발전 제어시스템의 융합보안 연구★

이 대 성*

요 약

한국수력원자력, 한국전력공사, 한국남동발전 등의 발전 제어시스템은 전력을 공급하는 국가의 주요 인프라 시설로 악의적인 해킹 공격이 진행될 경우 그 피해는 상상을 초월한다. 실제로 한국수력원자력은 해킹 공격을 당하여 내부 정보가 유출되는 등 사회적인 큰 문제를 야기하였다. 본 연구에서는 최근 이슈가 되고 있는 융합보안 연구에 대해 전력회사 중심의 발전 제어시스템을 대상으로 그 환경을 분석하고, 현황을 분석하여 다양한 발전 제어시스템의 안정화를 위한 전략체계 수립과 대응책을 제시하고자 한다. 다양한 물리적 보안시스템(시설), IT 보안시스템, 출입통제시스템 등에서 나오는 데이터 형태를 정규화하고 통합하여 융합인증을 통해 전체 시스템을 통제하고, 융합관제를 통해 위험을 탐지하는 방법을 제안한다.

A Study on Convergence Security of Power Generation Control System

Daesung Lee*

ABSTRACT

Korea Hydro & Nuclear Power Co., Ltd., Korea Electric Power Corporation, and Korea South-East Power Corporation are major infrastructure facilities of power supplying countries. If a malicious hacking attack occurs, the damage is beyond the imagination. In fact, Korea Hydro & Nuclear Power has been subjected to a hacking attack, causing internal information to leak and causing social big problems. In this paper, we propose a strategy and countermeasures for stabilization of various power generation control systems by analyzing the environment and the current status of power generation control system for convergence security research, which is becoming a hot issue. We propose a method to normalize and integrate data types from various physical security systems (facilities), IT security systems, access control systems, to control the whole system through convergence authentication, and to detect risks through fusion control.

Key words : Convergence Security, Convergence Authentication, Data Normalization, Integrated Control

접수일(2018년 4월 2일), 수정일(1차: 2018년 7월 6일, 2차: 2018년 10월 17일), 게재확정일(2018년 12월 26일)

★ 본 논문은 2016년도 부산가톨릭대학교 교내연구비에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

* 부산가톨릭대학교/컴퓨터공학과

1. 서 론

국가의 주요 기반시설은 항공시스템, 도로교통 시스템, 전력시스템, 해상운항시스템 등 다양하게 존재하고 있으며, 이들 시스템들은 각자의 영역에서 물리보안 위주로 출입통제 기술에 의한 출입 제한을 통해 내부시설을 보호하는 것에 주력하여 왔다. 그러나, ICT(Inforamtion and Communication Technology) 기술이 모든 산업의 기반기술로 내재화 되고, 최근에는 4차 산업혁명과 더불어 사이버물리시스템[4]과 같은 융합보안 연구가 부상하면서 국가의 주요 기반시설에도 ICT 융합기술이 적용되기 시작하였고, 이로 인해 예전에는 발생하지 않았던 새로운 신종의 융복합적인 보안 위협이 발생하게 되었다. 이러한 ICT 융합기술이 적용된 사이버물리시스템에 대한 사이버/물리적 공격과 방어에 대한 기존 연구가 있었으나[1, 2], 현재까지 궁극적인 해결책을 제시하고 있지는 못하다. ICT 융합기술의 발전에 따라, 새로운 보안위협도 지속적이고 융합적으로 발생하고 있는 상황이며, 이에 대한 이슈와 관련연구도 꾸준히 병행되고 있는 실정이다[5,6,7,8,9,10]

본 논문에서는 국가의 주요 기반시설 중에서 전력회사를 중심으로 실제로 진행된 융합보안 컨설팅을 통해 나타난 융합보안의 현황과 환경분석에 대해 살펴보고, 그 분석 결과를 바탕으로 사이버물리시스템을 안전하게 통제하기 위한 방안을 제시하고자 한다[3]. 융합인증을 위해 물리보안 시스템, IT 보안시스템, 사이버물리시스템 등에서 발생하는 데이터를 표준화하고, 이를 기반으로 전체시스템에 대해 통합관제를 실시함으로써 사이버물리시스템의 안전성을 강화하는 방안을 제시할 것이다.

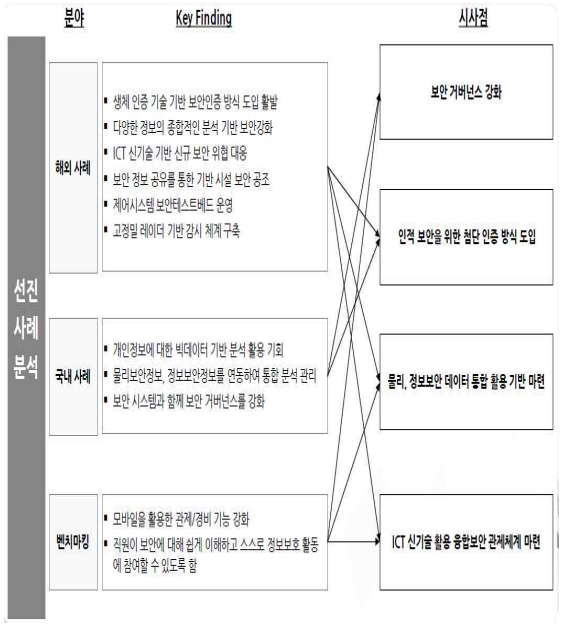
본 논문의 구성은 다음과 같다. 2장에서는 융합보안 현황 및 환경분석을 중심으로 관련연구에 대해 알아보고, 3장에서는 융합인증을 통해 융합통제 및 관제를 실시하는 방안에 대해 제시하며, 4장에서 결론을 맺고자 한다.

2. 관련 연구

N 전력회사를 대상으로 ICT 기술이 융합된 융합보안 시스템 구축을 위한 사전조사를 통해, 그에 따른 환경 및 현황분석이 진행되었다.

2.1 융합보안산업 기술동향

(그림 1)에서 알 수 있듯이, 해외 사례에서는 다양한 정보의 종합적인 분석에 기반한 보안 강화, ICT 신기술 기반 신규 보안위협 대응, 제어시스템 보안 테스트베드 운영 등이 주요 이슈로 나타나고 있으며, 국내 사례와 벤치마킹에서는 물리/정보보안 시스템과 모바일을 활용한 통합 분석 및 관제/경비 기능 강화가 주요 이슈로 나타나고 있다. 시사점으로는 물리/정보보안 데이터 통합 활용을 위한 기반을 마련하고, ICT 신기술 활용을 통한 융합보안 관제 체계를 마련함으로써 보안 거버넌스를 강화해야 함을 제시하고 있다.



(그림 1) 융합보안산업 기술동향 및 시사점

2.2 보안 고려사항 분석

융합보안산업의 기술동향에 맞추어 N 전력회사에서 진행되어야 할 융합보안 고려사항들에 대해 아래와 같은 분석 결과가 도출되었다.

기술	내용	보안고려요소
사물인터넷	▪ 사물인터넷은 다양한 산업영역에서 서비스 모델이 등장하고 있으며 최근 서비스 동향은 B2C서비스 확대, 수평적인 생태계 구조, ICT기술의 융합, 모바일, 웨어러블 등의 영역에서 서비스 활성화 ▪ 전력산업 분야에는 스마트 미터, 스마트그리드, 전력 사용, 제어시스템 운영 등에 활용	▪ 디바이스 네트워크, 데이터 인증 권한 관리 등
빅데이터	▪ 빅데이터는 전문학적으로 생성된 정형 또는 비정형 데이터를 처리하는 기술, 운영체계, 기반 아키텍처, 프로세스 등을 통칭하는 개념으로 모바일 인터넷 기기, 디지털 정보량, 앱 마켓의 급성장에 의해 생성 ▪ 전력 관련 대용량데이터를 활용한 빅데이터 분석이 활발히 진행중	▪ 대량 데이터 수집 분석 ▪ 오픈소스 기반 ▪ Privacy(개인정보, 생활정보)
클라우드 컴퓨팅	▪ 클라우드 컴퓨팅은 '인터넷을 이용한 IT 자원의 주문형(On-demand) 아웃소싱 서비스'로 인터넷 접속으로 필요한 응용 소프트웨어를 구동하여 작업을 가능케 하는 이용자 중심의 컴퓨팅 환경 ▪ 기민성(신속한 용량 증가 등), 효율성(협업 등이 용이) 측면에서 활용	▪ 가상화 취약점 상속 ▪ 사용다발의 다양성 ▪ 자원 공유/집중화
모바일	▪ 스마트폰 기술이 발전됨에 따라 고성능화와 함께 지문인식 등 생체인식 기능 등의 최신 바이오 기술이 도입되고, 다양한 분야와 융합되어 활용 ▪ 스마트워크의 기술은 커뮤니케이션, 보안관리, 시스템·데이터 재해복구, 시스템관리 기술로 분류할 수 있으며, 언제 어디서나 사내 업무 시스템을 활용할수 있도록 다양한 단말 플랫폼의 지원과 기간 시스템을 연계할 수 있는 모바일 오피스 아키텍처를 구성	▪ 인터넷망 해킹 및 DDoS 공격 ▪ 비인가자 접근 ▪ 악성코드 ▪ 도청 ▪ 디바이스 도난 및 분실

(그림 2) N 전력회사 전략기술 및 보안 고려사항

(그림 2)에서 알 수 있듯이 4차 산업혁명 시대의 기반기술이 되는 사물인터넷, 빅데이터, 클라우드 컴퓨팅, 모바일 분야를 중심으로 보안 고려사항을 도출하였으며, 각 분야의 주요 고려사항으로는

· 사물인터넷 – 인증, 권한 관리

· 빅데이터 – 대량 데이터 수집/분석, 개인정보 관리

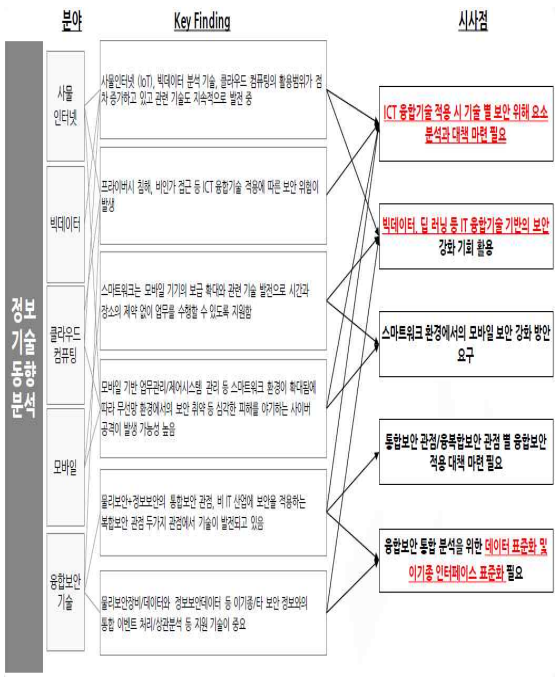
· 클라우드 컴퓨팅 – 가상화 취약성 및 자원 공유

· 모바일 – 악성코드 및 디바이스 도난/분실 관리

등으로 나타났다.

2.3 융합보안 구축 시사점

2.2 절에서 나타난 4차 산업혁명의 핵심기술이 되는 사물인터넷, 빅데이터, 클라우드 컴퓨팅, 모바일 분야를 중심으로 분석된 N 전력회사의 주요 보안 고려사항을 바탕으로 N 전력회사에서 필요한 융합보안 시스템의 구축 방향은 다음과 같이 도출되었다.



(그림 3) N 전력회사 융합보안 구축 시사점

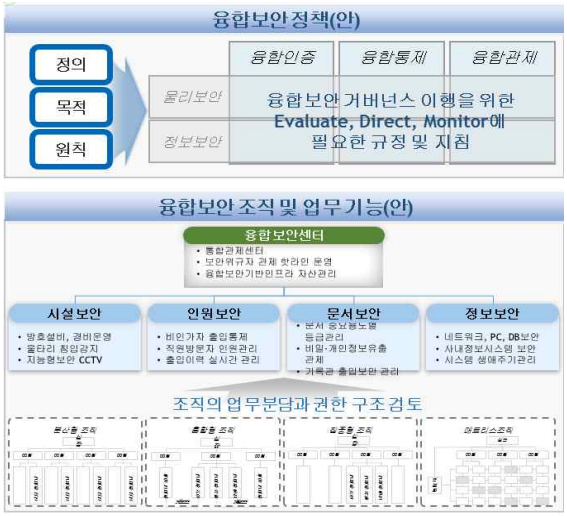
(그림 3)에서 알 수 있듯이, 융합보안 시스템을 효과적으로 구축하기 위해서는 다양한 물리/정보보안 시스템으로부터의 광범위한 데이터 수집과 수집된 데이터의 표준화 및 융합보안 통합분석을 위한 이기종 인터페이스 표준화가 절실한 것으로 나타난다. 또한, ICT 융합기술 적용 시 나타날 수 있는 보안 위해요소 분석과 그에 대한 대책이 필요하며, 대량의 빅데이터 분석을 통한 딥러닝 등의 인공지능 기반 보안기술 적용이 필요한 것으로 나타났다.

3. 융합 인증과 융합 관제를 통한 융합보안 거버넌스 구축

2.3절에서 제시된 시사점을 바탕으로 N 전력회사의 융합보안 시스템 구축을 위한 융합 인증과 융합 관제 방법은 다음과 같다.

3.1 융합보안 정책

융합 인증과 융합 관제를 통해 융합보안 거버넌스를 구축하기 위해서는 조직의 업무분담과 권한 구조를 검토하고, 이를 바탕으로 융합보안 조직 및 업무기능에 따른 융합보안 정책을 정의할 필요가 있다.



(그림 4) 융합보안 조직 및 업무기능 구성에 따른 융합보안 정책 설계

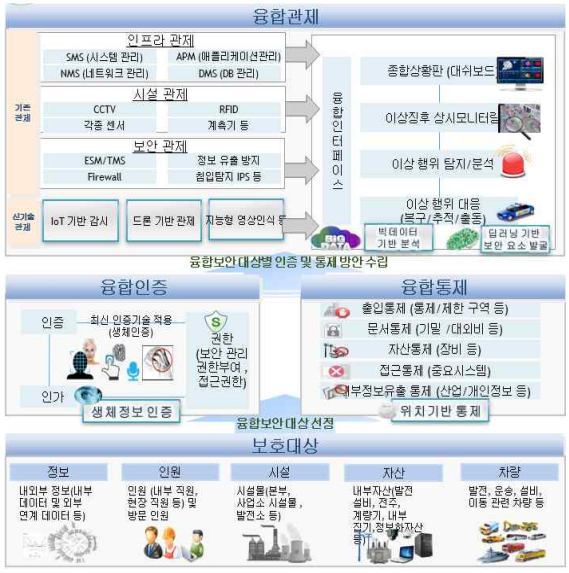
(그림 4)에서 알 수 있듯이, 융합보안 거버넌스 이행을 위해서는 조직의 업무분담과 권한 구조를 기반으로 융합인증, 융합통제, 융합관제를 위한 Evaluate, Direct, Monitor에 필요한 규정 및 지침을 마련하는 융합보안 정책이 필요하다.

3.2 표준 목표모델 정립

융합보안 정책을 기반으로 융합보안 보호대상을 선정하고, 대상별 융합인증, 융합통제 방안을 수립하여 IoT 기반, 드론 기반, 지능형 영상인식 등의 신기술 관제를 적용한 융합관제를 위한 표준 목표모델은 (그림 5)와 같다.

3.3 융합 인증

융합 인증을 위해서는 온/오프라인 인증체계를 단일화하고, 사용자 행위에 대한 로그 통합 편의성을 확보해야 하며, 실시간 행위 분석을 통한 예방적인 보안 통제가 시행되어야 한다.



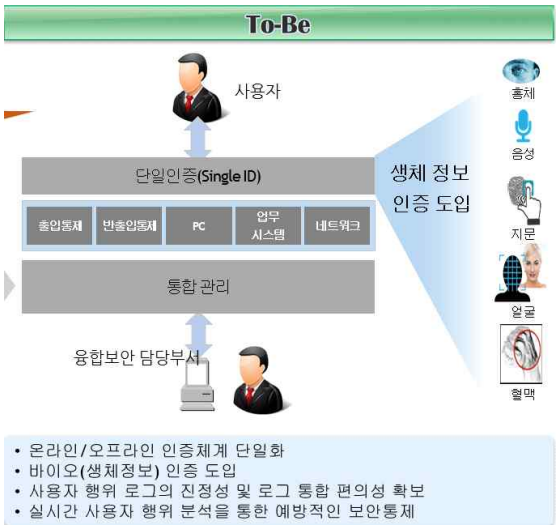
(그림 5) 융합보안 표준 목표모델 정립

아래의 (그림 6)은 융합인증이 시행되지 않는 상황으로, 물리적 보안과 IT보안이 단절되어 있으며, 각 부서별 사용자가 개별 인증을 해야 한다. 또한, 온/오프라인 인증체계도 분리된 상황이다.

(그림 6) 물리적/IT 보안이 단절된 개별 인증

아래의 (그림 7)은 온/오프라인 인증체계가 단일화되고, 융합보안을 담당하는 전담부서가 있으며, 인증방식도 생체 인증 등을 통해 다양한 시스템으로부터

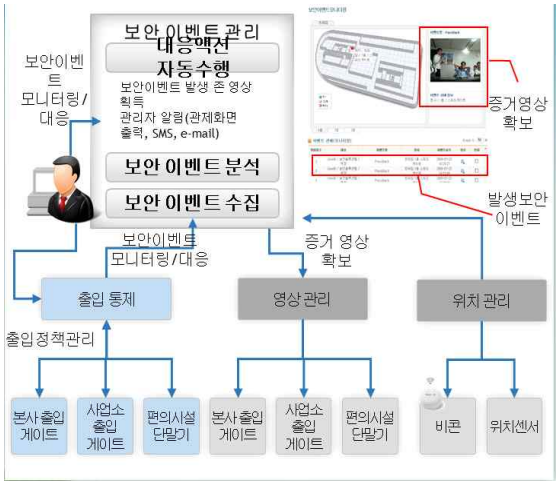
의 단일 인증을 시행하는 융합 인증 시스템이다.



(그림 7) 융합 인증 모델

3.4 융합 통제

융합 인증을 기반으로 융합 통제를 구현하는 방법은 다양하다. (그림 8)은 위치 기반으로 출입관리와 영상관리 정보의 융합을 통한 출입통제의 한 예이다.



(그림 8) 융합 통제 모델

3.5 융합 관제

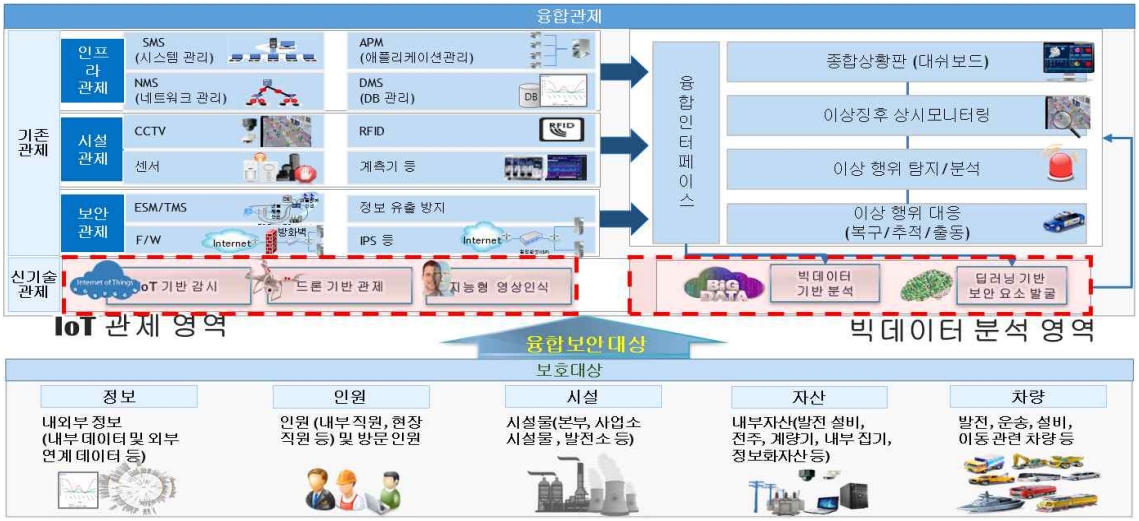
물리보안과 정보보안을 통해 생성되는 모든 정보를 융합하여 사전 이상 징후에 대해 탐지 및 차단하고, 보안 위협 발생 시 신속한 원인 규명과 조치/보고/공유가 가능한 융합관제 모델은 (그림 9)와 같다.

아래의 (그림 9)에서 알 수 있듯이 정보, 인원, 시설, 자산, 차량 등 다양한 융합보안 보호대상에 대해 기존 관제와 더불어 IoT 기반 감시, 드론 기반 관제, 지능형 영상인식 등의 신기술 관제를 접목하고 개별인증이 아닌 단일인증을 적용하여 온/오프라인에서 발생하는 인증 정보를 통일한다. 또한, 인증 정보와 더불어 온/오프라인에서 발생하는 모든 이벤트에 대해 이종 데이터가 표준화 될 수 있도록 융합인터페이스 기준을 마련하고, 수집된 다양한 융복합적 이벤트에 대해 빅데이터 기반의 인공지능 분석으로 보안 위협 발생에 따른 신속한 대응이 가능하게 한다.

4. 결 론

본 연구에서는 융합보안산업 기술동향에 근거하여 전력회사와 같은 발전 제어시스템의 융합보안 연구를 진행하였다. N 전력회사를 중심으로 현재의 융합보안 구축 환경과 현황을 분석하고, 보안 고려사항들을 도출하였으며, 그에 따른 필요한 시사점을 제시하였다. 제시된 시사점을 기반으로 융합 인증과 융합 관제를 통한 융합보안 거버넌스 구축을 위한 전략을 제시하였다. 그 방법으로는 조직의 업무특성과 권한에 따른 보안정책을 설정하고, 보안정책에 따른 융합보안 표준 목표모델을 정립해야 한다. 또한, 표준 목표모델에 따라 조직의 특성에 맞는 융합 인증, 융합 통제, 융합 관제를 실시해야 한다.

결론적으로 물리보안 시스템과 정보보안 시스템, 기타 인원/자산 등 다양한 시스템에서 발생하는 융합 데이터를 표준화하는 방안(이기종 인터페이스 표준화 등)이 선행되어야 하며, 표준화된 데이터를 인공지능 등을 활용하여 분석하고 사전 예측하기 위한 일원화된 인증체계와 융합 관제가 필요하다.



(그림 9) 융합 관제 모델

참고문헌

[1] Myung-Hoon Lee, Si-Hwa Bae, Sung-Yong Son, "A Security Design for a Smart Power Grid Field Test based-on Power IT Systems", 한국정보통신학회논문지 14(11), 2010.11.

[2] Woong Go, Jin Kwak, "Secure Data Transaction Protocol for Privacy Protection in SmartGrid Environment", 한국정보통신학회논문지 16(8), 2012.8.

[3] 한국남동발전, "스마트 융합보안 마스터 플랜 고도화 최종보고서", 2016.10.

[4] 은용순, 박경준, 원명규, 박태준, 손상혁, "사이버물리시스템 연구 동향", 정보과학회지 31(12), 2013.12.

[5] 노상도, "스마트공장 사이버물리시스템(CPS) 기술 동향 및 이슈, 전자공학회지 481-484, 2016.6.

[6] 김남준, 왕지남, "스마트 공장용 CPS 통합 Architecture", 대한산업공학회 춘계공동학술대회 논문집, 2017.4.

[7] 박정민, 강성주, 전인걸, 김원태, "네트워크 기반 자율제어 CPS(Cyber-Physical Systems) 기술", 한국통신학회지(정보와통신) 2013.9.

[8] 최승오, 김우년, "사이버 물리 시스템 테스트베드 기술 연구 동향", 정보보호학회지, 2017.4.

[9] 김성일, 김종성, "융합보안관제 시스템의 효율성 향상을 위한 이벤트 분류 및 처리에 관한 연구", 융합보안논문지, v.17, no.3 31-40, 2017.9.

[10] 유승재, "보안관제시스템 구성 및 개선방안 연구", 융합보안논문지, v.17, no.2, 69-80, 2017.6.

〔저자소개〕

이 대 성 (Daesung Lee)
1999년 2월 인하대학교 전자계산공학과 학사
2001년 2월 인하대학교 전자계산공학과 석사
2008년 2월 인하대학교 정보공학과 박사
2012년 3월 ~ 현재 부산가톨릭대학교 부교수
email : dslee@cup.ac.kr