情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

철도관제시스템의 정보보안에 대한 고찰

이 재 호*, 이 영 수**

요 약

철도시스템은 시설, 차량, 역사, 전기, 신호통신 등 거의 모든 분야가 통합되어 상호 유기적으로 동작함으로써 안전하고 신뢰성 있는 운행을 가능하게 한다. 특히, 철도에 처음으로 컴퓨터 시스템을 도입한 열차운행제어 설비인 관제시스템은 선구를 운행하는 모든 열차에 대하여 중앙에서 원격 감시 및 제어를 수행함과 동시에 열차운행에 관련된 모든 정보를 취합하고 이를 각 분야별로 전송하여 열차 운행의 정시성을 보장하는 중요한 설비이다. 따라서, 관제시스템은 열차운전 통제 및 감시의 일관성, 효율성, 적시성을 기하여 열차의 안전운행 확보와 지연을 최소화하고 있다. 이와 같이 열차운행의 중요 설비인 관제시스템은 국가 보안시설로 평상시는 일반인의 출입이 금지될 뿐만 아니라 시스템적으로 외부로부터의 침입 방지 및 보안 대책은 무엇보다도 중요한 현안이므로 관제시스템에 대한 보안 위협을 분석하고 이에 대한 보안대책 및 대응방안 등에 대하여 논의하고자 한다.

Ⅰ. 서 론

철도분야에서의 관제시스템은 초기에는 열차집중제어(CTC : Centralized Traffic Control)장치라 칭하였으며, 그 역할은 열차운행구간에 설치되어 있는 신호설비를 한곳에서 통제하여 인적착오에 의해 발생할 수 있는 사고를 방지함은 물론이고 선로를 효율적으로 활용하여 열차운행의 효율화를 추구하고 있다[1].

또한, 컴퓨터를 활용함으로 인하여 열차운행정보의 전산화, 통계관리, 중대사고 발생시 신속한 대처, 인건비 및 운전비용의 절감, 평균운행속도의 향상 및 보안도의 향상을 초래하였다.

한국철도는 크게 국가가 소유하거나 운영하는 일반철도와 지자체가 소유하거나 운영하는 도시철도로 구별된다. 일반철도의 경우 각 지역별(5개)로 운영되고 있는 일반철도 CTC와 고속철도의 개통과 더불어 운영되던 고속철도 CTC 및 일부 광역도시철도용 CTC를 2010년 철도교통관제센터(서울 구로소재)에 하나로 통합하여 운영하고 있다. 하지만 각 지자체가 운영하는 도시철도 관제실은 아직 각 선구별로 운영 중에 있으며, 여러 측면에서 관제의 통합에 대한 필요성이 제기되고 있다[2,3].

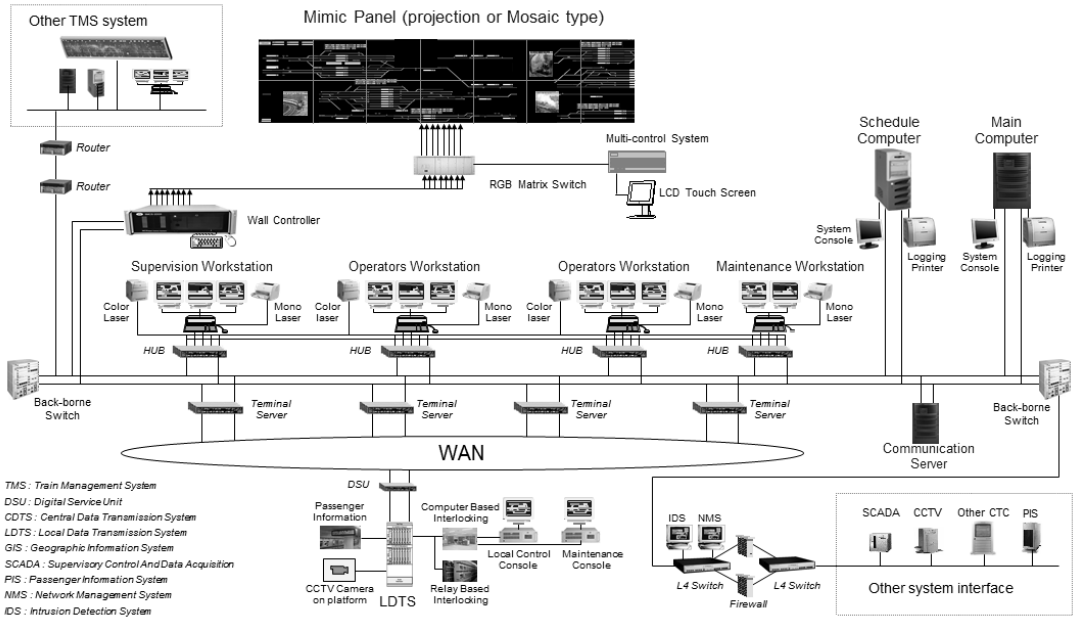
이와 같이 철도에서의 관제시스템은 “대도시 및 주요 철도노선 중첩지역의 철도종합상황실”에 해당하는 국가중요시설로 지정되어 있으며, 경비・보안 계획, 보호구역 설정 및 통제구역의 보호대책에 따라 관제센터의 건물을 포함한 모든 시설물에 대한 보안관리를 실행하고 있다.

일반적으로 초기의 CTC만을 칭하던 관제설비는 운영요건의 다양화와 복잡화에 따라 CTC, 집중원격감시시스템(SCADA: Supervisory Control and Data Acquisition), 정보통신시스템을 관제시스템의 설비로 분류하여 구성하고 있다. 각 설비의 주요업무로 CTC는 전 선구로부터 수집된 데이터를 바탕으로 중앙에서의 직접적인 열차운행 제어, 통제 및 감시를 수행하며, SCADA는 전 구간의 전차선 및 전력 공급장치의 원격제어 및 관리를 담당하며, 정보통신시스템은 광통신망의 모니터링 및 감시를 수행한다.

특히, 관제시스템에서 핵심시스템인 CTC는 전 구간에 대한 원격 감시 및 제어를 담당하고, 관제사에 의해 운행하는 모든 열차에 대한 통제를 수행하고 있으므로 외부로부터의 시스템 접근 및 침입에 대한 방호 및 보안대책은 무엇보다도 중요하다.

본 논문에서는 CTC시스템에 대한 외부로부터의 침입에 대해 분석하며, 이에 대한 보안대책 및 대응방안을 논의한다.

* 한국철도기술연구원 미래광역도시철도연구실 (prolee@krri.re.kr)
** (주)테크빌 연구소 (youngsoo.lee@techville.biz)



〔그림 1〕 일반적인 CTC 구성도

Ⅱ. 본 론

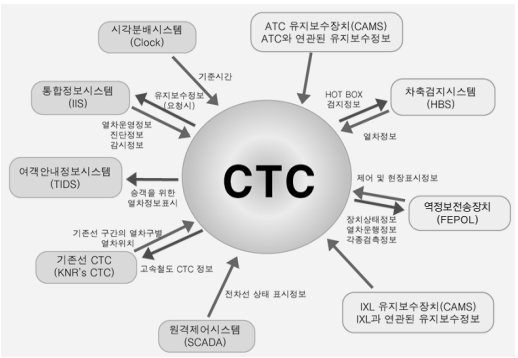
2.1 개 요

철도에서 열차운행을 통제하는 관제시스템의 보안을 확보하기 위하여 일반 통신망을 이용하지 않고 보호용자가 통신망을 구축하여 외부로부터의 접근이나 비정상적인 침입 및 비인가자에 대한 시스템의 접근을 근본적으로 차단하고 있다. 하지만 앞에서 설명한 바와 같이 관제시스템은 여러 가지 역할을 수행함으로 인하여 타 설비와의 인터페이스가 필수불가결하다, 따라서, CTC 시스템에 대한 접근은 크게 다음과 같은 2가지 방법이 고려될 수 있다.

① 연계되는 외부시스템을 통한 접근 : CTC시스템은 관제에 필요한 정보를 송·수신하기 위해, 외부시스템과 인터페이스를 구성하므로 이들 시스템을 통한 접근

② 사용자 인터페이스를 제공하는 콘솔 장치로의 접근 : 운영 및 유지보수를 위한 장치의 USB 포트 등을 통한 바이러스의 침투

위에서 보인 바와 같이 관제시스템에 접근 가능한 2가지의 경로에 대한 보안은 필수적이다.



〔그림 2〕 고속선 CTC와 외부장치간의 인터페이스

2.2 외부 인터페이스 종류

일반적으로 관제센터의 주 컴퓨터 및 통신서버는 현장설비 및 관련된 외부시스템으로부터 열차통제와 관련된 정보를 송·수신하기 위해 인터페이스를 구성한다. CTC의 외부 인터페이스는 주로 DSU(Digital Service Unit)를 통한 직렬 통신 및 CSU/DSU를 통한 TCP/IP 프로토콜을 사용하며, 그 내용은 [표 1]과 같다.

〔표 1〕 외부 인터페이스 방식

통신 방식	상세 내용
직렬 통신	RS-422(4,800~9,600bps) V.24 비동기 방식 이중화 회선(일반적)
LAN 통신	TCP/IP EI급(2.048Mbps) 이중화 회선(일반적)

일반적으로 직렬 통신망을 통한 외부로부터의 침입은 사실상 불가능하지만, LAN 통신에 의한 침입은 가능하므로 CTC시스템은 방화벽을 구축하여 보안을 강화하고 있다. 네트워크 보안에 있어서 방화벽은 외부 네트워크로부터 내부 네트워크를 보호한다는 대전제 아래 효과적으로 네트워크를 보호할 수 있는 기본 도구로 적용된다.

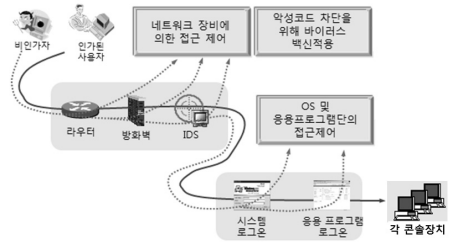
〔표 2〕 고속선 인터페이스의 예[4,5]

연계 시스템	방식	속도 (bps)	연계방식
고속선 - 일반철도 (통합관제)	LAN	1G	백본스위치간
고속선 - 일반철도 (예비관제)	LAN	100M	철도교통 예비관제센타 백본스위치
고속선 통합관제 - 예비관제	WAN	2,048M (E1)x2회선	외부접속 라우터 및 방화벽 이용
SCADA	RS-485	2,400	외부접속 터미널서버 이용
HBS	RS-232	1,200	
TIDS	RS-485	38,400	
FEPOL	RS-485	4,800	
CAMS	RS-485	4,800	
CMS	RS-485	9,600	
고속선감시 콘솔(오송)	WAN	2,048M (E1)	외부접속 라우터 및 방화벽 이용

HBS : Hot Box System
TIDS : Train Indicate Display System
CAMS : Computer Aided Maintenance System
FEPOL : Front End Processor for Operation Level

2.3 콘솔장치의 보안

CTC시스템의 콘솔장치는 운영자 및 유지보수자를 위한 인터페이스를 제공하며, 운영의 편의성을 위해 관련된 각종 정보를 표시하고 사용자의 명령을 처리하는 장치이다. 콘솔장치는 필요시 프로그램의 업그레이드 및 표시 화면의 변경을 위해 USB 포트 등을 사용할 수 있는 경우가 발생한다. 이에 따라 USB 등을 통한 악성 바이러스, 웜 등이 침투하거나 해킹의 수단으로써 이용될 수 있으며, 또한 네트워크를 통한 외부로부터의 침입이 발생할 수 있으므로 이에 대한 대응방안이 고려되어야 한다. [그림 3]은 콘솔장치의 보안 구성을 나타낸다.



〔그림 3〕 콘솔장치의 보안구성 방안

콘솔장치의 보안을 위한 운영방안은 다음과 같다.

① 콘솔장치의 기본 운영 수칙
- 콘솔에 임의적으로 장비의 장착을 금지
- 외장에 봉인을 부착하여 사용자 임의로 콘솔 외장의 개방을 금지
- 콘솔장치에 모뎀을 장착하여 외부망에 접속하는 것을 통제
- 중요한 업무 정보는 콘솔장치의 디스크에 저장하는 것을 금지

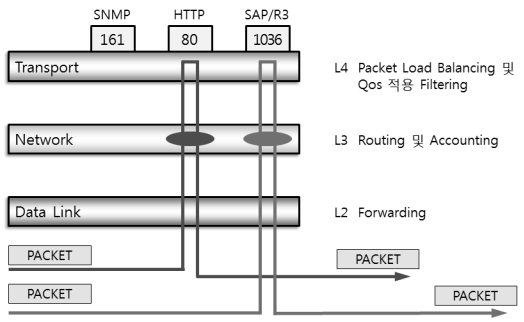
② 패스워드 설정
- 부팅시 CMOS에서 제공하는 암호를 설정
- 윈도우에서 제공하는 화면보호기 및 패스워드를 설정
- 사용자 ID와 동일하거나 추측이 용이한 패스워드의 사용 금지

③ 공유폴더의 관리
- 콘솔장치의 디스크내 모든 폴더는 원칙적으로 공유를 금지
- 공유폴더 사용시 보안담당자에게 사용 목적과 기간, 공유자의 신원정보를 제출하여 승인을 받음
- 폴더 공유시 암호를 설정하여 승인된 사용자만 접근을 허용

2.4 네트워크의 보안

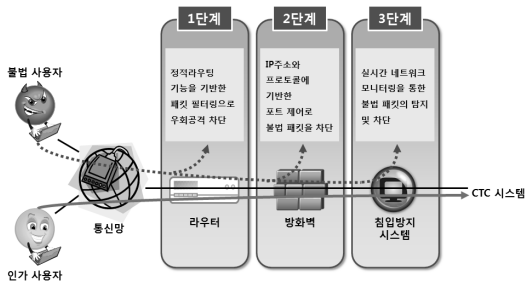
CTC 시스템과 내부 정보를 연계되는 외부 네트워크를 통한 불법적인 접근 및 침입으로부터 보호하기 위해

방화벽, QoS, 침입방지시스템, 안티 바이러스 등을 도입하고 있다.



〔그림 4〕 L4에서의 패킷 흐름

네트워크에 대한 보안 대책은 3단계로 나누어지며, 1단계는 라우터, 2단계는 방화벽 그리고 3단계는 침입방지시스템으로 구성하며 [그림 5]와 같다.

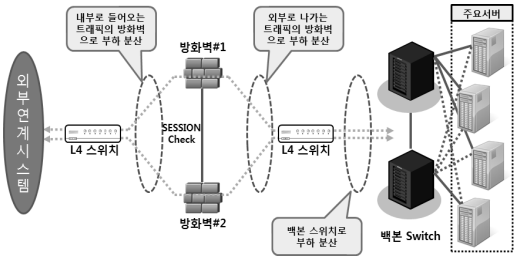


〔그림 5〕 네트워크의 보안 구성

1단계는 L4 스위치의 정적 라우팅 기능을 기반으로 한 패킷 필터링, QoS 적용 필터링으로 우회 공격을 차단한다.

2단계는 방화벽을 구축하여 IP 주소와 프로토콜에 기반한 포트 제어로 불법 패킷을 차단하며, 내부 및 외부로 전송하는 트래픽의 분산 및 로드 밸런싱을 위해 2개의 방화벽으로 구성한다. 방화벽 이중화는 fail- over 기능을 수행하여 방화벽의 장애시 중단없는 서비스를 제공하며, 업무 로드의 분산으로 처리시간 지연의 제거 및 확장이 용이한 장점을 가진다.

3단계는 침입방지시스템을 구축하여 실시간 네트워크 모니터링을 통한 불법 패킷의 탐지하며, 이를 차단하는 기능을 구현한다. 침입방지시스템의 구성 방안은 다음과 같다.



〔그림 6〕 방화벽 이중화 구성

- 비 인가된 사용자의 접근 및 작업 권한의 제한을 위한 보안 네트워크 시스템 구축
- 불법 침입을 막기 위해 강력한 접속자 인증(OTP)과 네트워크 단위의 접속 제한을 위한 보안정책을 지원
- 네트워크 공사로 인한 변경되는 IP 체계 및 네트워크 망을 수용
- 네트워크의 구조 확장 및 변경 용이성을 확보하여 장비의 증설, 철거 및 구성 변경에 따라 발생하는 작업을 지원

이와 같이 라우터, 방화벽, 침입탐지시스템을 유기적으로 구성하여 3차에 걸친 침입저지 단계를 구축함으로써 외부의 불법적인 침입으로부터 CTC 시스템의 네트워크 기밀성을 확보하여 침해 사고에 의한 시스템의 업무 중단을 방지한다.

Ⅲ. 결 론

지금까지 외부로부터의 침입 및 접근을 차단하기 위해, CTC 시스템에 대한 콘솔장치 및 네트워크의 보안 방법을 정의하였다. 더불어 CTC 시스템의 안전한 운용 및 중단없는 동작을 보장하기 위해서는 시스템 전반적인 보안 대책이 강구되어야 한다.

그러므로 CTC 시스템의 컴퓨터 범죄 방지 및 보안 확보를 위하여 네트워크, 서버, 데이터베이스 및 응용 프로그램 등의 영역에서 공통적으로 적용되는 운영 사이클을 적용하여야 하며 그 특징은 다음과 같다.

- 평상시 각종 장치에 대한 로깅 및 상태정보의 지속적인 모니터링
- 일간/주간/월간 등 주기별로 취합된 로그 및 이벤트 분석
- 취합된 로그 및 이벤트에 대해 사용자, 서비스 등

의 필드에 의해 통계치 및 보고서 작성
• 통계치 및 보고서의 분석을 통해 위험 내용에 대한 시정 조치

〔표 3〕 CTC 시스템의 전반적인 보안 방안

구 분	보안 방안
네트워크	- 방화벽(IPS) 설치 및 운영 - 특정 패킷에 대한 필터링 - 불필요한 데몬 및 서비스 제거 - 네트워크 로깅 관리
주컴퓨터	- 사용자 계정 및 패스워드에 대한 관리, 보안 정책의 설정 - 시스템 접근 권한 제한 및 분리 - 파일 시스템에 대한 보안 강화 - 올바른 시스템 구성 및 패치 적용 - 시스템 로그 분석, 감사 및 접근 통제
콘솔 장치	- CMOS 암호 설정, 화면 보호기 기동 및 패스워드 설정 - 파일 공유시 패스워드 설정 - 백신 프로그램의 설치 및 운영
데이터 베이스	- 비권한자의 데이터 접근 통제 - 사용자 및 업무 구분을 통한 계정 및 접근 권한 통제 - DBMS 고유의 보안 기능(Audit) 활용 및 핵심 정보 로깅
응용 프로그램	- 업무구분을 통한 계정 및 권한 통제 - 응용 프로그램별 및 단위 업무별 권한 통제 - 특정 시간대별 접근 통제 - 응용 프로그램 사용상태의 관리

일반적으로 관제시스템은 폐쇄적인 전용 네트워크를 사용하여 내부 및 외부 통신 인터페이스를 구성하고 있지만, 점차 내/외부 네트워크의 불분명화, 네트워크의 고속화, 복잡한 네트워크 환경 등으로 인해 더욱 강력한 보안 대책 및 방안을 수립하여야 한다.

특히, 철도분야의 관제시스템은 항공관제와 더불어 국가의 핵심시설이며, 시스템 운영 장애 및 중단은 열차 운행에 막대한 지장 및 혼란을 초래하므로 국철, 고속철도, 지하철, 경전철 및 지하철에서 운영하는 모든 관제시스템에 대한 보안 대책을 다시 한번 점검하고 보완할 필요성이 요구된다.

참고문헌

[1] G. Sciutto, “State of Art of Computer Application to the Railway Traffic Control and Automation”, *COMPRAIL’98*.

[2] 정종덕, 이영훈 외, “도시철도 스마트 관제 구축방안 연구”, *한국철도학회 춘계학술대회논문집*, pp. 1858-1865, 2012. 5.

[3] 전현덕, “철도통합관제시스템 구축 및 경영”, *한국철도학회 철도저널*, 제8권 제3호, pp. 57-69, 2005. 9.

[4] 철도청, CTC장치:경부고속철도 신호설비, 2007.

[5] 한국철도시설공단, 경부고속철도 2단계 CTC구축 제안요청서, 2008.

〈著者紹介〉

사 진

이 재 호 (Jaeho Lee)
정회원

1987년 2월: 광운대학교 전자공학과 졸업
1989년 9월: 광운대학교 전자공학과 석사
2005년 2월: 고려대학교 메카트로닉스학과 박사
1995년 2월~현재: 한국철도기술연구원 책임연구원
<관심분야> 열차제어시스템보안, 철도통신프로토콜

사 진

이 영 수 (Youngsoo Lee)
1988년 8월: 중앙대학교 전기공학과 졸업
2008년 2월: 서울과학기술대 철도전문대학원 철도전기신호공학과 석사
1988년 9월~2004년 7월: LG산전 철도신호개발팀장
2004년 8월~2010년 4월: 대아티아이(주) 연구소장
2010년 7월~현재: ㈜테크빌 연구소장
<관심분야> 철도시스템, 철도관제시스템, 정보보호