산업통상자원 사이버안전센터에서 관리(113개), 물리(18개), 기술(347개) 등 3개 분야 총 478개의 점검항목에 대하여 설비별로 취약점 분석평가를 받고 있다. 취약점분석평가의 항목별 세부 내용은 〔표 2〕와 같다

아래 〔그림 2〕는 A발전회사 3개 사업소의 취약점 분석평가 및 조치 결과를 도표로 분석한 결과이다. A발전회사는 2013년부터 매년 취약점분석평가를 실시하고 있으며 평가 초기 대비 보안 취약점이 다수 개선되고 보안 수준이 크게 향상되었다. 그러나 2018년부터는 점수 상승폭이 늘어나지 않고 비슷한 수준에서 정체되고 있음을 확인할 수 있다.

취약점분석평가 결과는 비공개 혹은 대외비로 관리되기 때문에 상세항목을 본 논문에 표기할 수는 없으나 윈도우즈 체제 PC의 주요한 취약점인 네트워크 공유나 보안패치 등에 관한 사항이라 사이버 위협 시 공격 통로를 제공할 수 있고 악성코드 유입 시 시스템 전체가 영향 받을 수 있어 취약점 조치 및 대응방안 수립이 필요하다.

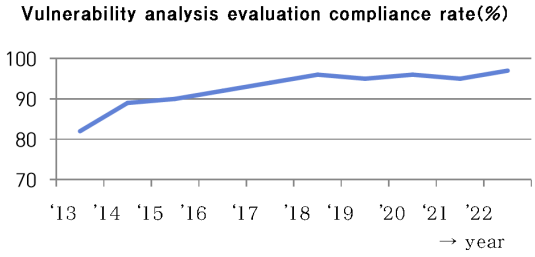

Fig. 2. Trend in compliance rate of vulnerability analysis and evaluation for power generation control systems

3.2.2 발전제어시스템 공개 취약점 관리현황

전 세계적으로 사이버 위협에 대응하기 위해 국가기관, 연구기관 및 제작사를 중심으로 제어시스템에 대한 공개 취약점 공유가 점차 확대되고 있다.

발전소도 내부적으로 지침을 수립하여 공개 취약점을 검색하고 보안패치를 수행하고 있다. 패치가 불가할 경우 중장기 계획을 수립하고 취약점을 관리하고 있다. 그러나 국내외 다양한 사이트에 실시간으로 올라오는 정보를 수동으로 검색하여 조치하기란 시간적으로도 기술적으로도 어려움이 따른다.

아래 〔표 3〕은 발전소에서 주로 참조하는 국내외

Table 3. List of cyber security public vulnerability sharing systems

Sharing system	Provided information
NCTI (National Cyber Threat Intelligence)	Cyber security threat, analysis, policy, and trend information
	Critical vulnerability requiring urgent action
	Vulnerability in domestic control system
	Vulnerability in exploited for hacking and recommendation
DHS ICS-CERT (Industrial Control Systems -Computer Emergency Response Team)	Warning, guideline regarding cyber security threat and vulnerability in control system and automation device
	Viewing vulnerability, security based on the manufacturer and system name
MITRE-CVE (Common Vulnerabili -ties and Exposures)	Providing standard identifier for security vulnerability and update
	Information on control system and software security vulnerability and update
	CVE Identifier, vulnerability, affected products and version, and reference URLs
System Manufac -turers	Notice on related information and security measures, when a manufacturer becomes aware of a vulnerability

주요 공개 취약점 공유 사이트 목록이다.

각 사이트에서 제어시스템 이름 및 버전별 주요 취약점과 대응방안 등의 정보를 확인할 수 있다. 그러나 취약점이 확인되어도 기술적 한계로 대부분 해소되지 않는 취약점으로 잔존하게 된다.

3.3 발전제어시스템 보안 취약점 개선을 위한 선행연구와 한계점

발전제어시스템의 장기 미개선 취약점을 개선하기 위하여 발전소 현장 및 다수의 논문에서는 테스트베드를 구축하여 취약점을 조치할 수 있는 방안을 제시하고 있다.

발전제어시스템과 프로그램 및 OS 등을 동일하게 구현한 TCP/IP 기반의 테스트베드 환경을 구축하고 발전제어시스템에 적용하기 전에 테스트를 실시하여 시스템 오류 및 영향도를 평가한 후 안전성이 확보되면 실제 시스템에 적용하는 방식이다.

아래 [그림 3]은 발전제어시스템 테스트베드 구성의 기본적인 예시이다. Controller의 입출력 전자카드의 값이 Network Switch를 통해 연결된 EWS(Engineering Work Station)에 의해 감시 및 제어된다. 테스트베드 환경에서 윈도우 기반의 서버인 EWS의 설정을 변경하여 실제 시스템에 미치는 영향도 및 안전성을 예측할 수 있다.

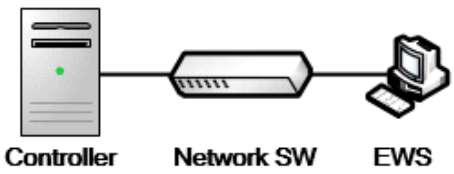

Fig. 3. Example schematic of a testbed setup

이러한 시도에도 불구하고 발전소 현장에서 고질적인 취약점이 개선되는 경우는 극히 드물고 여전히 제조사의 조치불가 공문 및 위험성 수용으로 대체되고 있다. 발전소 현장 및 논문들에서도 이러한 문제를 해결하기 위해 다양한 기술적 시도와 관리모델을 제시하였다.

2018년 이재명은 “산업제어시스템 보안취약점 제거 시 한계점 사례분석(패치적용 중심으로)”에서 실제 화력발전소의 보일러 주제어 시스템에 윈도우 보안 업데이트를 적용하는 실험을 진행하고 주요 취약점 제거를 위한 테스트베드 모델과 현업에서 수행가능한 기능시험 항목 등을 제시하였다[1].

2018년 곽민수는 “효과적인 발전제어시스템 취약점 관리모델”에서 공공기관 4개 사이트에서 운영 중인 제어시스템의 취약점 분석평가 결과를 기반으로 보안취약점을 분석하고 위험수용 방안 및 취약점 제거를 위한 시스템 업그레이드 등의 취약점 관리모델을 제안하였다[2].

현장 및 논문에서의 취약점 개선노력에도 불구하고 발전제어시스템의 보안 취약점 개선이 어려운 이유는 첫째, 많은 발전소 현장에서 발전소의 가용성을 해치지 않으면서 보안 취약점을 조치하기 위해 어떤 절차와 어떤 기술들을 고려해야 하는지 혼란스러워 하고 있다는 것이다. 발전제어시스템의 보안

취약점 개선은 현장 발전설비와 IT기술 양쪽 모두의 이해를 필요로 하지만 대부분의 발전소의 보안 담당자들은 전기 전공자들이기 때문에 IT관련 기술과 정보가 부족해서 보안개선에 어려움을 겪고 있다.

둘째, 보안에 대한 인식이 많이 개선되었다고는 하지만 여전히 전기의 안정적인 공급에 조금이라도 차질을 줄 수 있다면 보안은 고려대상에서 후순위로 밀리기 때문에 보안 담당자의 역할 수행 시 회사의 지원과 공감대 형성이 어렵다는 것 이다. 보안개선에 대한 안정성이 증명되고 가시적인 개선효과를 입증할 수 있는 선행사례의 공유가 아쉽다.

셋째, 발전제어시스템의 폐쇄적인 시스템 구성 특성 상 원제조사와 개발자에 대한 의존도가 크기 때문에 제조사에게 보안설정에 대한 확인을 요청하게 된다. 그러나 이미 시운전까지 모두 완료하고 시스템을 납품한 제조사의 추가적인 인력과 기술 투입을 이끌어내기는 쉽지 않다. 대부분의 제조사는 기술적 답변을 보류하고 책임을 회피한다. 다수 발전소의 개선 노력과 사례를 바탕으로 제조사에 보안 확인을 요청한다면 제조사의 적극적인 지원도 이끌어낼 수 있을 것이다.

발전소의 보안은 산업부의 취약점분석평가 등 정부와 발전소의 이행노력으로 상당부분 개선되었다. 이제는 고질적으로 해결되지 않는 취약점을 개선하고 보다 능동적이고 주체적인 보안개선이 필요한 시점이다. 본 연구에서는 그 대안으로 취약점 및 개선사례를 비롯한 발전제어시스템 사이버 보안 정보공유 모델을 제안한다. 국내외 사이버보안 정보공유 정책 및 연구결과와 실제 운영 중인 공유시스템 사례들을 분석하여 발전제어시스템의 특성에 맞는 정보공유 모델을 제시하였다. 이를 통해 발전소 보안담당자들의 기술역량이 강화되고 발전소 및 제조사의 보안 인식개선을 이루어 발전제어시스템의 보안 강화에 기여하기를 기대한다.

IV. 사이버 보안 정보공유 정책 및 사례연구

4.1 사이버 보안 정보공유 정책 및 가이드라인

사이버 위협에 대응하기 위해 최근 가장 주목받고 있는 대응책은 사이버 보안의 정보공유와 협력이다. 동시 다발적이고 대규모로 이루어지는 공격에 국가기관 및 기업이 단독으로 대응하기 어렵기 때문에 사이버보안 정보를 공유하고 협력하여 사전에 대응하는 것이 중요하다. 이에 우리나라를 비롯한 각 국가들은 국가 차원에서 법을 지정하고 다양한 공유시스템 운영을 지원하고 있으며 정보공유를 위한 국제표준과 가이드라인도 다양하게 제시되고 있다.

4.1.1 국내 사이버 보안 정보공유 정책

국내 다수의 국가 사이버 안보 법률에서 사이버 보안 정보공유에 관한 정책을 확인할 수 있다.

「정보통신기반보호법」 제16조(정보공유·분석센터) 항목에서 취약점 및 침해요인과 대응방안에 관한 정보를 제공할 수 있도록 정보공유 분석센터의 구축을 장려하고 있다[3].

「국가정보보안기본지침」 제8장 정보협력 항목에서는 각급기관·단체간 사이버위협정보의 체계적이고 효율적 공유를 위하여 정보공유시스템을 운영할 수 있도록 하고, 정보공유시스템 운영을 위한 준수사항 및 보안대책을 명시하고 있다[4].

또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 침해사고의 예방 및 피해 확산 방지를 위하여 사이버보안 취약점을 신고한 자에게 포상금을 지급할 수 있도록 하고 관련 절차를 대통령령으로 정하였다[5].

위 법령들은 사이버보안 정보공유의 중요성을 인지하고 국가적인 차원에서 지원 가능성을 열어뒀다는 점에서 의의를 찾을 수 있겠다. 그러나 관련 법안이 실효성을 가지기 위해서는 보다 구체적이고 상세한 절차를 수립해야 할 것이다.

4.1.2 해외 사이버 보안 정보공유 정책

미국, 유럽 및 일본 등 대부분의 선진국들도 우리나라와 같이 사이버보안 정보공유를 위한 정책적 기반 수립 및 활성화 법안을 운영하고 있다. 아래 [표 4]은 해외 사이버 보안 정보공유 법안이다.

미국정부는 사이버보안 정보공유법을 독립법안으로 발의하고 정보공유 기술 표준 개발과 공유에 따른 법적 책임 면책 등의 적극적인 참여 촉진 방안을 운영하고 있다. 유럽과 일본도 국가 차원에서 사이버보안 정보공유를 지원하고, 공공 및 민간 기관 간 사이버보안 정보공유를 법안으로 발의하였다.

Table 4. Laws on Cybersecurity Information Sharing in Major Countries

Country	Laws and Key Policies
United States	Cyber Information Sharing Act (CISA), established in 2015
	Establishment of a cyber threat information sharing system and procedures
	Development and standardization of cyber threat information representation and information specifications
	Voluntary information sharing and protection between private and public entities
	Exemption from civil and criminal liability resulting from sharing
EU (Euro -pean Union)	EU Cyber Security Strategy, established in 2014
	Establishment of a cyber security intelligence platform for sharing cyber threats and vulnerabilities
	Development of standards for cyber security information sharing and collaboration
	Promotion of collaboration across various sectors including private and public entities
	Development of automated information sharing and compatible sharing standards between systems
Japan	Basic Act on Cybersecurity, established in 2014
	National-level safe information exchange for responding to cyber attacks
	Operation of the Cyber Security Information Sharing Platform (J-CSIP) to facilitate information sharing and joint response to cyber threats between private and public entities

4.1.3 정보공유 가이드라인 및 국제표준

4.1.3.1 NIST SP 800-150

NIST(National Institute of Standard Technology)에서 발행한 SP 800-150(Guide to Cyber Threat Information Sharing)은 효과적인 사이버 위협정보 공유를 위해 정보공유 계획을 수립하고 구현 및 유지하는데 도움이 되는 가이드라인을 제시하고 있다. 주요 내용은 〔표 5〕와 같다.

NIST SP 800-150은 조직의 정보공유 목표를 수립하고 정보공유의 활동범위를 식별하여 적절한 정보공유 규칙을 수립할 수 있는 가이드라인을 제시하고 있다. 특히, 민감정보 및 개인정보 등 부적절한 정보공유로 인한 사고방지를 위한 노력과 위협정보의 출처를 추적 보존하여 공유정보 및 공유자에 대한 신뢰성을 확보하도록 하였다.

사이버 위협정보 공유를 위한 표준화된 데이터 형식과 전송 프로토콜의 개발 및 적용으로 위협 정보의 자동화 및 신속한 처리의 중요성을 강조하였다.

또한 정보공유 시스템에 새로운 취약점이나 보안 경고가 발생 시 경고의 심각성, 조직 내 영향을 받을 수 있는 시스템의 수량, 중요업무에 미칠 수 있는 영향 등을 고려하여 적절하고 신속한 대응을 할 수 있는 가이드라인까지 제시하고 있다.

NIST SP 800-150은 사이버위협 정보공유에 대한 개론부터 실제 현장에 적용 시 예상가능한 다양한 시나리오와 상황들을 고려하여 상세하게 가이드라인을 제시하고 있기 때문에 현장 적용 시 유용하게 활용될 수 있는 강점이 있다.

Table 5. Establishing and Participating in Sharing Relationships〔6〕

Establishing Sharing Relationships	Define Information Sharing Goals and Objective
	Identify Internal Sources of Cyber Threat Information
	Define the Scope of Information Sharing Activities
	Establish Information Sharing Rules
	Join a Sharing Community
	Plan to Provide Ongoing Support for Information Sharing Activities
Participating in Sharing Relationships	Engage in ongoing communication
	Consume and respond to security alerts
	Consume and use indicators
	Organize and store indicators
	Produce and publish indicators

4.1.3.2 ISO/IEC 27010

ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)에서 발행한 ISO/IEC 27010는 국가 인프라 산업 등과 같이 민감한 기밀정보의 공유 및 전송 시 보안을 강화하기 위해 개발된 국제표준이다.

ISO/IEC 27010은 공공 및 민간, 국내 및 국제, 동종 및 이종 산업 간의 민간정보교환에 대한 신뢰할 수 있는 정책 및 프로토콜을 제공하고 있다.

정상 상황을 비롯한 사이버 위기 상황에서도 정보의 안전한 공유와 주요 인프라를 보호하는 것을 목표로 아래 〔표 6〕과 같은 표준을 제안하고 있다.

Table 6. standard rules to prevent security issues when transferring confidential information〔7〕

standard rules	Exchanging information between organisations
	The risks of sharing knowledge
	Introducing controls to mitigate such risks
	Potential incidents which could occur

4.2 사이버 보안 정보공유 선행연구

사이버 보안 정보공유의 효과에 대한 기대감과 국가적인 차원에서의 관심이 높아짐에 따라 관련 연구 논문이 다수 존재하지만 발전제어시스템의 특성을 고려한 정보공유 연구는 전무한 상황이다. 국내외 다양한 사이버 보안 정보공유 논문을 분석하여 발전제어시스템에 효과적으로 적용할 수 있는 방안을 모색하고자 한다.

4.2.1 사이버 보안 정보공유의 필요성

동시 다발적이고 대규모로 이루어지는 공격에 국가기관 및 기업이 단독으로 대응하기 어렵기 때문에 사이버 보안 정보를 공유하고 협력하여 사전에 대응하는 것이 중요하고 효과적이다. 다양한 논문에서 정보공유의 필요성을 강조하고 있다.

2015년 윤오준은 “사이버공격 대응 분석을 통한 사이버안보 강화 방안 연구”에서 국내에서 발생한 주요 사이버공격 사례와 국가 종합대책을 분석하였다. 2009년 7.7DDoS 공격은 민관간 악성코드 등 관련 정보 공유 및 기관간 유기적 협력이 부족하였고 2013년 3.20 및 6.25 사이버테러는 민관군 유관기관 간 원활한 사이버위협 정보 공유체제가 미흡하였다고 분석하였다. 이러한 사이버공격을 계기로 국가 사이버안보 종합대책이 수립되고 정보공유의 중요성에 대한 인식도 많이 개선 되었지만 아직도 실시간으로 신속히 공유할 수 있는 정보시스템 구축 등의 체계가 부족하다고 지적하고 있다〔8〕.

2012년 고유미는 ‘개인정보 오남용 방지 및 보호를 위한 정보공유센터의 역할을 제안하며 정보공유의 중요성을 강조하였다. 정보공유시스템을 통하여 지식을 제공하고 재사용할 수 있다고 하였다. 특히 정보공유 활동은 개인 또는 별개의 조직에 내제된 정보를 전체적인 수준으로 확산시킴으로써 조직과 조직 간의 연결을 제공하고 경제적인 가치를 가져올 수 있다는 점에서 중요하다고 하였다〔9〕.

발전제어시스템의 경우 담당자가 대부분 전기나 기계 직군이라 IT 및 사이버보안 취약점 개선을 위한 지식과 기술의 한계를 가진다. 발전소 및 시스템 담당자 간 사이버보안 정보를 공유하고 협력할 수 있는 환경이 조성된다면 발전제어시스템의 전체적인 기술 수준이 향상되고 사이버 위협에도 효과적으로 대응할 수 있을 것이다.

4.2.2 사이버 보안 정보공유의 한계점과 활성화 방안

사이버 보안 정보공유는 대규모 사이버 위협에 대응할 수 있는 효과적인 대응안이지만 공유 데이터의 유출방지와 참여자들의 활발한 정보공유를 유도하기 위한 대책수립이 필요하다. 다양한 논문에서 이러한 정보공유의 한계점 극복과 활성화 방안에 대해 연구하였다.

2016년 이용균은 “지능적이고 자동화된 사이버 위협 정보 공유 모델 연구”에서 사이버 위협정보 공유가 구체적인 성과를 보이지 못하고 있는 이유로 기관별 시스템 차이로 인한 정보공유의 어려움과 대용량 데이터의 처리 및 자동화의 어려움, 민감 데이터 처리 문제를 들었다. 이를 극복하기 위해 법제의 정비, 민감 정보에 대한 관리대책과 참여유도 요소 개발을 위한 침해사고 신고 및 포상에 대한 개선안과 자동화된 정보 공유 체계를 위한 다차원 큐브 매트릭스 모델을 제안하였다〔10〕.

2017년 김하영은 “국내 사이버위협 정보 공유에 영향을 미치는 요인”에서 사이버 위협 정보 공유에 영향을 미치는 요인을 TOE(Technology Organi-zation Environment) 프레임 워크를 활용하여 법적책임, 자율화, 품질평가, 익명성, 최고경영자의 지원으로 나눈 뒤 분석하였다. 그리고 정보 공유 위반 사항에 대한 면책과 민간 정보 공유 시스템의 운영 그리고 공유되는 정보에 대한 평가 등이 정보공유에 영향을 미친다고 하였다[11].

2018년 박지백은 “사이버 위협 정보의 공유 활성화 방안”에서 표준화와 공유 체계 장벽제거, 정보 공유에 대한 보상 체계, 정보 평가 시스템의 구축 등이 영향을 미치고, 정보별 등급을 식별하고 정보 공유 기관별 보상 체계를 마련하는 것이 정보 공유 활성화에 영향을 줄 수 있다고 하였다[12].

2016년 김애찬은 “효과적인 사이버위협 정보공유 체계 수립을 위한 요구사항의 우선순위 도출에 관한 연구”에서 사이버 위협 정보 공유 체계 수립 시 확인되는 정책적 요구 사항과 기술적 요구사항에 대해 AHP 분석방법을 이용하여 우선순위를 도출하였다. 연구에 따르면 정책적 요구사항이 기술적 정책사항보다 중요한 것으로 확인되었으며, 정책적 요구사항에서는 법적근거의 마련과 정보 관리체계 마련이 중요하다고 하였다. 기술적 요구사항의 경우 정보의 표현 방식, 전송규격 표준화와 정보 수집 방법, 신뢰성의 개선이 중요한 요인이라고 하였다[13].

4.3 사이버 보안 정보공유 사례연구

국내에서 기존에 운영 중인 사이버 위협 정보공유 시스템들의 운영사례를 분석하여 기존 시스템의 장단점을 파악하고 발전제어시스템에 적용 가능한 모델을 제안하고자 한다.

4.3.1 사이버보안 정보 공유시스템 운영현황

사이버보안 관련 다양한 정보공유 시스템이 운영되고 있으며 시스템별로 공유정보의 수준 향상과 회원사의 참여도를 높이기 위해 노력하고 있다. 공공기관 및 민간기관 간 사이버 위협정보 공유와 협력도 확대되고 있다.

공공분야의 사이버보안 정보 공유시스템으로는 국가정보원에서 운영 중인 NCTI(National Cyber Threat Intelligence)가 있으며 최근 KCTI (Korea Cyber Threat Intelligence)를 개발하여 민간에도 주요 보안정보를 공유하고 있다. 공공기관 420개, 민간기업 170개가 참여하여 약 40만건의 사이버위협 정보를 공유하고 있다.

민간분야는 한국인터넷진흥원의 C-TAS(Cyber Threat Analysis & Sharing)가 대표적이며 공공기관의 주도하에 민간 기업들의 사이버보안 정보 공유를 수행하고 있다. 최근 한국인터넷진흥원은 사이버 보안 취약점 정보 포털을 개발하여 국내외 보안 취약점 및 제조사의 보안패치 정보를 통합하여 사용자가 쉽고 빠르게 정보를 검색하고 조치할 수 있는 서비스를 제공하고 있다. 제조사의 보안 소프트웨어 패치 정보, 국내외 보안 취약점 정보 등 약 20만건 이상의 정보를 제공하고 있다. 특히 가상의 기업환경에서 화이트 해커를 통해 자사의 보안 취약점을 점검할 수 있는 핵더챌린지와 취약점 신고 포상제인 버그바운티를 운영하는 등 정보공유 참여 확대를 위해 노력하고 있다.

ISAC(Information Sharing & Analysis Center)은 정부 주도하에 회원사 간 사이버테러 대응 정보를 공유하는 시스템이다. 정보통신, 금융, 에너지, 의료 등 분야별로 사이버 위협 정보를 분석하고 배포하는 등의 공동 대응으로 신속한 대처가 가능하고 비용을 절감하고 있다. 국내 뿐만 아니라 미국, 영국, 일본 등 타 국가와의 연계도 강점이다.

CTA(Cyber Threat Alliance)는 글로벌 보안 기업들이 사이버 위협에 공동으로 대응하는 민간 플랫폼이다. 회원사가 매일 의무적으로 제출하는 위협 정보를 클라우드 플랫폼을 통해 취합, 분석하고 정보를 공유하고 있다. 정보의 수준이 높고 제공 정보의 가치 및 양에 따라 상이한 접근 권한을 주고 있다.

이외에도 OSINT(Open Source Intelligence)는 공개 출처 정보를 이용하여 사이버 위협정보를 수집하여 정보를 제공하고 있다. 인터넷, 온라인 상용정보, 데이터베이스 등의 다양한 매체를 이용하고 있다. 정보의 신속성과 접근성 측면이 유리하여 수평적인 정보확산에 기여하지만 정보양이 지나치게 많고 허위정보의 판별이 필요하기 때문에 신뢰성은 다소 떨어진다.

발전제어시스템은 발전소 등 특정 기관에서만 사용되기 때문에 ISAC이나 CTA처럼 비슷한 분야의 기관 간 사이버보안 정보공유 환경을 조성하는 것이 정보 유출에 대비하고 공유정보의 수준을 향상시키는데 효과적일 것 으로 판단된다. 또한 기존 NCTI,

C-TAS와 같은 공신력 있는 공유시스템과 연계한다면 시스템 구현의 효율성과 신뢰성을 높일 수 있을 것 이다. 마지막으로 사이버보안 정보공유 포털의 신고 포상제도인 버그바운티처럼 다양한 참여 확대방안 및 포상정책을 실시하여 정보공유 활성화와 사이버보안 인식개선을 이끌어내야 할 것이다.

4.3.2 정보 공유시스템의 한계점 및 개선방향

위와 같이 공공 및 민간분야에서 다양한 사이버보안 정보 공유 시스템이 개발되어 운영 중 이지만 실제 현장의 기업 보안 담당자의 만족도나 활용도는 높지 않아 개선이 필요하다.

2020년 한국인터넷진흥원은 기업 보안담당자들의 위협정보 및 보안 트랜드 수집처 등을 알아보기 위하여「위협정보 및 보안 트랜드 수집처」설문조사를 실시하고 결과를 2020년 4분기「사이버 위협 동향 보고서」에 등재하였다. 보고서에 따르면 한국침해사고대응팀협의회 73개 회원사의 기업 정보보호 및 보안 실무자를 대상으로 한 설문조사 결과, 수집 위협정보에 대해 매우만족과 만족은 약 30%에 그치고 나머지 약 70%는 보통이나 부족하다고 응답하였다. 정보의 취합이 어렵고 수집된 정보를 내부 환경에 적용하기 어렵다는 의견이 많았다.

아래 〔그림 4〕는 수집 위협정보 만족도에 대한 설문조사 차트이고 〔표 7〕은 수집 위협정보에 대한 만족도가 낮은 이유에 대한 주요 응답이다.

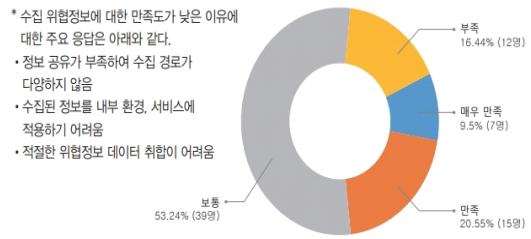

Fig. 4. Data Collection Threats Satisfaction〔14〕

Table 7. Reasons for low satisfaction with data collection threats〔14〕

Reasons for low satisfaction	The lack of information sharing and diverse data collection paths
	Challenges in applying collected information to internal environment and services
	The difficulty of adequately collecting threat intelligence data
	The challenge of selectively incorporating abundant threat intelligence data
	The insufficiency of tailored, up to date threat intelligence

이상 사이버보안 정보공유에 대한 선행연구와 기존 운영 시스템의 운영사례 등을 분석한 결과를 바탕으로 정보공유 활성화 방안을 정책과 기술적 측면으로 나누어 종합해보면 〔표 8〕과 같다.

Table 8. Measures to Enhance Cybersecurity Information Sharing

Category	Promotion Measures
Policy Domain	Establishment of legal basis and procedures for information sharing
	Encouragement of participation from various public and private institutions
	Exemption from civil and criminal liability for sharing cyber security information
	Compensation for information sharers and reporters
Technological Domain	Development of secure communication technologies for information sharing
	Automation of large-scale data processing
	Development of data processing technologies for classified information, etc.
	Provision of tailored, up-to-date information is crucial
	Evaluation of shared information and identification of information ratings

V. 발전제어시스템에 적용 가능한 사이버 보안 정보공유 모델제안

앞 장에서는 발전제어시스템의 운영 특성과 사이버보안 정보공유 관련 정책 및 시스템 운영사례에

대해 연구하였다.

본 장에서는 선행 연구와 정책, 가이드라인 및 사례 등을 바탕으로 발전제어시스템의 보안 취약점을 개선하고 사이버 위협에 대응할 수 있는 발전제어시스템에 특화된 사이버보안 정보공유 모델을 제안하고자 한다.

다음과 같이 크게 기술적 방안과 정책적 방안으로 구분하여 발전제어시스템의 사이버 보안 정보공유 모델을 구현하였다.

- (정책분야) 발전제어시스템 정보공유 정책수립 및 활성화 방안
- (기술분야) 발전제어시스템 사이버보안 정보공유 시스템 구현

5.1 발전제어시스템 정보공유 정책 수립 및 활성화 방안

발전제어시스템을 운영하는 한국전력 자회사인 발전회사는 조직문화 및 시스템 운영에 있어서 상당히 폐쇄적이고 보수적이라 새로운 정책의 수립 및 적용이 어렵다.

발전제어시스템의 사이버보안 정보공유 활성화를 위해서는 사이버보안 관련 상위법과 제도를 구체적이고 실효성있는 방향으로 개선하여 발전소 현장의 자발적이고 적극적인 참여를 이끌어내야 한다.

5.1.1 사이버보안 정보공유 법·제도 개선

우리나라는「정보통신기반보호법」,「국가정보보안기본지침」등의 법안에서 사이버보안 정보공유를 다루고 있다. 그러나 법안이 곳곳에 산재되어 있고 정보공유를 권고한다는 수준으로 짧게 언급만 되어있어 실제 시스템 현장에 적용 시 참조하기 어렵고 실효성이 떨어지므로 법률의 재정비가 필요하다.

첫째, 공공 및 민간 기관 별로 공유할 수 있는 사이버보안 정보의 범위를 규정하고 정보 공유 절차와 방법에 대한 명확한 가이드라인 제시가 필요하다. 과거 사이버보안 분야는 정보유출 방지가 중요했기 때문에 산업현장에서는 정보공유에 대한 개념자체가 생소할 수 있기 때문에 국가가 법과 제도를 통해 안내하여 혼란을 줄이고 공감대를 형성해야 한다.

둘째, 사이버보안 정보공유 및 공유센터 설치 등에 관하여 권고를 넘어서 의무사항을 포함하고 적극적인 참여시에는 적절한 인센티브를 지급하여야 한다. 또한 정보공유로 인한 불이익이 발생하지 않도록 해야 한다. 미국의 사이버보안 정보공유법(CISA)의 경우 자발적인 참여를 유도하기 위하여 공유에 따른 민형사상의 책임을 면책하였다. 우리나라도「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보보호 취약점 신고자에 대한 포상을 명시하고 있지만 미국의 경우처럼 상세한 절차와 기준을 제정해야 실효성을 높일 수 있을 것 이다.

셋째, 사이버보안 정보공유 기술규격 표준 개발과 관련 정책 배포를 법안으로 명시하고 국가 정책 수립과 기술지원이 필요하다. 산업현장에서는 국내외 수많은 사이버위협 정보 공유 시스템의 정보를 식별하고 대응하기에 인력 및 기술적으로 한계가 있다. 국가가 선도적으로 정보공유 기술 표준과 시스템 개발의 기반을 만들어 민간분야까지 확대될 수 있도록 법적 근거를 마련해야 한다.

5.1.2 발전제어시스템 정보공유 정책 및 활성화방안

발전제어시스템의 정보공유 활성화 방안은 다음과 같다.

첫째, 발전제어시스템을 운영하는 발전회사와 개발자인 제조사의 적극적인 참여를 유도하여야 한다. 현재는 정보공유에 대한 의무성이나 실질적인 혜택이 없기 때문에 발전회사나 제조사 모두 사이버 위협 정보와 공유에 적극적인 대응을 하지 않고 있다. 발전회사는 산업부 및 국정원의 사이버보안 점검 결과가 기관평가에 반영되므로 사이버보안 정보공유를 위한 시스템 개발 및 성과를 기관 평가항목에 추가하여 참여를 이끌 수 있다. 또한 민간기업인 제조사의 참여를 높이기 위해서는 발전제어시스템의 사이버보안 정보공유 및 개선 실적만큼 향후 입찰 시 계약 가점을 부여하고 실질적인 보상을 해줘야 한다.

둘째, 비공개 정보공유에 대한 제약사항을 검토하고 시대적 흐름을 반영하여야 한다. 시대와 사회적인 변화에 따라 정보의 공개를 통해 잃게 되는 가치와 얻게 되는 효과에 대한 비교가 필요하다. 지속적이고 대규모로 이루어지는 최근의 사이버 위협 공격에 대응하기 위해서는 예상 되어지는 보안 취약점들을 감추기보다는 현장 개선사례와 기술정보를 공유하여 취약점을 해소하는 것이 더 효과적일 것 이다.

셋째, 발전제어시스템의 수많은 보안 취약정보 중에서 신뢰할 수 있는 최신의 맞춤 정보를 선별하고

관리할 수 있는 방안을 수립하여야 한다. 정보공유를 의무화 하거나 실적위주의 정책이 되면 공유정보의 수준이 저하될 수 있으므로 정보에 대한 평가 프로세스를 정립하여야 한다.

넷째, 발전제어시스템의 사이버보안 취약점 및 관련 정보는 대부분 비밀정보에 속하므로 암호화 등 데이터 유출방지 대책을 수립하고 정보 송수신 시 안전한 통신 프로토콜을 사용하도록 국가의 정책 및 기술적 지원이 필요하다.

5.2 발전제어시스템 사이버보안 정보공유 시스템 구현

발전제어시스템의 사이버 위협정보를 효율적으로 수집하고 취약점 개선사례 등에 대한 기술정보의 공유와 기술교류가 가능하도록 발전제어시스템 사이버보안 정보공유 시스템 개발을 제안한다.

자산관리 시스템과 취약점 수집 시스템을 결합하여 최종적으로 발전제어시스템 사이버보안 정보공유 통합시스템 개발을 제안하며 주요 프로세스는 〔그림 5〕와 같다.

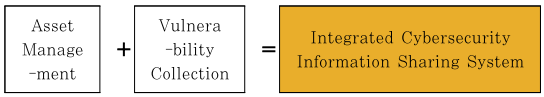

Fig. 5. System development process

5.2.1 발전제어시스템 자산관리 시스템 개발

발전제어시스템 사이버보안 정보공유 시스템 구현의 첫 단계는 발전제어시스템 자산관리 시스템의 개발이다. 자산이 정확하게 파악되고 관리되어야 사이버 위협정보 및 보안 취약점 등의 정보를 매칭하고 신속하고 효율적으로 대응할 수 있다.

현재 대부분의 발전소는 PC, 네트워크 스위치 및 Programmable Logic Controller(PLC) 등의 수많은 자산들을 수기로 관리하고 있어 정보의 누락과 업데이트 및 관리가 어렵다.

발전제어시스템 자산관리 시스템을 구현하면 설비 및 자산정보를 시스템에 입력하고 변동사항이 발생하였을 경우 실시간으로 정보의 업데이트가 가능하다. 또한 자산 별 통합관리도 유리하다.

자산정보에는 IP 등 주요 시스템 정보가 포함되기 때문에 정보 유출을 방지하기 위하여 시스템 및 사용자 별 권한을 분리해서 지정된 담당자만 해당 자산 및 취약점 관리를 수행 할 수 있도록 한다. 아래 〔표 9〕 은 자산관리시스템의 자산정보 입력예시이고 〔그림 6〕은 자산관리시스템의 개념도이다.

Table 9. Asset Information Input Example

Facilities	*(sample) Subject heading*
Host	*EWS*
Manufacturer	*EMERSON*
Model	*OVATION*
Version	*1.2.1*
IP	*10.10.10.10*
OS	*Window 10*
Implementation time	*'24.4.10*
Responsibility	*Gil-dong Hong*

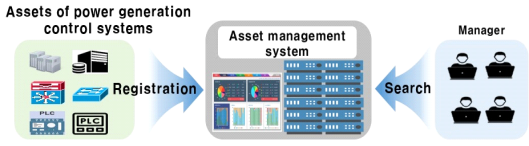

Fig. 6. Asset Management Overview

5.2.2 발전제어시스템 사이버보안 취약점 수집 시스템 개발

발전제어시스템 사이버보안 취약점은 수집 방법 및 내용에 따라 현장점검 취약점과 공개 취약점으로 구분할 수 있다

5.2.2.1 현장점검 취약점 수집

발전제어시스템은 매년 산업부「주요정보통신기반시설 취약점 분석 평가 기준」에 따라 관리(113개), 물리(18개), 기술(347개) 등 3개 분야 총 478개 항목에 대해 현장 보안점검을 받고 취약점을 관리하고 있다. 또한 국정원의「기반시설 보호대책 이행여부 확인」의 31개 항목에 대해 국정원 개발 취약점 점검툴(N-Checker)을 활용하여 보안점검과 취약점 관리를 수행하고 있다. 이렇게 현장점검을 통해 직접 수집한 취약점 정보 및 개선결과 등을 시스템

에 입력하여 DB화하여 관리한다면 수많은 자산 별 취약점 정보의 검색 및 이력 관리를 효율적으로 할 수 있을 것 이다.

특히 운영 중인 시스템의 보안 취약점 개선사례와 운영기술을 입력하면 동일 시스템을 운영하고 있는 타기관 담당자도 해당 기술내역을 참조할 수 있도록 구현함으로써 발전제어시스템 사이버보안 기술교류가 가능해질 것 이다. 정보를 공유한 기관 및 담당자에게 가점을 부여하거나 적절한 포상을 실시하는 등의 참여 촉진 정책도 병행되어야 할 것 이다.

현장점검 취약점 수집 정보의 입력은 수동 업로드 방식을 권고한다. 발전제어시스템과 연동된다면 자동으로 실시간 취약정보를 수집할 수 있겠지만 발전제어시스템의 운영특성상 단독망 구현이 중요하기 때문에 주기적으로 혹은 업데이트 상황이 발생할 시 수동으로 업로드 하도록 한다.

5.2.2.2 공개 취약점 수집

발전제어시스템의 공개 취약점 및 보안패치 등에 대한 정보는 전세계 취약점 정보공유 포털 및 발전제어시스템 제조사 홈페이지 등 에 공개되고 있다. 실시간으로 업데이트 되는 수많은 정보를 발전제어시스템 담당자가 일일이 확인하기는 힘들다. 발전제어시스템 자산의 정보와 매칭되는 취약점이 웹사이트에 공개되면 자동으로 정보를 수집할 수 있도록 구현하고 정보의 중요도, 영향력 등을 고려하여 분류하고 실시간으로 정보를 제공할 수 있어야 한다.

외부 사이트에서 공개 취약점을 수집하기 위해서는 외부와의 안전한 통신 채널을 구축하고 수집 데이터의 처리와 관리 등 다양한 기술 개발이 필요하다. 아래 〔표 10〕은 한국인터넷진흥원에서 공개한 정보공유 시스템 구축 상세기술로 발전제어시스템 사이버보안 공유시스템 구축 시 참조 가능한 다양하고 유용한 기술을 포함하고 있다.

아래 〔그림 7〕은 발전제어시스템 사이버보안 취약점 수집시스템 개념도 이다. 발전제어시스템의 운영특성을 고려하여 현장점검 내부취약점은 수동으로 업로드 하고 외부 공개 취약점은 자동으로 실시간으로 수집 및 업로드 할 수 있도록 구현하였다. 수집된 취약점 정보는 자산관리시스템과 연동된다.

Table 10. Cyber Threat Intelligence Automatic Collection Technology〔15〕

Classifi -cation	Detailed Technology
Automatic Collection based on Feed/Crawling	Development of technology for collecting known cyber threat information based on C-TAS and other feeds
	Gathering OSINT information from websites, blogs, newspapers, etc., using crawling techniques.
	Development of technology for managing the history/statistics of collected information
	Development of technology for automatically collecting associated/supplementary information related to collected cyber threat data
	Construction of an active collection channel management platform based on virtualization technology
NoSQL Data Managem -ent Platform for Large -scale Collection Data	Construction of a NoSQL-based data management platform for processing large volumes of data
	Establishment of databases and development of information management processes for handling large data volumes
	Development of methods for managing the history of duplicate collection information and handling duplicate data
	Design and construction of an architecture for distributed storage and processing/manage -ment of large volumes of data

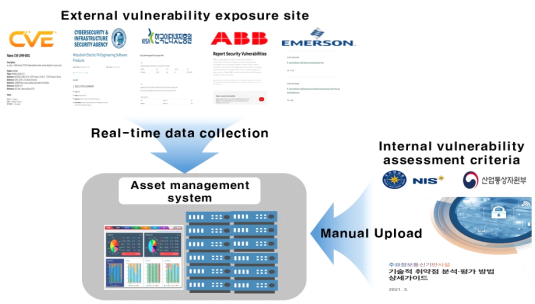

Fig. 7. Vulnerability Collection System Overview

5.2.3 발전제어시스템 사이버보안 정보공유 통합시스템 개발

발전제어시스템 자산관리시스템과 사이버보안 취약점 수집 시스템을 통합하여 최종적으로 발전제어시스템 사이버보안 정보공유 통합시스템 개발을 제안하고 개념도는 아래 [그림 8]과 같다.

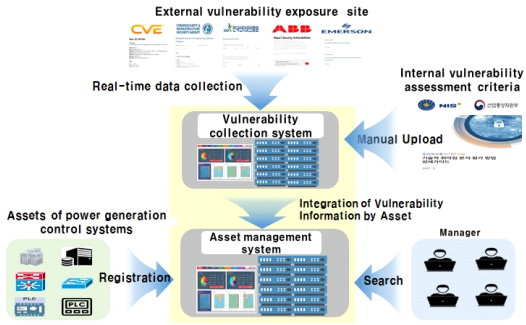

Fig. 8. Cyber security information sharing integration overview

발전제어시스템 사이버보안 정보공유 통합시스템은 발전제어시스템을 운영하는 전력회사(한국수력원자력, 발전회사 등)와 발전제어시스템 제조사 등을 회원으로 구성하여 웹 방식의 포털로 구현한다.

사용자(발전제어시스템 담당자)는 자산정보를 자산관리 시스템에 입력한다. 자체 점검 취약점 결과와 외부 사이트에서 수집한 공개 취약점이 자산관리 시스템과 연동되고 웹 포털을 통해서 실시간으로 자산 별 취약점 정보를 검색하고 열람할 수 있다.

사용자가 사이버 보안 취약점의 개선사례를 웹 포털에 입력하면 기관 및 개인에게 인센티브가 부여된다. 공유된 개선사례와 기술정보는 동일 시스템을 운영하고 있는 다른 사용자에게 제공되어 보안 취약점 개선 시 활용될 수 있을 것이다.

발전제어시스템은 국가기반시설이기 때문에 사이버 위협에 관한 기밀정보를 공유하기 위해 NIST의 SP 800-150(Guide to Cyber Threat Information Sharing) 및 ISO/IEC 27010과 같은 국제 표준을 참조하여 시스템을 구현할 수 있다. 특히, NIST의 SP 800-150은 사이버 위협 정보공유에 대한 개념부터 실제 현장에 적용가능한 다양한 시나리오 별 정보공유 가이드라인을 제시하고 있기 때문에 현장 적용 시 유용하게 활용될 수 있다. 가이드라인을 참조하여 정보공유를 위한 안전한 통신채널을 구축하고 최신의 정확한 정보를 수집, 분류한다. 또한 사용자 별 접근권한을 명확히 분리하고 설비 및 자산정보 변경 등에 대한 로그저장과 이력관리 기능으로 주요 정보의 유출을 방지해야 한다. 향후 다양한 보조 및 편의기능을 개발하고 지속적인 피드백과 참여유인 정책을 펼쳐 나간다면 발전제어시스템 보안관리 수준향상에 기여할 것이다.

VI. 제안보델 평가

6.1 기존 방법 대비 개선 사항

발전제어시스템의 보안 취약점 개선을 위해 발전소 현장 및 다수의 논문에서 테스트베드 구축을 통해 시스템 영향도를 확인하고 조치하는 방안을 제시해왔다. 해당 기술은 발전소 설비 운영과 IT 및 사이버보안 기술에 대한 전반적인 이해를 필요로 하고 몇 개월에서 몇 년에 걸친 검증기간을 거치기 때문에 그 가치가 크다. 그러나 관련 정보 및 기술을 공유할 수 있는 환경이 조성되어 있지 않아 대부분 일회성 시도로 끝나고 발전소 및 제작사의 지원을 이끌어 내기에도 한계가 있었다.

이에 본 논문에서는 보안 취약점을 자동으로 수집 관리하고 보안 취약점 개선사례와 기술정보를 공유할 수 있는 모델을 제안하였다. 제안모델을 통하여 사이버 보안 취약점을 신속하게 인지하고 대응할 수 있다. 또한 타사의 보안 취약점 개선사례와 기술정보의 교류를 통해서 담당자들의 역량이 강화될 것이다. 이를 통해 사이버보안 개선에 대한 공감대가 형성되고 미개선 취약점들의 개선실적이 크게 향상될 것으로 기대한다. [표 11]에서 보안취약점 관리를 위한 기존방법과 제안방법을 비교하였다.

Table 11. Comparing methods of security vulnerability management

Category	Existing Method	Proposed Method
Vulnera-bility Collec-tion	Cyber threat information manual search	Automatic collection and classification
	Difficulty in identify and respond promptly	Real-time notification and action

Category	Existing Method	Proposed Method
	Long collection time and high probability of omission	Significant reduction in collection time and minimal omission
Vulnera-bility Action	High dependence on manufacturers	Sharing of case studies on vulnerability remediation
	Lack of IT/ cybersecurity knowledge	Enhancement of system manager capabilities
	Individual construction of testbed to verify facility impact	Active support from power plants and manufacturers
	Lack of technology dissemination and exchange	Cyber threat collaborative response

6.2 사이버보안 정보공유 설문조사 결과

A발전회사 5개 사업소의 제어시스템 및 보안 담당자(30명)을 대상으로 설문조사를 실시하고 사이버보안 정보공유에 대한 사전인식과 제안모델에 대한 예상효과와 보완점을 확인하였다.
(조사기간 : 2023.12.4. ~ 12.22)

1. 현재 귀하 기관에서 운영하는 발전제어시스템의 보안수준을 어떻게 평가하십니까?

상당히 취약	다소 취약	보통	양호	우수
2	6	11	10	1

2. 발전제어시스템의 일부 취약점이 개선되지 못하는 이유는 무엇인가요? (중복가능)

시스템 운영특성	기술 및 정보부족	제조사 비협조	정보보안 관심부족	기타
12	15	3	18	1(인원)

3. 발전제어시스템 사이버보안 업무수행 시 기술교류에 대한 필요성을 얼마나 자주 느끼나요?

필요 없음	다소 필요	보통	가끔	자주
1	2	14	10	3

4. 사이버보안 정보공유를 발전제어시스템에 적용 시 효과가 있을 것으로 생각하십니까?

1(효과없음)	2	3	4	5(효과많음)
1	5	23	1	-

5. 발전제어시스템 사이버보안 정보공유 시 어떠한 정보가 공유되면 좋을 것 같습니까? (중복가능)

공개 취약점	보안 취약점	시스템 관리기술	네트워크 관리기술	기타
6	20	8	8	-

6. 발전제어시스템 사이버보안 정보공유 시 가장 우려되는 점은? (중복선택 가능)

정보유출	악성코드	효과성	업무량 증가	기타
9	7	10	4	-

7. 발전제어시스템 사이버보안 정보공유 활성화 방안은? (중복가능)

정책 의무화	공유시스템 개발	홍보	금전 등 혜택	기타
19	5	3	15	2(교육)

8. 발전제어시스템 사이버보안 정보공유 시 받고 싶은 혜택은? (중복가능)

금전	기관가점	개인가점	포상	기타
11	7	9	3	-

설문을 통하여 발전제어시스템 및 사이버보안 담당자 대부분이 실제 업무를 수행하면서 정보와 기술의 공유에 대한 부족을 느끼는 것으로 나타났다. 그러나 막상 사이버보안 정보공유 시스템의 활용에는 정보유출 등으로 부담을 느끼거나 관심이 크지 않았다. 이 논문을 계기로 발전제어시스템에 사이버보안 정보공유에 대한 긍정적인 인식과 관심이 증가되고 정보공유 시스템의 적극적인 활용으로 발전제어시스

템의 보안관리 수준이 향상되기를 기대한다.

VII. 결 론

발전제어시스템의 유지보수와 정보보안 업무를 수행하면서 고질적으로 해결하지 못하는 취약점에 대한 기술적 한계와 아쉬움이 항상 있었기 때문에 실제 현장에서 적용할 수 있는 발전제어시스템의 보안 취약점 개선을 위한 제도적 그리고 기술적 방안에 대한 조사와 연구를 진행하였다.

발전제어시스템의 보안 취약점 개선을 위한 선행연구의 한계점을 분석하고 대안으로 사이버보안 정보공유모델을 제안하였다. 발전제어시스템의 운영특성을 파악하고 사이버보안 정보공유정책, 실제 구현사례들을 분석하여 발전제어시스템에 효과적으로 적용할 수 있는 정책과 기술방안을 제시하였다.

사이버보안 정보공유는 가장 주목받는 사이버위협 대응책 중 하나이지만 발전제어시스템의 폐쇄적인 운영특성으로 현장에 적용하기가 쉽지 않기 때문에 그 해결방안과 효과성을 위주로 논문을 작성하였다. 그러다보니 공유 시스템 운영을 위한 상세기술은 상대적으로 간략하게 다루었음을 유의하기 바란다.

향후 기회가 된다면 구체적인 시스템까지 구현하여 개발과정에서 도출되는 점을 보완하고 실질적인 효과까지 측정해보고 싶다.

과거 사이버보안은 얼마나 잘 감추고 있는지가 초점이었다면 이제는 얼마나 잘 대응하는지가 중요해졌다. 발전제어시스템의 대규모 사이버위협에 맞서기 위해서는 국정원, 발전소, 제조사 등 유관기관의 협력과 공동대응이 중요하다는 인식이 보다 확대되길 바란다. 이 논문을 계기로 발전제어시스템의 사이버보안 정보공유 연구가 보다 활성화되고 발전제어시스템의 보안강화와 사이버위협 대응을 위한 다양한 접근방식의 연구들이 나오길 기대해본다.

References

[1] Jae-myeong Lee, “Security vulnerability management in Industrial Control System(ICS) environment and its limitations : focus on secyrity patching”, Graduate School of Information Security, Korea University, Dec. 2018

[2] Min-su Gwak, ″Effective Vulnerability Management Model for Power Plant Control Systems,″ ,Graduate School of Information Security, Korea University, Dec. 2018

[3] National Law Information Center, ″Information and Communication Network Protection Act,″ Chapter 4, Protection and Response to Incidents of Key Information and Communication Infrastructure, Article 16 (Information Sharing and Analysis Center), June 2022.

[4] National Law Information Center, ″Guidelines for National Information Security,″ Chapter 8, Information Cooperation, p114, January 2023.

[5] National Law Information Center, ″Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.,″ Article 47-6 (Rewards for Reporters of Information Protection Vulnerability).

[6] NIST SP 800-150 “Guide to cyber Threat Information Shaaring”, October 2016

[7] ISO/IEC ISO 27010:2015 “Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications”, November 2015

[8] Yoon Oh Jun, Bae Kwang Yong, Kim Jae Hong, Seo Hyung Jun, Shin Yong Tae, “A Study on Measures for Strengthening Cybersecurity through Analysis of Cyberattack Response”, Convergence Security Journal, vol.15, issue.4, p71-78, June 2015

[9] Yumi Ko, Jaewon Choi, Beomsoo Kim, “Protecting Individuals from Secondary Privacy Loss using Breached Personal Data Information Center”, Journal of the Korea

Institute of Information Security and Cryptology, vol.22, no.2, p391-400, April 2012.
〔10〕 Yonggyun Lee, "Research on an Intelligent and Automated Cyber Threat Information Sharing Model," Graduate School of Information Security, Korea University, Dec 2016.
〔11〕 Ha-Young Kim, Tae-Sung Kim, "Factors that Affect Sharing Cyber Threat Information in South Korea", Journal of the Korea Institute of Information Security and Cryptology, vol.27, no.5, p1167-1188, Dec 2017.
〔12〕 Park Jiback, Choi Byunghwan, Cho Haksu, "Activation Measures for Cyber Threat Information Sharing", Korean Journal of Communications, vol.35, no.7, p41-48, June 2018
〔13〕 Kim Aechan, Lee Donghoon, "Study on Deriving Requirements Priority for Establishing Effective Cyber Threat Information Sharing System," Journal of the Korea Institute of Information Security and Cryptology, vol.26, no.1, p61-67, Feb 2016.
〔14〕 Korea Internet & Security Agency, Cyber Threat Trends Report for the 4th Quarter of 2020, Survey Results on Threat Information and Security Trends, p28.
〔15〕 FFinal Report on Cyber Threat Intelligence (CTI) and Information Sharing Technology Development for National-level Incident Response, Korea Internet & Security Agency, 2020

〈저자소개〉

민 호 기 (Hogi Min) 정회원
2004년 2월: 광운대학교 전자정보통신공학과 학사
2022년 9월~현재: 고려대학교 정보보호대학원 석사과정
2007년 1월~현재: 한국남동발전 근무
〈관심분야〉 제어시스템 보안, 사이버보안 정보공유

이 중 희 (Junghee Lee) 종신회원
2000년 2월: 서울대학교 컴퓨터공학과 학사
2003년 2월: 서울대학교 컴퓨터공학과 석사
2013년 2월: 조지아 공과대학교 전기 및 컴퓨터 공학 박사
2003년 3월~2008년 8월: 삼성전자 연구원
2014년 8월~2019년 1월: 텍사스대학교 샌안토니오캠퍼스 전기 및 컴퓨터 공학부 교수
2019년 3월~현재: 고려대학교 정보보호대학원 교수