JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 9: 1166~1175, Sep. 2021

스마트시티 내 긴급차량 우선신호 제어시스템 구축과 효과성 분석 및 ISMS-P 기술적 통제항목 개선 방향성 연구

윤태석[1] · 박용석[2*]

Establishment and Effectiveness Analysis of Emergency Vehicle Priority Signal Control System in Smart City and Directions for ISMS-P Technical Control Item Improvement

TaeSeok Yoon[1] · Yongsuk Park[2*]

[1]Graduate Student, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea
[2*]Professor, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea

요 약

국내 스마트시티와 긴급차량 우선신호 제어시스템의 현재 상황과 발전동향을 알아보고, 긴급차량 우선신호 제어시스템의 기존 효과분석과 신호제어시스템의 보안을 위한 국내외 선행 연구 내용을 바탕으로, 긴급차량 우선신호 제어시스템을 구축하고 긴급차량에 실제 적용 및 시험운행을 통해 시간단축의 효과성을 분석하였다. 더불어 실시간 신호시스템 제어의 보안관리 및 안정적인 서비스를 위해 기존 ISMS-P 인증제도와 한국인터넷진흥원 사이버보안 가이드의 보안요구사항과 보안위협 항목에 따른 보안대책의 연관성에 따라 비교하여 맵핑함으로서, 인명구조나 화재 등 긴급상황 발생 시 시민의 소중한 생명과 재산을 지킬 수 있는 골든타임 확보 가능성을 높일 수 있도록 ISMS-P 인증제도의 기술적 통제항목 개선을 제안한다.

ABSTRACT

We investigate the current situation and development trend of domestic smart city and emergency vehicle priority signal control system analyzing the existing effectiveness of 1) emergency vehicle priority signal control system and 2) control emergency vehicle priority signal, based on domestic and foreign prior research for signal control system security. The effectiveness of time reduction was analyzed through actual application and test operation to emergency vehicles after establishing the system. In addition, for security management and stable service of real-time signal system control we propose improvement for the technical control items of the ISMS-P certification system to secure golden time to protect citizens' precious lives and property in case of emergency by classifying and mapping the existing ISMS-P certification system and the Korea Internet & Security Agency's cyber security guide according to the items of security threats.

키워드 : 긴급차량 우선신호, 스마트시티, 스마트교통, 스마트교차로, ISMS-P

Keywords : Priority signal preemption for emergency vehicles, Smart city, Smart traffic, Smart intersection, ISMS-P

Received 18 August 2021, **Revised** 27 August 2021, **Accepted** 9 September 2021

*** Corresponding Author** Yongsuk Park (E-mail:yongspark@sjcu.ac.kr, Tel:+82-2-2204-8062)
Professor, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.9.1166 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

대한민국 스마트도시 조성 및 산업진흥 등에 관한 법률에서는 스마트도시를 “도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시를 말한다” 라고 정의하고 있다[1].

스마트도시법과 국제표준 ISO 37210의 도시성과 평가지표 46개 항목의 내용을 분석한 결과, 스마트도시법의 주된 내용은 스마트도시 조성지원을 통한 활성화의 측면이 강하고, ISO 37210 또한 스마트 서비스의 제공 수준의 평가지표만 있을 뿐 스마트시티 서비스 보안에 관련한 내용은 찾아볼 수 없었다[2].

국토교통부는 우수한 정보통신기술을 바탕으로 유비쿼터스도시 정책을 선도적으로 추진하기 위해, 2008년도 세계최초로 관련 법률인 “유비쿼터스도시의 건설 등에 관한 법률”을 제정 및 시행하고 제1·2차 종합계획에 이어 U-City의 한계 극복을 위해 2017년 “스마트도시법”으로 개편하고, 제3차 스마트도시 종합계획을 발표하여 2023년까지 도시 성장 단계별 스마트시티 맞춤형 조성과 확산을 촉진하고 있으며, 이에 따라 최근 각 지자체에서는 도시에 ICT·빅데이터 등 신기술을 접목하여 각종 도시문제를 해결하고 삶의 질을 개선할 수 있는 다양한 스마트시티 서비스를 도입하고 있으나 보안관련 인증제도나 법적 규제가 미흡하여 보안 위협에 노출되어 있다[3].

본 논문에서는 국내 지방자치단체의 스마트시티 서비스 발전 현황과 긴급차량 우선신호 제어시스템의 도입 배경을 파악하고, 기존 긴급차량 우선신호 제어시스템의 효과 분석과 신호제어시스템 보안에 관한 국내외 선행연구 내용을 알아보고, ISMS-P 보안 인증제도의 기술적 통제 항목과 한국인터넷진흥원의 안전·재난·환경 사이버보안 가이드의 스마트 긴급차량 우선신호 분야를 항목별로 맵핑하여 스마트시티 내 긴급차량 우선신호 제어시스템의 안전한 서비스 운영을 위하여 ISMS-P 인증제도의 기술적 통제항목 개선을 제안한다.

Ⅱ. 스마트시티 서비스 발전동향과 긴급차량 우선신호 제어 시스템의 도입 배경

국내의 스마트시티는 2003년도 화성동탄, 송도, 판교 등 U-City 구축사업으로 시작되었으며, 2008년도 유시티법 제정이후 2013년도 까지 건설과 정보통신산업의 융복합 신성장 육성을 1단계로, 2014년부터 2017년도까지 공공을 중심으로 한 정보시스템 연계사업의 일환으로 스마트시티 통합플랫폼을 전국 지자체에 보급하는 2단계 사업과 더불어 스마트도시법으로 전면개정을 시행하였으며, 2018년도 스마트시티 추진전략과 스마트도시 종합계획을 발표하고 도시문제 해결과 혁신 생태계 육성 목표라는 3단계를 추진하고 있다[3].

4차산업혁명위원회와 관계부처가 합동으로 제시한 스마트시티 서비스 개요도를 살펴보면 교통, 환경, 공공안전 등으로 구성되어 있으며, 긴급차량 우선신호 제어시스템은 교통분야가 아닌 공공안전 분야의 사고 및 범죄 긴급구난에 포함되어 있다<그림 1>[4][5].

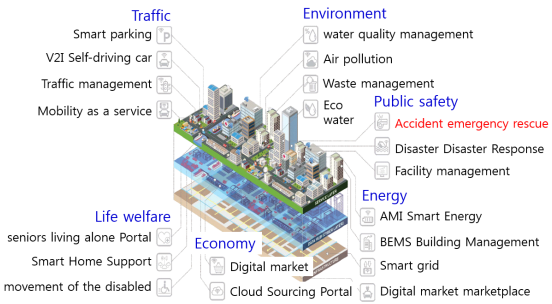

Fig. 1 Smart City Service Overview

국내의 스마트시티 추진 지자체는 정부의 다양한 정책 추진과 확산 노력에 힘입어 수도권은 물론 지방도시까지 확대되어 2019년 총 67곳으로 집계 되었고, 지방자치단체의 스마트시티 조성을 위해 국토교통부에서 보급하는 스마트시티 통합플랫폼은 2019년도까지 49개 지자체에 구축을 완료하고, 2022년도까지 108개 지자체에 스마트시티 센터를 구축 할 예정이다[3].

지자체 스마트 서비스의 사업 유형을 연도별로 재구성한 결과 2014년의 경우 방범 및 방재가 35%, 교통서비스 32%로 2개 분야가 전체의 67%를 차지하였으나, 2018년도 서비스 현황은 <표 1>과 같이 보다 다양한 서비스의 사업비율이 확대되는 것을 확인할 수 있었다[3].

Table. 1 Reconstruction of the smart city service status of local governments

Service Classification	2014 Expense ratio	2018 Expense ratio
Crime prevention, Disaster prevention	35%	24%
Traffic	32%	22%
Administration	-	15%
Environment, Energy, Water Resources	-	15%
Facility management	-	8%

스마트시티의 서비스 분야중 24%를 차지한 방범 및 방재 부문은 행전안전부의 가이드라인에 따라 자가망 및 전용회선을 이용한 폐쇄망으로 구성되어 있으나, 22%를 차지하는 교통서비스는 경찰청 표준규격에 따라 무선망을 적용하고 있어[6], 신호제어시스템의 교통신호제어기와 무선통신을 사용하는 디바이스로 구성된 긴급차량 우선신호 제어시스템의 보안 취약점 분석을 통한 보안통제항목 개선을 본 논문에서 연구하고자 한다.

한편 국토교통부는 2018년도부터 전국 지자체에 긴급차 우선 신호 시스템 44개소를 설치하였으며, 2021년 4월30일 보도자료를 통해 교통량을 실시간 분석하고 긴급차에 우선신호를 보내는 '스마트 신호운영 시스템'을 전국으로 확대 구축하겠다는 계획에 따라 2021년도에만 19개 지자체 372개소에 긴급차량 우선신호 시스템을 구축할 계획이라고 발표하면서, 긴급차량 우선신호 제어시스템은 긴급차량의 목적지를 사전에 공유하고 긴급차량의 이동경로에 따라 교차로 신호를 일시적으로 제어하여 우선 통행할 수 있도록 맞춤형 신호를 부여하여 사고처리 시간 단축 및 골든타임 확보에 효과가 있다고 설명하고 있어 본 논문에서 실제 긴급차량에 적용하여 우선신호 도입 효과를 분석하기로 하였다[7].

우선 긴급차량 우선신호 제어시스템을 크게 현장제어방식<그림 2>과 센터제어방식<그림 3>의 구성도로 작성하였다.

현재 경찰청의 표준 규격은 현장제어 방식의 긴급차량 우선신호 시스템의 표준규격만 마련되어 있으나[8], 현장제어방식은 목적지까지의 모든 교차로의 신호제어기마다 현장장치를 별도로 설치하기 때문에 비용이 많이

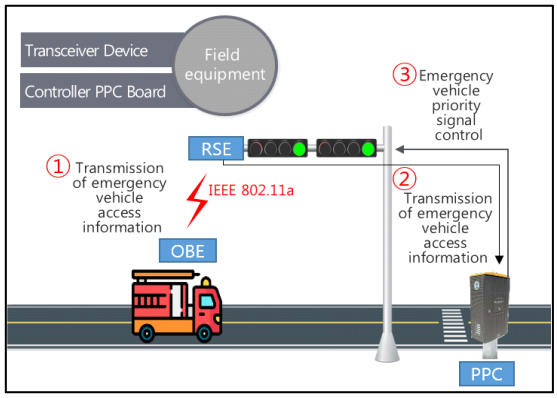

Fig. 2 Field control method emergency vehicle priority signal configuration diagram

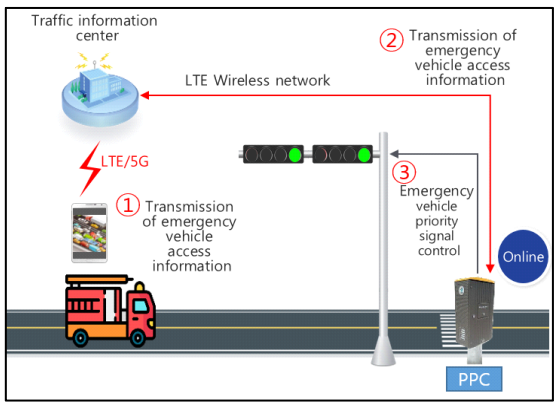

Fig. 3 Center control method emergency vehicle priority signal configuration diagram

들고 유지보수 또한 어려워, 경기도 수원시와 대전광역시 등 다수의 지자체에서는 현장제어 방식에 비해 구축비용이 적게 들고 우선신호 구간 확장시 추가설비 없이 센터에 연결된 모든 교차로에 적용이 가능한 센터제어방식의 긴급차량 우선신호 시스템을 구축하고 운영하고 있어 본 논문에서는 보다 효율적인 센터제어방식을 도입하여 효과성 분석을 실시하였다[9].

Ⅲ. 긴급차량 우선신호 시스템의 적용효과 분석

긴급차량 우선신호시스템 도입에 따른 효과분석의 선행연구로 조성만(2020)은 대전광역시의 긴급자동차 출동이력자료를 바탕으로 분석 대상구간을 선정하고,

신호현시와 교통량 등 자료 수집을 통해 미시적 시뮬레이션 프로그램인 VISSIM을 활용하여 긴급자동차 우선신호 도입 전·후의 통행속도와 시간 단축효과를 시뮬레이션 방식으로 분석하였다[10].

본 논문에서는 실제 긴급차량의 운행을 실시하여 우선신호 도입의 효과성을 분석하기 위하여 파주시 교통정보센터에 교차로 신호제어를 위한 센터 소프트웨어를 개발하여 설치하고, 긴급차량 디바이스에서 운영할 안드로이드 전용앱을 개발하여 스마트폰에 탑재하였으며, 교차로에 설치된 신호제어기를 온라인으로 실시간 제어하기 위하여 통신회선을 LTE망으로 교체하여 '센터 제어방식'의 긴급차량 우선 신호시스템으로 구성하였다<그림 4>.

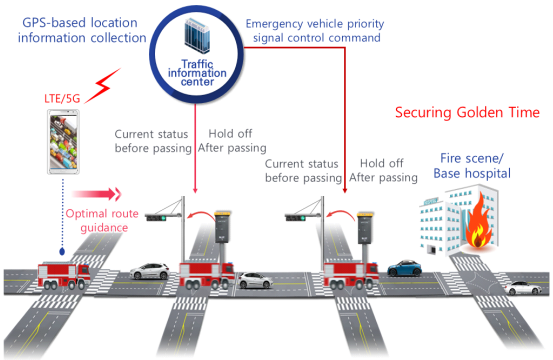

Fig. 4 Paju City Emergency Vehicle Priority Signal Service Concept Map

센터 제어 방식 긴급차량 우선신호 시스템은 긴급차량에 설치된 전용단말기로 화재현장 등 목적지를 설정하면 최적의 경로를 안내하고, 경로와 현재위치 등을 센터로 전송하게 된다. 센터에서는 최종 목적지까지 설정된 신호제어기에 제어 명령을 내리고, 해당 교차로에 긴급차량이 도착하는 예정시간에 따라 신호현시를 유지하고, 긴급차량이 통과하면 현시유지 제어모드를 해제하고 일반 신호운영 상태로 복귀한다.

긴급차량 우선신호 제어시스템은 긴급차량 단말기의 위치정보를 수신하고 신호제어기의 상태정보를 전송하는 DMZ존과 교차로에 설치된 신호제어기를 실시간 제어하는 신호존으로 분리하여, 망연계 장비를 통해 데이터를 안전하게 연계하도록 구성하였다<그림5>.

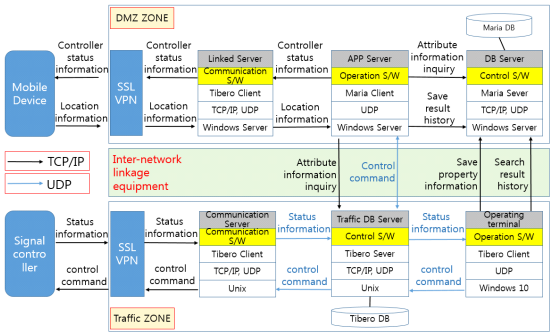

Fig. 5 Paju City Emergency vehicle priority signal control data flow chart

긴급차량 우선신호 제어시스템의 기능에 따른 구성요소는 긴급차량 단말기와 신호운영단말 그리고 우선신호제어서버로 구성하였으며 기능은 아래와 같이 구현하였다<표 2>.

Table. 2 Component-specific function definitions

Component	Function definition
Emergency vehicle device	1. Priority signal section selection 2. Priority signal section display 3. Signal controller display 4. Signal controller status display 5. Service termination
Signal control operation terminal	1. Emergency vehicle basic data management 2. Accept/reject priority signal request 3. Priority signal automatic acceptance setting 4. Priority signal processing result history 5. Priority signal statistical processing
Priority signal control server	1. Allow automatic acceptance of emergency vehicle priority signal 2. Receiving emergency vehicle location information 3. Predicting the arrival of emergency vehicles at intersections 4. Priority signal control and release 5. Automatic release of priority signal path departure

긴급차량 도입 효과 분석에 앞서 파주시 남북철도교통과와 파주소방서의 협조로 정체가 가장 심한 주요도로 2개 구간을 <그림 6>과 <그림 7>과 같이 선정하고, 각 구간에 해당하는 모든 교차로의 신호현시를 조사하여 현행화하고 실시간 온라인 제어 상태를 확인하였다.

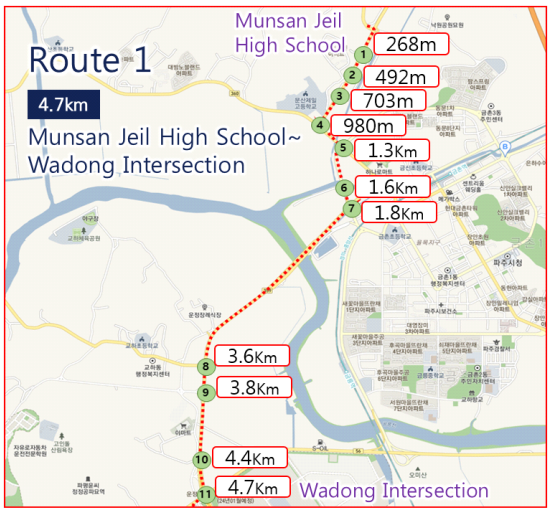

Fig. 6 Emergency vehicle priority signal application survey section route 1

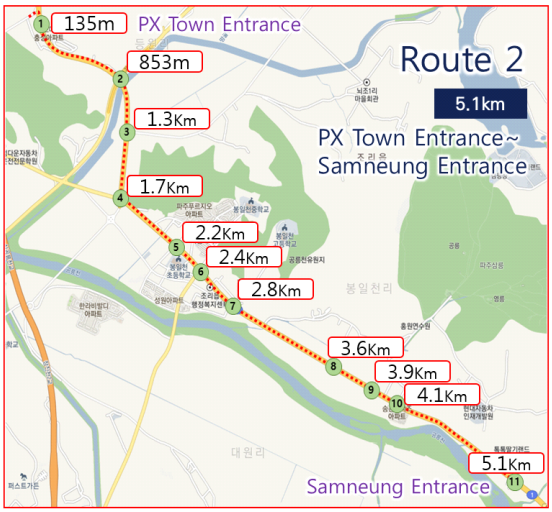

Fig. 7 Emergency vehicle priority signal application survey section route 2

조사 방식은 2개조로 나누어 1조는 일반승용차에 탑승하여 현장조사 양식에 우선신호 미적용시 출발시간과 도착시간을 기입하였고, 2조는 30분 후 실제 긴급차량에 탑승하여 우선신호를 적용한 출발시간과 도착시간을 기입하였다.

2개 구간의 효과분석을 위해 각 구간별로 1일차에는 비첨두시 2회를 실시하고, 2일차에는 오전첨두와 비첨두, 오후첨두 3회를 실시하여 전체 4일간 2개 구간에서 총 10회의 현장조사를 통해 긴급차량 우선신호 시스템 미적용시 대비 적용시의 단축시간을 계산하여 비첨두시와 첨두시의 평균 단축효과를 분석하였다<표 3>.

Table. 3 Comparison of travel time before and after emergency vehicle priority signal application

Division	Applicable section	Distance traveled (km)	Emergency vehicle priority signal not applied Departure time (Hour:Minute)	Emergency vehicle priority signal not applied Driving time ①	Emergency vehicle priority signal application Departure time (Hour:Minute)	Emergency vehicle priority signal application Driving time ②	Shortened time (②-①)	Shortening effect (%)
1	Munsan Jeil High School ~ Wadong Intersection (Off-peak hours)	4.7	14:05	09:25	14:36	06:20	-3:05	32.7%
2			15:06	06:58	15:33	04:36	-2:22	34.0%
3			14:43	08:36	14:35	05:02	-3:34	41.5%
4	Munsan Jeil High School ~ Wadong Intersection (Peak hour)	4.7	08:39	08:38	08:15	05:22	-3:16	37.8%
5			17:29	13:12	17:44	07:37	-5:35	42.3%
6	PX Town Entrance~ Samneung Entrance (Off-peak hours)	5.1	14:02	10:37	16:02	06:00	-4:37	43.5%
7			16:22	10:00	16:43	05:47	-4:13	42.2%
8			15:12	09:19	15:05	05:02	-4:17	46.0%
9	PX Town Entrance~ Samneung Entrance (Peak hour)	5.1	08:06	10:17	07:56	05:19	-4:58	48.3%
10			17:18	13:48	17:28	08:04	-5:44	41.5%
Average effect	Off-peak hours Effect of application	4.9	14H~16H	09:24	14H~16H	06:01	-3:41	40.3%
	Peak hour Effect of application		08~09H/ 17~18H	11:28	08~09H/ 17~18H	06:35	-4:53	42.6%

2개 조사구간의 평균 거리는 약 4.9Km 이며, 비첨두시간 적용효과는 2개 구간 평균 약 3분 41초 단축되었고, 시간 단축효과는 40.3% 였으며, 출퇴근 첨두시의 적용효과는 미적용시 평균 통행시간 11분 28초에서 적용시 6분 35초로, 약 4분 53초 통행시간 단축과 42.6%의 단축 효과를 보여, 비첨두시보다 첨두시에 긴급차량의 우선신호의 통행시간을 더욱 단축하는 효과가 있음을 도출하였다[11].

Ⅳ. 긴급차량 우선신호 시스템의 보안위협과 ISMS-P 기술적 통제항목 개선방안

한국인터넷진흥원은 보도자료를 통해 2020년 7대 사이버 공격 전망을 발표하며, 융합서비스를 노리는 새로운 보안위협의 등장(빛스캔)이라는 제목으로 교통시스템 해킹을 통한 교통마비와 같은 스마트시티 보안 위협이 등장할 것으로 전망하며 사이버 공격에 대한 경각심을 일깨웠다[12].

교통신호제어시스템의 보안위협에 관련된 해외 선행연구를 살펴보면, 인도의 L. Sumia(2018)는 교차로 신호시스템과 긴급차량 사이의 간격을 측정한 다음 교통신호가 해킹되었는지 확인하고, 사고유형 및 응급차량

유형을 고려하여 신호시스템에 긴급차량 우선신호제어권을 할당하는 방식을 연구하였으며[13], 카타르의 Elyes Ben Hamida(2015)는 신호제어시스템의 보안 위협을 분석하고, 안전한 메시지의 서명과 검증을 위해 타원곡선 디지털 서명 알고리즘을 활용하여 신호대기시간에 영향을 주지 않는 교통신호제어 알고리즘을 제안하였다[14].

국내의 선행 연구로 김병기(2019)는 "스마트교통 분야 내 자율주행 자동차의 ISMS-P 기술적 통제항목 개선을 위한 연구"에서 자율 주행 자동차의 V2X, V2D, V2I, V2N 시스템에서의 보안 취약점을 파악하고, 한국인터넷진흥원의 스마트교통 사이버보안 가이드의 보안요구사항에서 제시한 내용을 토대로 ISMS-P의 기술적 통제항목의 개선사항을 제안하였다[15].

본 논문에서는 긴급차량 우선신호 제어시스템이 포함된 한국인터넷진흥원의 안전·재난·환경 사이버보안 가이드의 보안위협을 논문 구성에 맞게 재구성하였다<표 4>[16].

Table. 4 Cyber Security Guide Security Threat Reconstruction

Security threat	Security Threat Description
Software/firmware Tampering and Abuse	- Illegally forge or falsify the software and firmware of emergency vehicle terminals, or exploit vulnerabilities to insert malicious code or illegally access sensitive data
Transmission message leaks and tampering	- Illegally leaking or tampering with sensitive data transmitted through wired/wireless networks between emergency vehicle system equipment
Stored data breach and tampering	- Illegally leaking or tampering with operation-related important or sensitive data stored inside the system
Camouflage (Spoofing)	- Attempts to illegally access emergency vehicle service by disguising as a legitimate user or terminal
Physical interface Access	- Illegally replacing or stealing firmware through access to the physical interface of the terminal or inserting malicious code without permission
Weak network service	- Attempt to access the server or sensitive data through unnecessary network services of emergency vehicle terminals that have not been removed
Insufficient security configuration options	- Unauthorized access to IoT devices is allowed due to insufficient security configuration such as application of strong passwords for terminals and systems, application of encryption, and setting of access rights by user authority
Denial of service attack	- Inducing a large amount of network traffic, depleting terminal resources and bandwidth, or interfering with normal emergency vehicle priority signal control service through radio signal interference or crosstalk
Random attack	- Attempts to illegally access a terminal or network by performing a random attack on user authentication information

다음으로 ISMS-P 인증기준 세부점검 항목 중 논문과의 연관성을 고려하여 기술적 통제항목 5개 분야 28개 항목을 비교 대상으로 도출하였다<표 5>[17].

Table. 5 Derivation of technical control items for ISMS-P

Control items	Detailed control items	
2.5 Authentication and Permission Management	2.5.1	User Account Management
	2.5.2	User identification
	2.5.3	User authentication
	2.5.4	Password Management
	2.5.5	Manage special accounts and privileges
	2.5.6	Review access rights
2.6 Access control	2.6.1	Network access
	2.6.2	Information system access
	2.6.3	Application access
	2.6.4	Database access
	2.6.5	Wireless network access
	2.6.6	Remote access control
	2.6.7	Internet access control
2.7 Encryption Enforcement	2.7.1	Apply password policy
	2.7.2	Encryption key management
2.8 Information system introduction/ development security	2.8.1	Defining security requirements
	2.8.2	Security Requirements Review and Examination
	2.8.3	Separation of test and operating environment
	2.8.4	Test data security
	2.8.5	Source program management
	2.8.6	Operational environment transfer

Control items	Detailed control items	
2.9 System and service operation management	2.9.1	Change management
	2.9.2	Performance and fault management
	2.9.3	Backup and recovery management
	2.9.4	Log and access record management
	2.9.5	Check log and access history
	2.9.6	Time synchronization
	2.9.7	Reuse and disposal of information assets

<표 6>은 <표 5>에서 도출한 ISMS-P 기술적 통제항목에 맞춰 사이버보안 가이드의 보안 요구사항을 논문 구성에 맞게 비교하여 분리하였고, <표 7>은 보안 요구사항에 해당하는 보안 위협을 모두 매칭하였다.

Table. 6 Comparison of ISMS-P and Cybersecurity Guide Security Items

ISMS-P Control items	Cyber security Guide Requirements
2.5 Authentication and Permission Management	- User authentication and role grant
2.6 Access control	- Device authentication and status check - Network Security - Hardware security - Integrated hacking attack detection and response
2.7 Encryption Enforcement	- Cryptographic technology
2.8 Information system introduction/ development security	- Firmware and software security - Save data protection - Secure update
2.9 System and service operation management	- Audit log - Security management

Table. 7 Security threat matching by security requirements

Cyber security Guide Requirements	Cyber Security Guide security threat
User Authentication and Role Granting	- Camouflage(Spoofing) - Insufficient security configuration options - Random attack
Device authentication and status check	- Camouflage(Spoofing) - Denial of service attack
Network security	- Vulnerable network services
Hardware security	- Physical interface access
Integrated hacking attack detection and response	- Denial of service attack
Encryption technology	- Software/firmware tampering and abuse - Leakage and tampering of transmitted messages - Store data leaks and tampering - Camouflage(Spoofing)
Firmware/Software Security	- Software/firmware tampering and abuse
Protect stored data	- Store data leaks and tampering
Safe update	- Software/firmware tampering and abuse
Audit log	- Insufficient security configuration options
Security management	- Insufficient security configuration options

<표 6>과 <표 7>의 비교표를 바탕으로 ISMS-P 기술적 통제항목에 대한 안전·재난·환경 사이버보안 가이드의 스마트 긴급차량 우선신호 서비스 보안 요구사항과 보안위협을 항목별 맵핑도로 구성하였다<그림 8>.

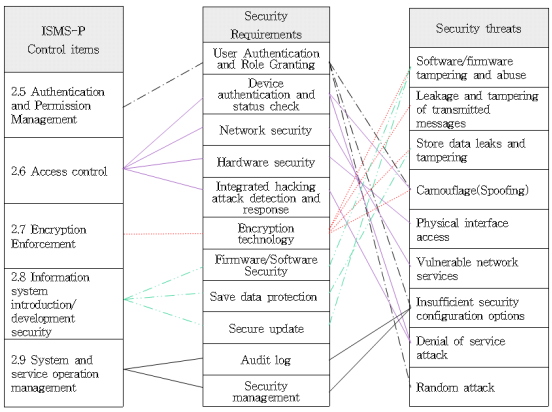

Fig. 8 Mapping diagram for security requirements and security threat items in the cybersecurity guide for ISMS-P technical control items

<그림 8>의 맵핑도에 따라 안전·재난·환경 사이버보안 가이드의 스마트 긴급차량 우선신호 서비스의 보안 대책을 적용하여 긴급차량 우선신호 제어시스템에 적합한 주요 확인사항을 토대로 ISMS-P의 기술적 통제항

목과의 연관성을 고려하여 중복사항을 제외하고 개선 사항을 도출하였다<표 8>.

Table. 8 ISMS-P technical control item improvement plan for emergency vehicle priority signal system

ISMS-P control field	Detail Contents	Key points to check
2.5 Authentication and Permission Management	The priority signal system should establish password combination rules or security configuration options for privilege escalation attempts to control unauthorized access due to spoofing attacks or random attacks.	- Is the password combination rule applied to the vehicle terminal? - Does it control attempts to escalate privileges? - Is the certification information secured?
		- Are password strengthening options configured and privileges separated by role?
		- Is it prepared for a software random attack?
2.6 Access control	Forced access through the physical interface of the priority signal system and access control due to vulnerable network services should be implemented.	- Is role-based access control?
		- Does the organization control access to vehicle terminals disassembled and storage media for vehicles? - Is unauthorized access controlled through the terminal port?
		- Are open ports blocked from being identified?
		- Is Denial of Service (DoS) attack blocked? - Is it blocking radio signal jamming attacks?
2.7 Encryption Enforcement	Encryption policies shall be established to prevent leakage and falsification of emergency vehicle priority control data and storage data.	- Is it encrypting sensitive information over the wireless network? - Are collection and theft of wireless signal constrolled? - Is a secure version of SSL used?
		- Does it prevent leakage and falsification of stored data of vehicle terminals? - Does it prevent leakage and falsification of stored data of center control servers and operating terminals?
2.8 Information system introduction/ development security	Measures to prevent abuse and falsification of software and firmware on emergency vehicle priority control servers and terminals shall be established and implemented.	- Are unsafe software/ firmware updates reviewed? - Are web and mobile interface vulnerabilities checked? - Are development source code security vulnerabilities checked?
2.9 System and service operation management	The operation plan for the audit log, security alert, and encryption option of the emergency vehicle priority control system should be established and implemented, and the status of policy application should be managed.	- Are encryption options managed for in-vehicle terminals? - Are audit logs generated and stored? - Are security alerts monitored and managed?

Ⅴ. 결론 및 시사점

우리나라는 국토교통부의 스마트 서비스 확산 사업에 따라 각 지방자치단체의 스마트시티 센터를 중심으로 교통, 안전, 재난, 환경 등의 서비스를 통합하여 도입함으로서 시민서비스의 향상에 큰 도움이 되고 있지만, 방대해진 서비스만큼 보안 위협에 따른 대응과 더불어 전문인력에 의한 보안인증제도의 도입과 관리가 필요한 현실이다.

ISMS-P 인증 심사 항목은 나날이 발전하고 있는 다양한 스마트 서비스를 안전하게 제공하기 위한 상세 항목을 충분히 포함하기 어렵고, 지방자치단체의 스마트시티센터는 의무적인 ISMS-P 인증 심사 대상이 아니기 때문에 KISA에서 운영중인 ISMS-P 인증심사를 받은 지자체의 스마트시티 센터는 2021년 7월까지 서울특별시 한 곳 뿐이다[18].

본 논문에서는 지방자치단체의 스마트시티에서 점차 확대하여 도입중인 긴급차량 우선신호 제어시스템의

안전하고 안정적인 서비스 제공을 위해, 실제 긴급차량을 이용한 효과성 분석을 실시하고 국내외 교통신호시스템 관련 선행연구를 고찰하여, 한국인터넷진흥원의 사이버보안가이드에 따른 보안 위협과 보안 요구사항을 파악하고, ISMS-P 기술적 통제항목과의 항목별 맵핑을 통해 국민의 소중한 생명과 재산을 지킬 수 있는 긴급차량 우선신호 제어시스템의 ISMS-P 기술적 통제항목 개선을 제안 하였다.

긴급차량 우선신호 제어시스템의 효과 분석을 위한 선행연구는 가상의 시뮬레이션으로 가상적인 효과를 분석하여, 실제 긴급차량에 도입하여 운행시에 일어날 수 있는 교차로 신호제어기의 신호현시 비동기화로 인한 극심한 교차로 정체나 돌발상황의 반영이 어려웠지만, 본 논문에서는 실제 긴급차량에 적용하여 효과분석을 실시하였기 때문에 보다 현실적이고 정확한 단축효과를 확인할 수 있었다.

ISMS-P 기술적 통제항목 개선 또한 사이버 보안 가이드의 보안요구사항 뿐 아니라 보안위협과 그에 따른 보안대책까지 비교하여 맵핑함으로서 긴급차량 우선신호 제어시스템의 안전한 서비스 운영에 적합한 상세한 보안 확인사항을 도출하였다.

앞서 설명한 바와 같이 지방자치단체의 스마트시티 센터는 의무적인 ISMS-P 인증 심사 대상이 아니기 때문에 긴급차량 우선신호 제어시스템을 신규 구축할 경우 국토교통부나 지자체에서는 본 논문에서 도출한 기술적 통제항목 준수를 권고하고, 주요정보통신기반시설 기술적 취약점 분석・평가 방법 상세가이드에 반영이 필요하다.

향후 긴급차량 우선신호 제어시스템의 전국 확대시 인근 지자체의 스마트시티 간 정보연계로 긴급상황에 빠르고 효과적으로 공동 대응 할 수 있도록 소방청과 경찰청, 국토교통부와 한국인터넷진흥원 등 관계부처를 중심으로 하는 기술 표준 마련과 함께 스마트시티센터의 안전한 실시간 신호제어를 위한 보안 인증제도의 체계 수립과 관리방안에 대한 후속 연구가 필요하다.

References

[1] Ministry of Legislation. The Act on the Creation of Smart Cities and the Promotion of Industries, etc. [Internet]. Available: http://www.law.go.kr/.

[2] ISO 37120 briefing note: The first ISO International Standard on city indicators, 2015. [Internet]. Available: https://www.iso.org/.

[3] Ministry of Land, Infrastructure and Transport. 3rd Smart City Comprehensive Plan, 2020. [Internet]. Available: https://www.molit.go.kr.

[4] Fourth Industrial Revolution Committee. Smart City Promotion Strategy for Urban Innovation and Future Growth Motives, 2018. [Internet]. Available: https://www.korea.kr/.

[5] The Korea Information and Communication Technology Association. Key Convergence Cases of the Fourth Industrial Revolution Smart City Concept and Standardization Status, 2018. [Internet]. Available: https://www.tta.or.kr.

[6] National Police Agency. Standard Specification For Traffic Signal Controller, 2019.

[7] Ministry of Land, Infrastructure and Transport. 'Smart Signal Operation System' that analyzes traffic volume in real time and sends signals to emergency vehicles will be expanded nationwide, 2021. [Internet]. Available: https://www.molit.go.kr.

[8] National Police Agency. Standard Specification for Emergency Vehicle Priority Signal System, 2019.

[9] Suwon City. Applies to emergency vehicle priority signal system, fire truck, and police vehicle, 2021. [Internet]. Available: https://www.suwon.go.kr/.

[10] S. M. Jo, “A Study on the Effectiveness Analysis according to Preemption System for Emergency Vehicle,” Graduate School of Information Security at Hanbat University, 2020.

[11] Paju City. Secure 'Golden Time' with emergency vehicle priority signal system, 2021. [Internet]. Available: https://www.paju.go.kr.

[12] Korea Internet & Security Agency. In 2020, who will threaten my daily life?, 2019. [Internet]. Available: https://www.kisa.or.kr/

[13] L. Sumi and V. Ranga, “Intelligent Traffic Management System for Prioritizing Emergency Vehicles in a Smart City,” *International Journal of Engineering*, vol. 31, no. 2, pp. 278-283, 2018.

[14] E. B. Hamida, H. Noura, and W. Znaidi, “Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures,” *Electronics*, vol. 4, no. 3, pp. 380-423, 2015.

[15] B. K. Kim, “A Study on Improvement of ISMS-P Technical Control Items for Autonomous Vehicles in Smart Transportation Sector,” Graduate School of Information Science at Soongsil University, 2019.
[16] Korea Internet & Security Agency. Cybersecurity Guide for Safety, Disaster and Environment, 2019. [Internet]. Available: https://www.kisa.or.kr/.
[17] Korea Internet & Security Agency. ISMS-P Detailed inspection items for certification criteria, 2019. [Internet]. Available: https://isms.kisa.or.kr/
[18] Korea Internet & Security Agency. ISMS-P Certificate issuance status, 2021. [Internet]. Available: https://isms.kisa.or.kr/.

윤태석(TaeSeok Yoon)
숭실사이버대학교 컴퓨터정보통신학과(학사)
세종사이버대학교 정보보호대학원 석사과정
현재 한국정보기술(주) 공공사업본부 부장
※관심분야 : 스마트시티, 지능형교통체계, 스마트교차로, 긴급차량 우선신호

박용석(Yongsuk Park)
서강대학교 컴퓨터학 (학사)
뉴욕(POLY) 대 (석사, 박사)
AT&T (Bell) Labs, 삼성전자
현재 세종사이버대학교 정보보호대학원 주임교수
현재 세종사이버대학교 IT학부 교수
※관심분야 : IT서비스 및 보안, 산업보안, 4차산업혁명, 클라우드, IoT 등