댐·보 등 수자원분야 정보통신기반시설 보안대책

유세환* · 장동배*

*한국수자원공사

Security measures of Information and Communication infrastructure of Water Resources Field

Se-Hwan Yu* · Dong-bae Jang**

*K-water Water Resources Development Dept

E-mail : ysh32@kwater.or.kr

요 약

정보통신기반시설은 국가 안전보장, 행정, 국방, 치안, 금융, 통신, 운용, 에너지 등의 업무와 관련된 전자적 제어·관리시스템 또는 정보통신망으로, 수자원분야는 국민의 편의와 안전에 중요한 수도·발전·댐관리 등을 전자적으로 수행할 수 있도록 제어시스템이 구축되어있다. 수자원분야는 또한 물관리 패러다임의 변화에 따라 제어시스템은 하나의 네트워크로 통합·관리되어 수계별로 유역통합물관리가 실현되고 있다. 이러한 제어시스템은 다른 제어망, 업무망, 외부기관과의 연계등의 많은 보안상의 취약점을 노출하고 있고, 이에 대한 사이버테러는 사회·경제적으로 큰 혼란을 야기할 수 있으므로 제어시스템에 대한 보안의 중요성이 대두되고 있다. 본 논문에서는 정보통신기반시설 - 특히 댐·보 등 수자원분야의 제어시스템 보안대책에 대해 알아보고자 한다.

ABSTRACT

ICT infrastructure is electronic control systems or communication network related to national security, public administration, defense, policing, finance. Water resources sector has been building a system of control that can be performed electronically, communications, management, energy, and other work-related. Water resources sector has been a paradigm shift in water management and the control system is integrated into a single network. The control system security vulnerabilities are exposed - other control networks, business networks, linking with outside agencies, etc. Cyber terrorist society can cause a huge mess economically, The importance of security for control systems is becoming. In this paper, ICT infrastructure - the water resources in the field of control systems will analysis security measures,

Ⅰ. 서 론

정보통신기반시설이란 정보통신기반보호법 제2조에 의거, 국가 안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련되어 해킹, 바이러스 및 분산서비스거부공격등의 사이버위협으로 운영이 중단될 시 국가의 안전과 국민생활에 지장을 초래하는 된 전자적 제어·관리시스템 및 정보통신망을 뜻하는 것으로, 정보통신기반시설은 금융·통신·수자원 등 국가기능 유지와 관련된 전자제어관리망, 정보 송·수신 정보통신망 등 공공/민간분야의 총 209개 시설이 지정되어 있다. 표1은 분야별 주요 정보통신기반시설 현황이다.

표 1. 분야별 주요 정보통신기반시설 현황

분 야	주요 정보통신기반시설
행 정	행정업무 시스템 등
방송통신	인터넷접속망 등
금 융	인터넷뱅킹 시스템 등
에너지	SCADA 시스템 등
건설교통	운항관리 시스템 등
사회복지	보험관리 시스템 등
기타	입법정보 시스템 등

수자원분야의 발전·댐·수도 등은 제어시스템으로 구성되어 있는데, 최근의 보안침해사고의 동향은 물리적인 침해보다 제어시스템에 대한 사이

버공격으로 변화하는 추세이며, 각 나라들은 사이버테러에 대한 정보시스템 보호의 중요성이 대두되고있다. 또한 수자원분야에 대한 사이버테러에 의한 침해사고 발생 시 피해규모 및 범위가 방대하고, 타 기반시설·정보통신망으로의 급속한 피해 확산이 예상되므로 수자원분야 제어시스템의 보안 취약점을 알아보고 수자원분야의 특성에 맞는 보안대책방향에 대해 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 정보통신기반시설 보안일반에 대해서 설명하고, 3장에서는 제어시스템 도입시 보안대책에 대해서 알아보고, 4장에서는 수자원분야 정보통신기반시설에 대한 보안대책을 제시하고, 5장에서는 결론을 맺는다.

Ⅱ. 정보통신기반시설 보안일반

정보통신기반시설을 구성하는 제어시스템은 시스템을 구성하는 장비의 동작을 관리 및 제어하는 장비들을 조작할 수 있도록 하는 시스템이며 시스템을 구성하는 장비의 센서나 작동장치의 필드 장치, 제어용 네트워크, 감시제어시스템 등으로 구성된다. 일반적으로 필드로부터 수집된 데이터와 센서데이터를 취득·저장하고, 제어하는 기능을 수행한다. 이러한 제어시스템을 통해 각종시설물을 효율적으로 관리·제어할 수 있다.

이러한 시스템을 구축하고 운영하기 위해서는 사업계획단계에서 자체 보안성 검토를 하여야하는데, 정보통신기반시설은 자체 보안성 검토 대상사업으로 그 대상은 공항·철도·항만·수자원 등 주요기반시설을 중앙에서 감시를 하는 감시제어 시스템과 그 부속시설을 포함한다.

또한 법적으로는 정보통신기반시설은 정보통신기반보호법의 적용을 받으며 정보보호 책임자, 실무자, 제어·보안담당자를 지정하여 운영하여야 한다.

그리고 전자제어관리시스템보안관리지침에 의거하여, 제어시스템이 연계된 제어망은 반드시 외부망과 분리된 폐쇄망으로 운영하고, 제어시스템을 운영하는 시설은 통제구역으로 지정·관리되어야 한다. 또한 백신프로그램을 운영하고, 휴대용 저장매체는 사용통제하고, 외부에서 원격접속을 통한 제어시스템 유지보수는 원천적으로 금지된다.

2.1 제어시스템 도입절차

제어시스템 도입을 할 경우, 아래 그림과 같은 절차대로 제어시스템을 도입하여야 하며, 사업계획단계에서 네트워크 관리, DB·Web관리, 운영 및 설정관리, 제어기기의 인증·암호화·접근통제, 물리적 접근통제 및 보호대책, 안전한 소프트웨어 개발등의 제어시스템 구성 및 운영계획의 보안 위협을 분석하고 이에 필요한 보안대책을 수립하여야 한다.

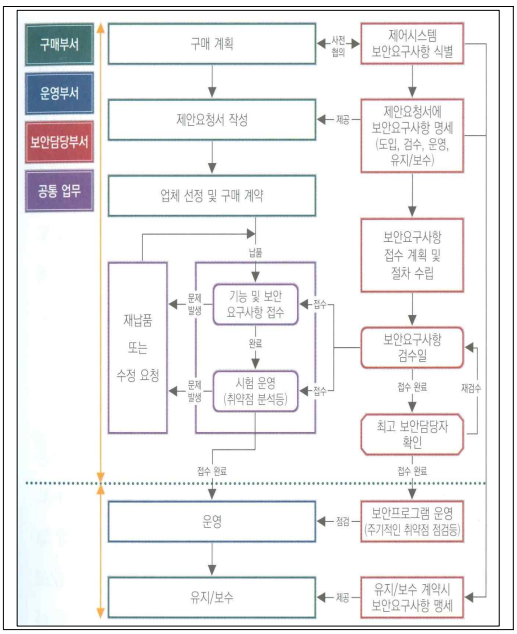

그림 1. 제어시스템 도입절차

주요 보안 요구사항으로는 아래 표와 같다.

표 2. 제어시스템 도입시 보안요구사항

구분	보안요구사항
제어기기	인증, 암호화, 접근통제, 모니터링 등
물리적보안	물리적 접근통제 및 보호대책 적용
감사	장애 및 침해사고 분석, 재발방지 대책 수립을 위한 감사정책 수립 및 시행
안전한 소프트웨어	안전하지 않은 함수 제한 등 취약점 최소화

2.2 수자원분야 정보통신기반시설

수자원분야의 정보통신기반시설은 발전통합운영시스템 등 2개가 지정되어 있으며, 표3과 같다.

표 3. 수자원분야 정보통신기반시설

구분	용도	지정년월
발전통합운영시스템	다목적댐 발전기 및 수문제어	´10. 02월
수도통합운영시스템	상수도 수처리 자동화	´10. 02월
댐 홍수경보시스템	안정적 수문통제	´12. 02월

수자원분야의 정보통신기반시설은 다름 그림과 같은 형태로 구성되어 있으며, 크게 업무망, 제어망(발전/수도/댐 등)으로 구성되어 있고, 업무망과 제어망간은 서로 폐쇄망으로 구성되어 있다.

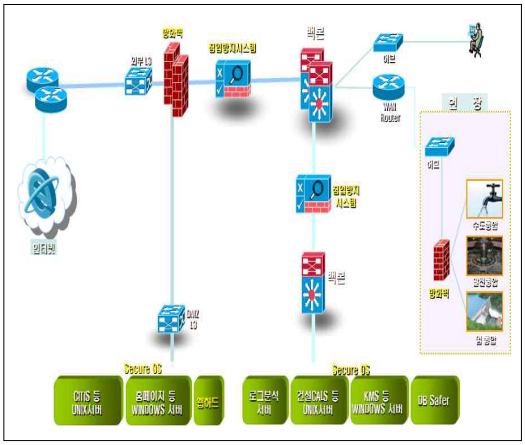

그림 2. 수자원분야 정보통신기반시설 구성도

Ⅲ. 제어시스템 도입시 보안요구사항

제어시스템은 편리성의 이유등으로 주요기반시설에 지속적으로 사용되나, 보안에 대한 고려 없이 해당시스템의 기능적인 측면만을 추구하여, 많은 보안위협에 노출되게 된다. 그리고 보안대책을 수립하더라도 기존 제어시스템의 운영중단이 필요할 수 있다. 따라서 제어시스템 도입시 보안에 대한 요구사항을 식별하고 보안성을 검토하여 이를 반영하여야 한다.

운영부서는 제어시스템 도입 계획을 수립하고, 제어시스템 구성 및 운영계획을 작성하여 구매부서와 보안담당부서에 제공하여야 한다. 구매부서는 이를 바탕으로 시스템 구매계획을 수립하며, 보안담당부서는 제어시스템 보안 요구사항을 식별하여야 한다. 보안요구사항은 기 수립된 제어시스템 도입 계획을 수립하고, 제어시스템 구성 및 운영계획을 작성하여 구매부서와 보안담당부서에 제공하여야 한다. 구매부서는 이를 바탕으로 시스템 구매계획을 수립하며, 보안담당부서는 제어시스템 보안 요구사항을 식별하여야 한다.

보안요구사항은 기 수립된 제어시스템 구성 및 운영계획의 보안 위협을 분석하고, 이에 필요한 보안대책들을 식별하여 시스템구성, 운영, 보안기술의 적용에 있어 필요한 사항들을 도출한다. 다음은 제안요청서에 반영할 보안요구사항이다.

3.1 문서화

도입 제어시스템의 하드웨어 및 소프트웨어에 대한 보안대책 현황과 보안설정 정보, 개발 및 운영에 필요한 사항을 관리하여 최적의 보안상태를 설정할 수 있도록 제어시스템 도입 시 구매, 검수, 운영, 유지보수와 관련된 보안요구사항을 명시한다.

3.2 서비스 관리 및 관리실행권한

제어시스템 운영과 관련이 없는 불필요한 기능은 해상시스템의 보안취약점을 이용한 시스템 침투에 활용될 수 있으므로, 제어시스템 운영에 필요한 서비스 목록 관리 및 불필요한 서비스는 제거한다. 또한 제어명령, OS 명령, 중요 파일의 실행, 열람 권한은 제어시스템 운영에 필요한 사용자에 한하여 최소한으로 주어지도록 관리한다.

3.3 제어시스템 및 DB 운영 및 설정관리

도입되는 제어시스템에는 패스워드, 유지보수를 위한 관리자계정 등의 보안취약요소가 많으므로 시스템 도입시점에 최적의 보안설정을 적용해야한다. 또한 제어시스템의 정보를 저장하기 위한 DB에 대해서는 암호화, 인증, 취약점 점검 등의 보안대책을 수립하여야한다.

3.4 네트워크 관리

외부로부터의 제어시스템의 사이버침해를 예방하기 위해 네트워크를 분리하여 구성하고, 접근통제 및 감시, 암호화등의 보안대책을 적용한다.

3.5 제어기기 및 물리적 보안

현장 필드의 PLC등의 장비에 대한 보안대책을 수립하여야 하고, 현장 및 제어시스템에 대한 물리적 접근 및 비인가 사용에 대한 보안대책이 필요하다.

3.6 안전한 소프트웨어 개발

소프트웨어 개발 프로세스에서 보안을 고려한 개발 및 안전하지 않은 것으로 알려진 프로그래밍 사용을 제한하는 등 소프트웨어가 지닐 수 있는 취약점을 최소화하여야 한다.

Ⅳ. 수자원분야 정보통신기반시설 보호대책

정보통신기반시설로 지정된 시설에 대해서는 망분리 제도가 원칙으로, 망분리란 업무용도로 사용하는 내부망과 인터넷 접속이 가능한 외부망을 따로 구축하는 것으로, 수자원분야의 업무망은 망분리가 가능토록 구성되어 있다.

일반적인 제어시스템은 일반적인 시스템과 달리 다양한 성능과 안정성을 요구한다. 그러나 업무상의 필요에 의한 제어망간 연계 및 국민의 알권리를 위한 대외기관 자료공개등의 접점으로 인해 침해사고의 원인이 발생한다. 제어시스템 보안대책에서 가장 중요한 점은 제어시스템과 타시스템과의 연계접점을 없애는 것이므로, 제어망과 업무망간의 데이터 연계운영방안에서 논한다.

사이버위협으로부터 기반시설보호를 위해 제어망은 원칙적으로 폐쇄망구조로 운영되어야 하고, 불가피하게 서로 다른 기능의 제어망과의 데이터 통신, 업무망으로의 데이터 전송, 외부기관 정보공개를 위한 데이터 전송을 위한 연계가 필요하다. 이러한 연계접점에서 보안상의 취약점을 노출하고 있다. 그러나 효율적인 업무수행을 위한 자료공유를 위해 제어망과 다른 망간의 연계운영은 불가피하다. 제어시스템의 보안성 강화를 위해서

는 제어망과 업무망, 제어망간의 연계되는 접점을 최소하하여야 한다.

수자원분야는 크게 댐 · 수도 · 발전 등으로 제어시스템이 구성되고, 각각의 제어망 내 각기 다른 현장 필드의 제어시스템이 운영되고, 통합관리 · 운영을 위해 본사에서 전체 제어시스템이 통합관리되고 있다.

이러한 구조에서 제어망과의 연계점점방안에 대해서 알아본다.

4.1 제어망과 업무망 간의 점점 최소화

필드의 제어망과 업무망 구간의 접점을 아래 그림과 같이 최소화하여 취약점 대상을 제거해야 한다. 제어망과 업무간간 데이터 연계가 필요한 경우 본사내 제어망과 업무망을 통해 데이터 전송을 할 수 있도록 한다. 이를 위해 제어망과 업무망 사이의 방화벽의 양방향정책을 제어망에서 업무망으로의 단방향정책을 통하여, 업무망에서 제어망으로 불법적인 접근을 차단한다.

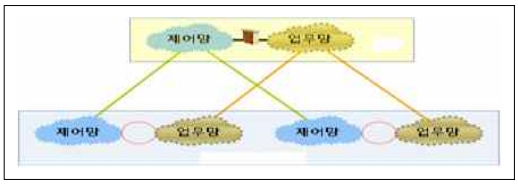

그림 3. 제어망과 업무망 구성

4.2 제어망과 제어망 간의 점점 최소화

제어망과 제어망 구간의 접점도 아래 그림과 같이 최소화 하되, 제어시스템 특성상 서로 다른 제어시스템간의 데이터 연계가 필수적이다. 이때는 본사의 DMZ내 취득되는 데이터를 연계하여 운영한다. 이때는 서버팜 DB에서 현장 필드의 제어시스템으로 데이터를 전송토록 한다. 또다른 방법으로는 본사내 제어망간 방화벽을 경유하여 데이터를 전송하는 방법이 있다. 만약 현장 필드에서 실시간으로 데이터가 필요한 경우에는 구간내 시리얼통신(RS-232 등)으로 구성하여, LAN통신이 불가능하도록 한다.

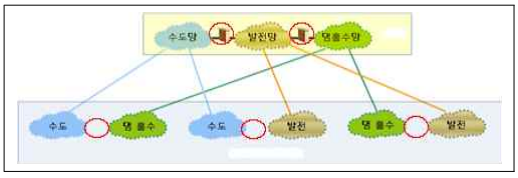

그림 4. 제어망과 제어망 구성

4.3 서버보안 등

서버보안솔루션 및 백신프로그램 설치를 설치하고, 이상발생시 원격제어를 할 수 있도록 원격제어프로그램을 설치한다. 이때는 원격접속은 제어망간 접속만 가능토록한다. 제어망 내의 서버류는 업데이트가 불가능하므로, 서버류의 프로그램이 자동패치될 수 있도록한다.

V. 결 론

정보통신기반시설을 구성하는 제어시스템은 다양한 분야에서 사용되고 있다. 기존의 제어시스템은 물리적인 공격에 대책위주로 이루어졌지만, 제어시스템을 목적으로 한 사이버 공격이 증가하면서 보안정책의 재정립이 필요하였다.

따라서 본 논문에서는 제어시스템을 도입부터 구축시까지 보안착안사항에 대해서 알아보고 수자원분야의 기반시설보안대책에 대해서 알아보았다.

앞으로 제어시스템 보안을 위하여 철저한 보안대책 수립과 체계적인 시스템 도입이 필요하다.

참고문헌

[1] 정보통신기반보호법
[2] 전자제어관리시스템보안관리지침
[3] 주요정보통신기반시설 데이터 연계운영 보안강화, 한국수자원공사, 2012년 8월
[4] 제어시스템 도입 시 보안요구사항, 한국수자원공사, 2012년 9월
[5] 최명균, 이동범, 곽진, “제어시스템에 대한 보안정책 동향 및 보안 취약점 분석”, 정보보호학회논문지, 21권 5호, 2011년 8월
[6] 윤정한, 김우년, 서정택, “제어시스템 네트워크 보안기술 동향”, 정보보호학회논문지, 22권 5호, 2012년 8월