# 국가 인프라 시설의 융합보안 연구

이대성*

*부산가톨릭대학교

# A Study on Convergence Security of National Infrastructure

Daesung Lee*

*Computer Engineering, Catholic University of Pusan

E-mail : dslee@cup.ac.kr

## 요 약

항공관제시스템, 도로교통시스템, 한국수력원자력 등의 관제 및 발전 시스템 등은 국가의 기반 인프라 시설로 악의적인 해킹공격이 진행될 경우 그 피해는 상상을 초월한다. 실제로 한국수력원자력은 해킹 공격을 당하여 내부정보가 유출되는 등 사회적인 큰 문제를 야기하였다. 본 연구에서는 최근 이슈가 되고 있는 융합보안 연구에 대해 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, 통합관제를 통해 위험을 탐지하는 방법을 제안한다.

## ABSTRACT

Control and development systems such as air traffic control systems, road traffic systems, and Korea Hydro &Nuclear Power are the infrastructure facilities of the country, and if the malicious hacking attacks proceed, the damage is beyond imagination. In fact, Korea Hydro & Nuclear Power has been subjected to a hacking attack, causing internal information to leak and causing social problems. In this study, we analyze the environment of the development control system and analyze the status of the convergence security research, which is a recent issue, and propose a strategy system for stabilizing various power generation control systems and propose countermeasures. 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

키워드

융합보안, 융합인증, 데이터 정규화, 통합관제

## Ⅰ. 서 론

국가의 주요 기반시설은 항공시스템, 도로교통시스템, 전력시스템, 해상운항시스템 등 다양하게 존재하고 있으며, 이들 시스템들은 각자의 영역에서 물리보안 위주로 출입통제 기술에 의한 출입제한을 통해 내부시설을 보호하는 것에 주력하여 왔다. 그러나, ICT 기술이 모든 산업의 기술로 내재화 되고, 최근에는 4차산업혁명과 맞물리면서 국가의 주요 기반시설도 ICT 융합기술이 접목되어 새로운 신종의 융합적인 보안 위협이 발생하게 되었다. 이러한 기반시설에 대한 과거의 공격과 방어에 대한 기존 연구가 있었으나[1, 2], ICT 융합기술의 발전에 따라, 새로운 보안위협도 지속적이고 융합적으로 신생하고 있는 상황이다. 본 논문에서는 국가의 주요 기반시설 중에서 전력회사 중심으로, 실제로 진행된 융합보안 컨설팅을 통해 나타난 융합보안의 현황 및 환경분석, 그리고 융합인증을 통한 통합관제를 위한 방안을 제안하고자 한다[3]. 2장 본론에서는 환경과 현황을 분석하고, 3장 결론을 통해 통합관제를 위한 융합인증 방법에 대해 제안하고자 한다.

## II. 본 론

N 전력회사를 대상으로 ICT기술이 융합된 융합보안 시스템 구축을 위한 사전 조사가 진행되었고, 그에 따른 환경 및 현황분석은 아래와 같다.

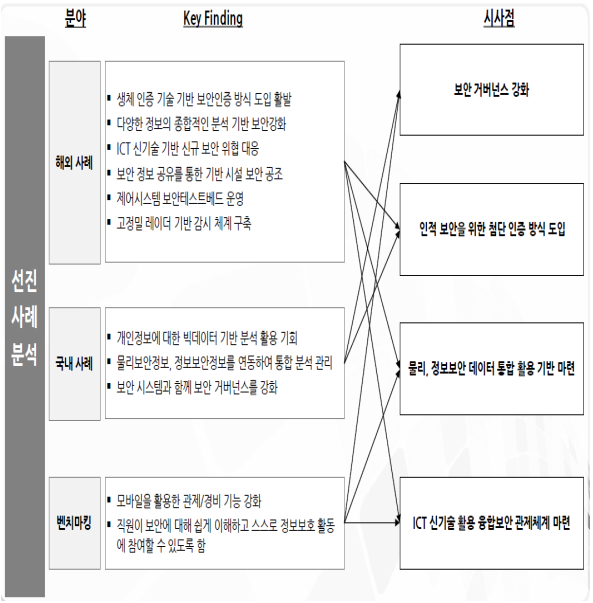


그림 1. 융합보안산업 기술동향 및 시사점

| 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<br>• 전력산업 분야에는 스마트 미터, 스마트그리드, 전력 사용, 제어시스템 운영 등에 활용 | • 디바이스 네트워크, 데이터, 인증 권한 관리 등 |
| 빅데이터 | • 빅데이터는 천문학적으로 생성된 정형 또는 비정형 데이터를 처리하는 기술, 운영체계, 기반 아키텍처, 프로세스 등을 통칭하는 개념으로 모바일 인터넷 기기, 디지털 정보량, 앱 마켓의 급성장에 의해 생성<br>• 전력 관련 대용량데이터를 활용한 빅데이터 분석이 활발히 진행중 | • 대량 데이터 수집 분석<br>• 오픈소스 기반<br>• 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<br>• 기민성(신속한 용량 증가 등), 효율성(협업 등이 용이) 측면에서 활용 | • 가상화 취약점 상속<br>• 사용단말의 다양성<br>• 자원 공유/집중화 |
| 모바일 | • 스마트폰 기술이 발전됨에 따라 고성능화와 함께 지문인식 등 생체인식 기능 등의 최신 바이오 기술이 도입되고, 다양한 분야와 융합되어 활용<br>• 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<br>• 비인가자 접근<br>• 악성코드<br>• 도청<br>• 디바이스 도난 및 분실 |

그림 2. N사 전략기술 및 보안 고려사항 분석

융합보안산업의 기술동향에 맞추어 N사에서 진행되어야 할 융합보안 고려사항들에 대해 환경과 현황에 대해 분석하였고, 그 결과로 나타난 시사점은 다음과 같다.

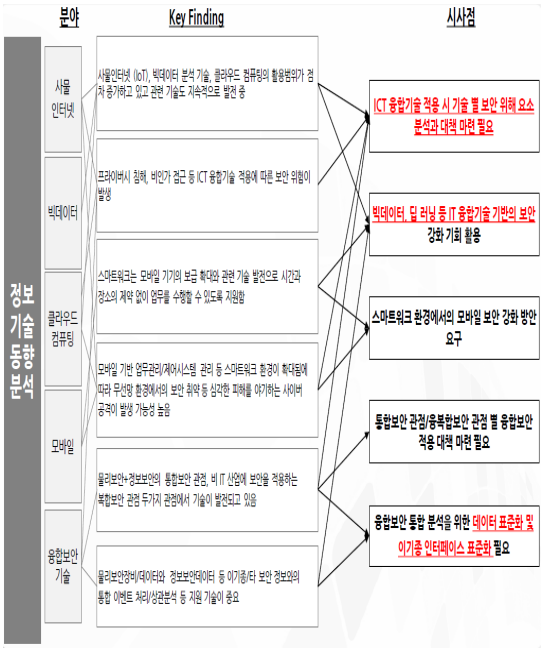


그림 3. 융합보안 구축 시사점

## III. 결 론

본 연구에서는 융합보안산업 기술동향에 근거하여 N 전력회사를 중심으로 현재의 융합보안 구축 환경과 현황을 분석하고, 보안 고려사항들을 도출하였고, 필요한 시사점에 대해서도 제안하였다. 핵심 결론으로는 물리시스템과 정보시스템이 융합된 상황에서 발생되는 다양한 융합데이터를 분석 및 데이터를 표준화 하고, 이를 위한 이기종 인터페이스 표준화 작업도 병행되어야 하며, 표준화 이후의 융합인증을 일원화 하여 통합관제가 가능하도록 융합보안시스템을 구성해야 한다는 결론을 제시하였다.

## 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, 2497-2506

[2] Woong Go, Jin Kwak, "Secure Data Transaction Protocol for Privacy Protection in SmartGrid Environment", 한국정보통신학회논문지 16(8), 2012.8, 1701-1710

[3] 남동발전, "스마트 융합보안 마스터플랜 고도화 최종보고서", 2016.10