자율주행차 보안 위협 대응을 위한 보안 수준 점검 항목의 상대적 중요도 분석

An Analysis of the Relative Importance of Security Level Check Items for Autonomous Vehicle Security Threat Response

임 동 성*

* 주저자 및 교신저자 : 오산대학교 사이버보안과 조교수

Dong Sung Im*

* Dept. of CyberSecurity, of Osan University

† Corresponding author : Dong Sung Im, seaids@osan.ac.kr

Vol. 21 No.4(2022)
August, 2022
pp.145~156

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2022.21.4.145

Received 27 August 2021
Revised 9 September 2021
Accepted 20 July 2022

요 약

본 연구는 자율주행차 보안 강화를 목적으로 자율주행차 특징, 보안 위협, 국내외 컴플라이언스 등 자율주행차 보안 관련 현황 분석을 통해 보안 수준 점검 항목을 도출하였고 이를 토대로 AHP 모형에 적용하여 상대적 중요도를 확인하였다. 실증 분석 결과 사이버보안 관리체계 수립·이행, 암호화, 위험평가 등의 순으로 중요도 우선 순위가 나타났다. 본 연구의 의의는 자율주행차관련 보안 수준 점검 항목을 도출하고 연구 모형을 실증함으로써 인명 피해까지 초래할 수 있는 사이버 보안 사고 감소 및 관련 기업들의 자율주행차 보안 관리 수준을 향상시킬 수 있다. 그리고 자율주행차 점검 항목의 상대적 중요도를 고려하여 점검을 수행한다면 보안 수준을 조기에 식별할 수 있을 것이다.

핵심어 : 자율주행차, 보안, 사이버보안 관리체계, V2X, AHP

ABSTRACT

To strengthen the security of autonomous vehicles, this study derived checklists through the analysis of the status of autonomous vehicle security. The analyzed statuses include autonomous vehicle characteristics, security threats, and domestic and foreign security standards. The derived checklists are then applied to the AHP(Analytic Hierarchy Process) model to find their relative importance. Relative importance was ranked as one of cyber security management system establishment and implementation, encryption, risk assessment, etc. The significance of this study is to reduce cyber security incidents that cause human casualties as well improve the level of security management of autonomous vehicles in related companies by deriving the autonomous vehicle security level checklists and demonstrating the model. If the inspection is performed considering the relative importance of the checklists, the security level can be identified early.

Key words : Autonomous vehicle, Security, Cyber Security Management System, V2X, AHP

Ⅰ. 서 론

정부는 오는 2027년까지 레벨4 자율주행차 상용화를 목표로, 1조 974억원을 자율주행 기술부문에 투자한다고 하였다. 또한 삼정 KPMG 조사에 따르면, 국내 자율주행차 시장 규모는 2035년 26조, 글로벌 시장 규모는 1334조원로 지금보다 150배 성장할 것으로 전망하고 있다(Yonhap News, 2021). 이처럼 정부 투자 및 시장 규모 확대로, 운전자 개입없이 스스로 움직이는 자율주행차는 스마트폰이 기존 휴대폰을 찰라에 대체했듯이 기존 자동차를 빠르게 대체할 것이다. 자율주행차는 4차 산업 혁명의 신기술을 통해 차안에서 운전자가 사무공간처럼 일을 하거나 인포테이먼트로 휴식을 취할 수 있고, 노약자와 같은 교통 약자에게 이동성 증대 등의 다양한 편의성을 제공할 것이다. 또한 보다 나은 안전성 확보를 위해 차량과 차량, 차량과 교통 인프라 등과의 외부 연결을 확대하고 있다.

그러나 자율주행차의 지능화 및 연결성 확대는 편의성을 배가시키지만, 사이버 공격을 위한 접점이 확대되어 결국 자율주행차의 보안 위협도 증가하고 있다. 가장 많이 알려진 자율주행차 보안 위협 사례 경우로, 2015년 7월 Black Hat USA 2015에서 Charlie Miller와 Chris Valasek이 약 18㎞ 떨어져 있는 Jeep 체로키 차량을 대상으로 해킹을 시연하였다. 이때 원격에서 차량의 속도와 방향을 자유자재로 움직였고 이로 인해 피아트 크라이슬러 오토모빌스(Fiat Chrysler Automobiles)는 약 140만대의 차량에 대해 소프트웨어 보안 업데이트 리콜을 시행하였다(Wired, 2021). 그리고 16년 중국 텐센트의 킨시큐리티랩에서 테스라 모델 S 차량을 원격 해킹하여 브레이크를 급제동하는 상황을 연출하는 등 다양한 보안 위협 사례들이 지속적으로 보고되고 있다. 또한 기존 IT 환경의 경우 해킹시 생명과는 거리가 먼 사이버 영역에서의 피해이지만, 자율주행차에 대한 사이버 공격 피해는 도로의 마비, 인명 피해 등 물리적 환경에 직접 영향을 미칠 수 있기 때문에 체계적인 보안 대응체계가 필요할 것이다. 그리고 자동차 사이버 보안의 국제기준 UNR No.155이 2020년 6월 채택, EU에서 2022년 7월 시행될 예정인데 해당 법규에서는 자동차 제작사들은 차량 사이버 보안 관리 체계를 수립·이행하고, 차량에 대한 보안 위험평가·관리를 수행하도록 하고 있다. 이처럼 컴플라이언스 측면에서도 사이버 보안에 대한 요구 사항이 증가하고 있는 것도 현실이다. 그러나 기존 연구는 기술적 보안 동향 중심의 단편적 연구로, 인간의 생명을 위협할 수 있는 다양한 자율주행차 보안 공격관련 대응에 있어서 어려움이 존재한다. 이에 국내외 컴플라언스와 관리적·기술적·물리적 보안 점검 항목을 결합한 통합적 연구가 반드시 필요하다. 그리고 조직은 시간과 비용이라는 자원이 한정되어 있기 때문에 점검 항목의 상대적 중요도를 고려하여 우선적으로 일부 점검한다면, 시간과 비용을 절감할 수 있을 뿐만 아니라 보안 수준을 조기에 식별할 수 있을 것이다. 따라서 본 연구는 자율주행차 보안 위협, 관련 법률, 국내외 차량 보안 컴플라이언스 등을 분석하여 자율주행차관련 통합적 보안 수준 점검 항목을 도출하였다. 그리고 점검 항목간 상대적 중요도를 실증 분석하였는데 본 연구 결과를 토대로 시간과 자원이 부족한 업체의 경우, 상대적 상위 랭킹 순위 항목을 선별적으로 사용한다면, 보안 수준을 빠르게 식별할 수 있을 것이다.

본 논문의 구성은 2장에서 본 논문의 관련 이론인 자율주행차 특징 및 보안 위협, 자동차관리법·자율주행차법 등의 관련 법률, 국외 컴플라이언스인 UNR No. 155, 선행 연구 등에 대하여 기술한다. 3장에서는 자율 주행차 보안 수준 점검 항목 도출 및 상대적 중요도 비교를 위한 연구 모형 및 방법을 제시한다. 그리고 4장에서는 AHP(Analytic Hierarchy Process) 분석 기법을 이용하여 상대적 중요도를 실증 분석하고 5장에서 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 관련 이론 및 연구 고찰

1. 자율주행차

자율주행차에 대한 정의들을 살펴보면 국립국어원의 우리말샘 사전에서는 “사람이 운전하지 아니하여도 스스로 달리는 자동차”(National Institute of Korean Language, 2021)라고 정의하고 있으며, 제2조 제1호의3 자동차관리법 및 자율주행차법 제2조 제1호에서도 유사하게 “운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차를 말한다”로 정의하고 있다. 즉 인간의 개입 없이 다양한 기술들을 활용하여 안전하게 스스로 움직이는 자동차라고 할 수 있다.

그리고 자율주행차의 동작 매커니즘은 인지, 판단, 제어로 나누어 설명할 수 있다. 인지 부문은 도로위의 차로, 신호등, 터널, 횡단 보도 등 고정 지물과 보행자, 차량 등의 변동 지물 등의 주변 환경을 인식하는 단계로 카메라, 레이저, 라이더 등의 ADAS(Advanced Driver Assistance System) 센서를 통해 정확하고 빠르게 관련 데이터를 수집하고 인지한다(Seo et al., 2018). 즉 사람의 눈에 해당되는 ADAS 센서로 주변 상황을 인지하는데, 안전을 고려하여 V2X(Vehicle to Everything)라는 외부 통신을 통해서도 주변 상황을 인지한다. V2X 기술은 차량 외부 연결 통신으로 V2V(Vehicle to Vehicle), V2I(Vehicle to Infra), V2P(Vehicle to Pedestrian), V2N(Vehicle to Nomadic Devices)등으로 분류하며, 도로 위의 자동차에 운영 가능한 모든 형태의 통신 기술을 포함한다. 해당 기술은 도로와 차량을 지능화하고 안전을 고려하는 ITS(Intelligent Transport System) 시스템을 구현하는데 필요하다(Jang, 2016). 하지만 V2X 통신 기술은 자율주행차가 외부로 연결되는 통로이기 때문에 외부 해커의 공격에 취약할 수 있다. 이에 자율 주행차의 안전성을 고려하여 V2X 통신 기술에 대한 보안 대응책이 필요하다. 판단 부문에서는 인지 기술에서 수집·제공되는 데이터를 기반으로 자율주행차가 해야할 행동을 결정하는 것으로 가감속, 조향 등의 안전에 가장 중요한 액션들을 판단한다. 즉 수집된 정보를 통해 추월, 차선 변경, 좌우 회전, 정차 등의 주행 상황을 입체적으로 판단하고 운전자를 대신해 조향 및 가감속을 결정하는데, 또한 교통신호 및 장애물 등을 반영하여 최적화된 주행 경로를 결정·생성한다. 제어부문은 인지 및 판단 기술을 기반으로 차선 변경, 조향, 가감속 등의 액션을 수행하는데 단순 제어 매커니즘으로 볼 수 있다.

2. 자율주행차 보안 위협

자율주행차에 ECU(Electronic Control Unit)는 전자 제어 모듈로서 센서, 액추에이터 등을 제어·관리하는 역할을 수행한다. 자율주행차의 경우 외부 접점이 다양해지고 있으나 인증이 취약하여, 공격자는 이러한 환경을 활용하여 ECU 펌웨어를 위변조한다. 또한 해커는 ECU SW 결함을 이용하여 악의적인 공격 및 차량의 오동작을 발생시킬 수 있다(Kwon et al., 2018).

네트워크를 내부와 외부로 나누어 위협을 확인할 수 있다. 차량 내부 네트워크인 CAN(Controller Area Network)상에서 세션을 가로채 정보를 탈취하고 송·수신되는 데이터를 위·변조하는 중간자 공격(Man in the middle Attack; MITM)이 나타날 수 있다. 그래서 세션 하이재킹, 스니핑 공격(Sniffing), 재사용 공격(Replay attack) 등을 통해 차량의 제어권 탈취, 시스템 오동작 등의 서비스 장애를 발생시킬 수 있다. 또한 CAN은 송신 장치에 대한 정보를 갖지 않는 BroadCast 방식의 BUS 구조로 Priority에 따라 패킷들을 처리한다. 만약 짧은 시간내에 Priority 높은 패킷들을 다량으로 발생시키는 DoS 공격이 이루어질 경우, ECU 장비들이 마비될 수 있다. 자율주행차는 GPS, V2V DSRC(Dedicated Short-Range Communications), V2X의 WAVE(Wireless

Access in Vehicular Environments) 등 무선망을 통해 외부 네트워크과 연결된다. 이때 중간자 공격을 통해 세션을 가로채고 주요 정보를 탈취하여, 송수신 메시지를 위변조할 수 있다. 또한 차량 시스템 과부하, 서비스 장애 등의 심각한 위협을 야기 시킬 수 있는 DoS 공격이 외부 네트워크를 통해서도 가능하다.

그리고 미흡한 접근통제 및 권한관리관련, 차량 유지보수를 위해 차량 내부 구성요소에 접근 가능한 직원이 악의적인 의도를 갖고 있고 접근 통제가 약한 경우 ECU관련 펌웨어를 변조하여 차량 안전 운행에 중대한 영향을 끼치거나, 차량의 중요 데이터를 위변조하거나 불법 유출할 수 있다. 차량 진단 및 업데이트시에도 보안 위협이 존재한다. 차량 주요 Unit의 결함 및 성능 등을 진단하기 위해 OBD(On Board Diagnostics) 포트를 사용한다. 해당 포트는 유무선을 통해 컴퓨터와 연결하고 CAN 버스와 통신하여 ECU 값들을 확인한다(Kim and Lee, 2017). 이때 공격자는 CAN 메세지 패킷을 위변조하여 엑셀레이터값 조작, 엔진 정지 등을 할 수도 있다. 그리고 쉐보레 콜벳 OBD-Ⅱ에 보험사의 동글을 장착 불법 행위를 통해 SMS, telnet 원격 제어가 가능한 경우도 있었다. 즉 진단 및 업데이트를 위해 USB, OBD 포트 등 사용시 공격자가 불법적 조작, 물리적 데이터 손실, 악의적인 프로그램을 설치하여 차량 시스템을 마비시킬 수 있다.

3. 국내외 관련 Compliance

1) 국내 법률

자율주행 자동차관련 국내법인 자동차관리법, 자율주행 자동차법을 살펴볼 필요가 있다. 가장 먼저 자율주행차를 다루었던 자동차관리법은 2015년 8월 시험 운영을 위해 일부가 개정되었다. 특히 제27조 제1항에 “자동차를 등록하지 않고 일시 운행하려는 자는 대통령령으로 정하는 바에 따라 국토교통부장관 또는 시도지사의 임시운행 허가를 받아야 한다.”라고 명시하고 있으며, 동항 단서 조항에서는 “자율주행 자동차를 시험 연구 목적으로 운행하려는 자는 허가 대상, 고장감지 및 경고장치, 기능해제장치, 운행구역, 운전자 준수 사항 등과 관련하여 국토교통부령으로 정하는 안전운행 요건을 갖추어 국토교통부 장관의 임시운행 허가를 받아야 한다.”라고 규정하고 있다. 또한 제2조 제1호의3에 최초로 자율주행 자동차를 “운전자의 개입 없이 자동차가 알아서 운행이 가능한 차”라고 정의하였으며, 시험주행을 하려면 차량의 후면에 표식을 붙여야 한다고 명시하고 있다(Lee, 2020).

그리고 자동차관리법을 보완하고 자율주행차의 상용화를 위해 특별법인 자율주행자동차 상용화 촉진 및 지원에 관한 법률(자율주행차법)이 2020년 5월 1일부터 시행되었다. 자율주행 자동차와 완전자율 주행자동차에 대한 내용이 조금 더 세분화되었고, 자율주행 자동차 상용화 촉진을 위해 규제 완화 및 배제, 규제 권한을 이양하기 위한 여객의 유상운송에 관한 특례(제9조), 화물자동차 운송사업에 관한 특례(제10조), 자동차 안전기준에 관한 특례(제11조), 지능형교통체계 표준에 관한 특례(제12조), 도로시설에 관한 특례(제13조)와 같은 규제 특례를 규정하고 있다. 또한 시범운행 지구 지정·운영 및 관리, 안전구간의 지정, 익명 개인정보 사용시 개보법 배제, 전문 인력 양성이 포함되어 있다. 그리고 사고시 손해배상책임, 자율주행차 보안 등에 있어서 추가 개정을 통해 보완이 이루어질 것으로 기대한다.

2) 자동차 사이버 보안 국제 기준

자동차 사이버 보안 관련 UNECE(United Nations Economic Commission for Europe) 산하 WP.29에서 2020년 6월 자동차 사이버 보안 국제기준(UNR No.155)을 채택하였고, 해당 법규는 EU에서 2022년 7월 시행될 예정이다. UNR No.155를 살펴보면 자동차 제작사들은 차량 사이버 보안 관리를 위한 체계(Cyber Security Management System; CSMS)를 갖추고, 차량 형식에 대한 위험평가·관리를 수행하여야 한다. 특히 제작사들은

보안 위협 식별·평가·분류·관리 프로세스, 차량 보안성 시험 프로세스, 보안 위협 모니터링 및 탐지·대응 프로세스 등의 사이버보안 관리 체계가 적절한지를 입증해야 한다. 또한 해당 차량의 부품, 애프터마켓 소프트웨어 등 제작사 외부의 공급업체·시스템에 대한 위험도 관리하도록 하고 있다. 또한 UNR No.155에서 차량의 기술적 보안관련 위협 및 조치 목록을 다음과 같이 분류하고 있다. 차량관련 백엔드 서버 위협은 자율주행차와 연결된 백엔드 서버 데이터·네트워크·애플리케이션 등의 자원에 대한 침해, 통신 채널을 이용한 차량 위협은 차량 내외부 통신 접근 경로에서 데이터 위협 및 네트워크를 활용한 공격, 자동차 업데이트 절차 관련 위협은 차량관련 모듈 업데이트시 절차 오용 및 손상을 통한 위협일 수 있다. 그리고 차량의 외부 연결 및 접속에 대한 위협은 USB 포트 및 OBD 포트 등의 외부 인터페이스, 서드파티 소프트웨어 등 외부 접속 매개를 통해 차량 시스템을 공격하는 위협, 자동차 데이터·코드에 대한 위협은 자율주행차에서 사용하는 데이터·코드·환경설정변수 등에 대한 공격 위협으로 분류하고 있다. 그리고 비의도 인간행동 위협 및 악용될 수 있는 잠재적인 취약점 위협은 정상적 행위자가 의도하지 않게 사이버 공격을 용이하게 하는 행동 혹은 SW 및 네트워크 등 설계시 충분히 보호하지 않아 나타날 수 있는 잠재적 보안 취약점에 대한 공격일 수 있다. 한편 국내 승인관련 사항을 살펴보면 국내는 UNR No.155을 기반으로 형식 승인보다 자가 인증으로 접근하고 있으며 법제화 및 국제 동향에 따라 추후 변경 예정이다.

3) 국내 자동차 사이버 보안 가이드

2018년 5월 발표된 스마트 교통 사이버 보안 가이드는 자율주행차 시장의 성장, 다양한 접점을 통한 연결 확대로 보안 취약점 증가 등으로 2019년 12월 추가 개정되었다. 해당 보안 가이드는 스마트 교통 분야의 국제 표준을 기반으로 위협과 취약성에 대해 가용성 손상, 데이터 손실, 중간자 공격, 부적절한 암호 사용, 부적절한 접근 통제, 부적절한 물리적 통제, 악의적 프로그램 실행, 미흡한 사용자 관리 등 10가지로 구분하였다. 그리고 이에 대한 보안 대응 항목을 개발·관리보호, 물리적 보호, 인증, 암호, 데이터 보호로 분류하였다.

또한 2020년 12월 국토부에서 발표한 자동차 사이버 보안 가이드에서는 국제 기준인 UNR No.155을 기반으로 차량 사이버 보안 관리를 위한 체계(CSMS) 수립·이행 등의 관리적 보안과 통신 채널을 이용한 차량 위협, 실도로 차량 관련 백엔드 서버 위협, 차량의 외부 연결 및 접속에 대한 위협, 차량 데이터·코드에 대한 위협, 비보호로 인한 잠재적 취약점 등을 기술 영역에서 대응·점검해야 할 항목으로 범주화하였다.

4. 관련 선행 연구

Kwon et al.(2018)는 자율주행차의 기술 단계와 인지·판단·제어로 구성되어 동작되는 원리를 기술하였고 자율주행차에서 발생할 수 있는 보안 위협과 IEEE 1609.2, ISO 14229 등의 보안 기술 표준화를 설명하였다. 그리고 자율주행차의 대중화를 위해 지속적인 보안 기술 연구와 실증적인 적용이 이루어져야 한다고 언급하였다. Seo et al.(2018)는 자율주행차 기술관련 동향과 V2X 원격 엑세스, CAN 버스내에서의 Flooding 등의 보안 취약점을 도출하였고 이를 통해 일부 기능을 대상으로 차량 시스템 공격 시나리오를 정의하고 대응 방안을 개발하였다. 또한 CAN 보호를 위한 메시지 인증 혹은 암호화, 통신 채널 보호 등의 보안 요구 사항을 제시하였다. Kim(2020)는 자율주행차가 상용화됨에 따라 나타날 수 있는 사이버 공격을 기술하였고 이와 관련된 2019년 스마트 교통 사이버 보안 가이드의 보안 위협 10가지와 보안 요구 항목인 개발·관리보호, 물리적 보호, 인증, 암호, 데이터 보호를 언급하였다. 그리고 통합 관제 시스템 구축, 교육 및 훈련 등의 안전성 개선 방안을 제언하였다.

하지만 대부분의 관련 연구에 있어서 보안 기술 동향에 치우져 있고, 자율주행차 보안 수준 점검 항목 및

상대적 우선 순위를 분석하려는 연구 및 노력이 부족한 것으로 판단된다.

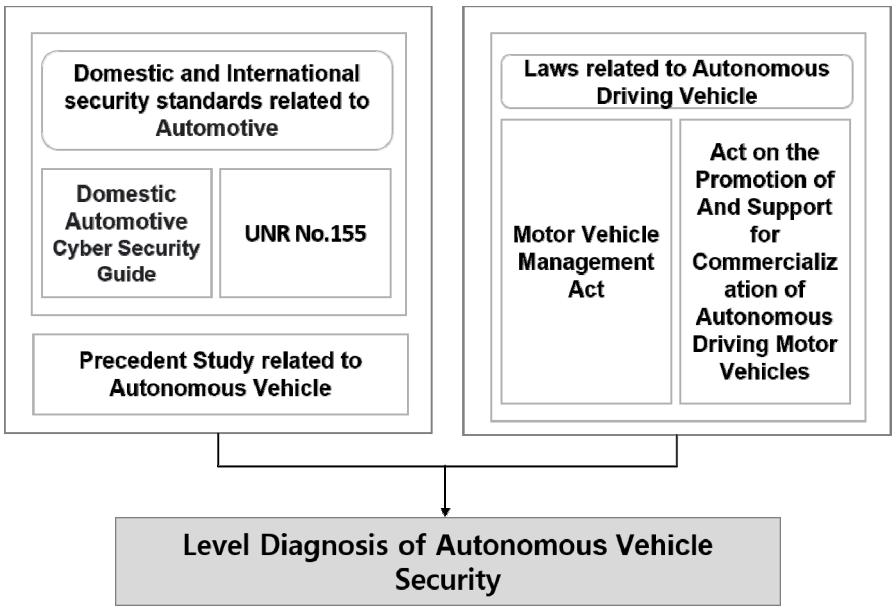
5. 계층 분석 기법

Thomas L Satty 교수에 의해서 1970년대 초에 개발된 AHP 기법은 효과적인 의사결정을 위해 의사결정 전 과정을 단순화하고 최종적인 의사결정에 이르게 하는 모형이다(Satty, 1986). AHP는 쌍대 비교를 통해 평가자가 일관성 있게 판단 할 수 있게 해주는 특징으로 상대적 중요도를 계량화하여 판별하는데 많이 이용되고 있다. AHP는 최상위 계층에 평가 목표를 두고 그 하위에는 목표에 영향을 주는 평가 기준을 설정한다. 그리고 평가 기준은 여러 단계로 나누어서 다시 하부 세부 평가 기준으로 계층화 할 수 있다. 좀더 고찰해 보면 다수의 속성들을 계층적으로 배열하고 여기에 설문 결과 데이터를 기입하여 계층별 쌍대비교(Pairwise comparison)를 수행한다. 쌍대비교 행렬로부터 각 계층별 의사 결정요소의 상대적 중요도를 추정한 후 일관성 비율(Consistency Ratio; CR)을 구하여 유효성 여부를 수행한다. 일관성 비율은 평가자의 응답 일관성 여부를 검증하는 것으로 일관성 비율이 10% 이내인 경우, 판단에 일관성이 있는 것으로 간주한다.

Ⅲ. 연구모형

1. 자율주행차 보안 수준 점검 항목 도출

기존에 연구되었던 이론적 고찰과 함께, 자동차관리법·자율주행차법 국내 법률과 UNR No.155 국제 기준 및 국내 차량 사이버 보안 가이드에서 자율주행차 보안과 연관된 점검 항목들을 분석하여 <Fig. 1>과 같이 도출한다.



<Fig. 1> Derivation of Security Checklist of Autonomous Vehicle

그리고 도출된 자율주행차 보안 수준 점검 항목들은 AHP 모형의 계층화 구성 요소로 이용한다. 좀더 살펴 보면 자율주행차 내부에 Malware를 설치하고 CAN 버스를 Flooding하여, ECU의 장애를 유발하는 위협은 운전자의 안전에 영향을 미칠 수 있다. 이에 차량 내부 데이터·네트워크를 위협하는 악성 소프트웨어와 CAN 내부 네트워크를 고갈시키는 공격 등을 탐지·대응할 수 있는 보안 운영 관리가 필요하다. 따라서 국제 기준인 UNR No.155 차량 내부 데이터·코드위협 22.1의 악성 소프트웨어 활동 점검 항목과 24.1의 CAN 버스를 플러딩하거나 높은 메시지 전송률을 통해 내부 네트워크 통신 서비스 위협시 대응 항목을 보안 운영관리 점검 항목으로 도출하였다.

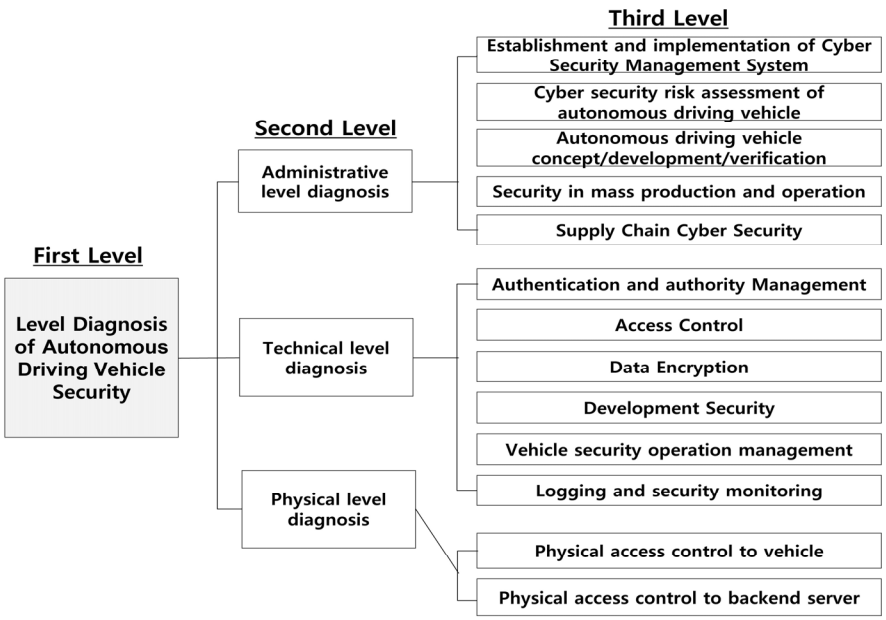
도출된 해당 항목을 스마트 교통 사이버 보안 가이드의 데이터 보호 악성 프로그램 대응과 매핑하여 기술적 부문의 차량 보안 운영관리 점검 항목으로 최종 확정하였다. 아래 <Table 1>은 관련 법률, 국내외 차량 보안 표준 등의 컴플라이언스와 기존 관련 연구들에서 도출된 자율 주행 자동차 보안 관리 수준 점검 항목들이다.

<Table 1> Checklists derived by this study for autonomous driving vehicle security

Item	Checklists	Description
Administrative Diagnosis	Establishment and implementation of Cyber Security Management System	Establishment and Implementation of overall system including establishment and implementation of Cyber Security Management System(CSMS) and management and supervision of CSMS
	Cyber security risk assessment of autonomous driving vehicle	Asset identification, risk assessment, and risk scenario planning
	Autonomous driving vehicle concept/development/verification	Establishment and Implementation of cyber security requirements in project planning/concept/development/verification stage
	Security in mass production and operation	Establishment and implementation of cyber security incident response during mass production and operation, and establishment and implementation of update management
	Supply Chain Cyber Security	Specification of cyber security items in the business agreement, security activity evaluation during Supplier development and after development
Technical Diagnosis	Authentication and authority Management	Authentication and authority management including authority management when accessing vehicle resources and secure user authentication in case of vehicle communication channel threat (man-in-the-middle attack, etc.)
	Access Control	Control user access to autonomous vehicles and backend servers, access control such as secure network access and network separation
	Data Encryption	Encryption of data storage and transmission/reception for Operating vehicle, communication channels and backend servers
	Development Security	Establishment and implementation of security policies when developing vehicles, communication channels, backend servers, etc.
	Vehicle security operation management	Security operation management of SW update, vaccine, operation to prevent CAN flooding/malicious V2X, etc.
	Logging and security monitoring	Storage and monitoring about security logs of vehicles, communication channels, backend servers, etc.
Physical Diagnosis	Physical access control to vehicle	Control of unauthorized hardware access to vehicle key modules
	Physical access control to backend server	Control of illegal physical access to backend servers

2. 연구 모델

도출된 차량 보안 점검 항목을 기반으로 항목간 상대적 중요도 평가를 위한 연구 모델은 <Fig. 2>와 같다. 연구 모델의 목표를 제1 계층으로, 제2 계층은 자율주행차 보안 수준 점검 항목의 3개 영역인 관리적, 기술적, 물리적 점검을 구분하여 하위 평가 기준을 구성하였다.



<Fig. 2> Hierarchy Model

제3 계층에서는 13개의 하위 항목으로 구성하였는데 관리적 보안 수준 점검 하위 항목은 사이버 보안 관리체계(CSMS) 수립 및 이행, 자율주행차 사이버 보안 위험평가, 자율주행차 컨셉·개발·검증, 양산 및 운영시 보안, 공급망 사이버 보안이며 기술적 수준 점검 하위 항목은 인증 및 권한 관리, 접근 통제, 자율주행 데이터 암호화, 차량 보안 운영관리 등이다. 마지막으로 물리적 수준 점검 하위 항목은 차량에 대한 물리적 접근 통제, 백엔드 서버 물리적 접근 통제이다.

3. 연구 방법

1) 조사 방법 및 표본 특성

본 연구의 AHP 설문 조사는 2021년 6월 14일부터 7월 14일까지 1개월간 실시하였고 설문 방법은 설문의 객관성 및 정확도 향상을 위해 유선상으로 각 항목에 대해 우선적으로 설명을 한 후, 직접 방문 또는 이메일을 통해 작성하도록 하였다. 설문지의 평가 항목은 3개의 상위 점검 항목(2계층)과 13개 하위 점검 항목(3계층)으로 구성하여 같은 계층간 쌍대 비교하도록 하였다. 그리고 평가 수치 척도는 AHP 설문에서 가장 많이 사용하는 9점 척도를 사용하였고, 가중치 분배는 비교 대상의 가중치를 모두 합하면 1이 되는 Distributive 모드를 활용하였다. 즉 두 개의 점검 항목을 서로 쌍대 비교하는데 어느 항목이 상대적으로 더 중요한지를 9점 척도 안에서 점수를 부여하도록 구성하였다. 또한 조사 대상자는 5년 이상의 보안 경력 및 CISA, CISSP,

ISMS-P 등 공인 보안 자격증을 가진 보안 회사의 정보보호 전문가로 선정하였다. 따라서 정보보호 전문가 20명을 대상으로 상대적 중요도를 산출하였고 일관성 비율이 0.1이상인 2부를 제외하고 유효한 18부를 분석에 이용하였다. 설문 표본의 인구 통계학적 특성을 상세 살펴보면 응답자의 연령은 40-49세가 50.0%로 가장 많은 비중을 차지하였고, 학력은 석사 33.3%, 박사 11.1%로 전체의 44%이상을 차지하고 있음을 확인할 수 있었다. 또한 정보 보호 경력은 11-19년 사이가 55.6%로 가장 많은 비중을 차지하고 있으며, 다음으로는 20년 이상이 16.7% 등의 순으로 확인되었다. 다음으로는 20년 이상과 6-10년 사이가 16.7%, 3-5년 사이가 11.1% 등의 순으로 확인 되었다.

2) AHP 절차

본 연구는 단계별로 상대적 중요도 분석을 진행하였는데 1단계는 자율주행차 보안 수준 점검을 계층 구조화하였다. 2단계로서 전문가 20명에게 AHP 관련 설문 조사를 진행하였는데 해당 설문은 두 개의 항목을 서로 비교하는데 어느 점검 항목이 상대적으로 더 중요한지를 평가하는 것이다. 3단계는 일관성 비율을 확인하고 쌍대비교 행렬을 이용하여 보안 점검 항목 계층별 상대적 중요도를 산출하였다. 그리고 각 계층의 상대적 중요도를 곱하여 나온 중요도 수치로 우선 순위를 도출하였다.

Ⅳ. 실증 결과

AHP를 통해서 자율주행차 보안 수준 점검 영역 및 세부 하위 점검 항목에 대한 상대적 중요도 분석 결과는 다음 <Table 2>와 같다.

<Table 2> Checklists The priority analysis of importance among checklists

Higher Standard		Lower Standard			Final Relative importance	Priorities
Classification	Relative importance of higher standard	Checklist items	Relative importance of lower standard	Priorities of lower standard		
Administrative diagnosis	0.4760	Establishment and implementation of Cyber Security Management System	0.4920	1	0.2342	1
		Cyber security risk assessment of autonomous driving vehicle	0.2310	2	0.1100	3
		Autonomous driving vehicle concept/development/verification	0.1190	3	0.0566	6
		Security in mass production and operation	0.1080	4	0.0514	7
		Supply Chain Cyber Security	0.0500	5	0.0238	11
Technical diagnosis	0.4530	Authentication and authority Management	0.1840	2	0.0834	4
		Access Control	0.0990	4	0.0448	9
		Data Encryption	0.4750	1	0.2152	2
		Development Security	0.0590	5	0.0267	10
		Vehicle security operation management	0.1430	3	0.0648	5
		Logging and security monitoring	0.0390	6	0.0177	13
Physical diagnosis	0.0710	Physical access control to vehicle	0.6670	1	0.0474	8
		Physical access control to backend server	0.3330	2	0.0236	12

이를 통해 제2계층(상부 영역) 각 영역별 가중치 및 순위와 제3계층(하부 영역)의 세부 하위 보안 점검 항목별 가중치 결과값을 확인할 수 있다. 또한 제2계층과 제3계층을 종합하여 세부 하위 점검 항목별 전체 가중치의 상대적 우선 순위를 파악할 수 있다. 실증 상세 결과를 살펴보면, 상부 영역 간 쌍대비교 결과는 관리적, 기술적, 물리적 점검의 중요도 결과가 각각 47.6%, 45.3%, 7.1%로 나타났다. 따라서 상부 영역 간 쌍대비교에서 관리적 보안 수준 점검이 가장 중요한 것으로 확인되었다. 이러한 결과는 자율주행차 보안성 강화를 위해 보안 조직 구조화, 자원 활용을 통한 CSMS 구현, 관리 체계 관리·감독 등을 포함하는 전반적 사이버보안 관리체계 수립·이행과 자산식별, 위험평가, 보호 대책 수립 등을 수행하는 보안 위험 관리들이 베이스라인으로 구조화되어야 하기 때문이다. 또한 기반이 취약한 사이버보안 관리체계 상에서 기술적 보안 점검은 효과적일 수 없다.

하부 영역을 살펴 보면 자율주행차 관리적 보안 수준 점검 측면의 하부 영역에 대한 우선 순위 분석 결과, 사이버보안 관리체계 수립·이행이 49.2%로 가장 높은 가중치를 보이며 위험평가 23.1%, 자율 주행차 컨셉·개발·검증 11.9%, 양산 및 운영시 보안 10.8% 등의 순으로 나타났다. 특히 관리 체계 수립·이행이 가장 높게 나타난 것은 CSMS 이행, 관리체계 관리·감독 등 보안 관리 체계를 라이프사이클 전반에 걸쳐 확립하는 것이기 때문이다. 기술적 점검 측면의 하부 영역에 대한 우선 순위 분석 결과, 암호화가 47.5%로 가장 높은 가중치를 보이며 인증 및 권한관리 18.4%, 차량 보안 운영관리 14.3%, 접근 통제 9.9%, 개발 보안 5.9% 등으로 나타났다. 이중 암호화가 상대적으로 중요하다고 판단되는 이유는 송수신 패킷이 암호화 되어 있어 인증 우회 및 불법 접근을 지연·차단시킬 수 있으며, 또한 중요 데이터에 대한 암호화 저장으로 비허가자에 의한 정보 식별이 불가능하기 때문이다. 물리적 점검 측면의 하부 영역에 대한 우선 순위 분석 결과, 차량 물리적 접근 통제 66.7%, 백엔드 서버의 물리적 접근 통제 33.3% 순으로 나타났다. 즉 차량에 대한 물리적 접근 통제 부문이 상대적으로 중요하게 나타난 것은 운전자가 직접 차량과 함께 자율 주행하는 것이며, 차량 자체가 차량의 운전을 도와주는 백엔드 서버 인프라보다 보안이 더 중요하다고 판단했기 때문이다.

마지막으로 상부 영역과 하부 영역의 상대적 가중치를 통해 최종 우선순위를 살펴보면. 자율주행차 관리적 보안 수준 점검 영역의 사이버보안 관리체계 수립·이행이 23.4%로 1순위, 기술적 점검 영역의 암호화가 21.5%로 2순위, 관리적 점검 영역의 위험평가가 11%로 3순위 등의 순으로 나타났다. 따라서 보안 수준을 조기에 식별하고자 하는 회사에서는 상대적 우선 순위를 활용하여 자율주행차 보안 수준 점검 활동을 효과적으로 수행 할 수 있을 것이다. 다음 <Table 3>에서는 기존 연구와의 비교를 통해 본 모형의 우수성을 평가하였다.

<Table 3> The Comparison precedent studies with the proposed Model

Evaluation items		Precedent Study	Proposed Model
Compliance	Security Standard System	Only Domestic compliance analysis (Cyber Security Guide for Smart Transportation)	Multiple Compliance analysis including overseas (UNR No.155, Cyber Security Guide for Smart Transportation, Automotive Cyber Security Guide)
	Law	Motor Vehicle Management Act	Motor Vehicle Management Act, Autonomous Vehicle Act
Research method		A fragmentary Study for focusing on technological security trends	Integrated Study that combines administrative, technical, and physical security items
Check items and their relative importance		Few Precedent Studies	Derivation of check items for the first time through domestic and international compliance and security threat technology analysis Identification of relative importance ranking by applying AHP technique (Early identification and time·cost savings through screening check of high-ranking items)

기존 선행 연구에서는 기술적 보안 동향 중심의 단편적 연구로 국내 컴플라이언스만 분석하여, 통합적으로 자율주행차 보안 수준을 점검하는데 어려움이 존재하였으나 본 연구에서는 UNR no.155, 자동차 사이버보안 가이드 라인 등의 국내외 다수 컴플라이언스를 분석하고 이를 관리적보안·기술적보안·물리적 보안 항목으로 결합한 통합적 최초 연구로, 자율주행차 보안 위협에 효과적으로 대응할 수 있을 것이다.

또한 자율주행차 보안 수준 점검을 위한 시간과 자원이 부족한 경우, 예를 들어 AHP 적용으로 도출된 상대적 중요도 우선순위 Top 5 항목들을 우선적으로 점검한다면, 전체 항목 점검 대비 보안 수준을 좀더 빠르게 식별할 수 있을 뿐만 아니라 점검 시간과 비용을 절감할 수 있다.

Ⅴ. 결론 및 향후 연구 방향

자율주행차의 시장 확대와 안전·편의성을 고려한 외부 연결 접점이 다양해지고 있어, 자율주행차의 보안 위협도 증가하고 있다. 따라서 운전자의 안전을 책임지는 자율주행차 보안 강화를 위해 본 연구는 자율주행차 특징, 보안 위협, 국내 관련 법률, 국내외 컴플라이언스 등 자율주행차 보안 관련 현황 분석을 통해 점검 항목을 도출하였다. 이를 토대로 AHP 모형에 적용하여 상대적 중요도를 확인할 수 있었다. 실증 결과를 요약하면 점검 항목 중요도 평가에서 상부 영역 중 자율주행차 관리적 보안 수준 점검이 가장 중요한 것으로 확인되었다. 이러한 결과는 보안 조직 구조화, CSMS 구현, 관리 체계 관리·감독 등을 포함하는 전반적 사이버보안 관리체계 수립·이행과 위험 평가 관리 등의 관리적 보안 수준 점검 항목들이 베이스라인으로 체계적으로 잘 잡혀 있어야 그 위에 기술적 보안·물리적 보안 점검을 계층화 할 수 있기 때문이다. 그리고 기존 연구에서는 기술적 보안 점검에만 치중하였다. 또한 하부 영역은 암호화 등의 순으로 나타났는데 이중 암호화를 중요하게 판단한 이유는 송수신 패킷이 암호화 되어 있어 인증 우회 및 불법 접근을 차단시킬 수 있으며, 중요 데이터에 대한 암호화 저장으로 비허가자가 데이터를 탈취하더라도 데이터 정보 식별이 불가능하다. 이는 인증 및 권한관리·접근 통제 항목 등이 취약하더라도 암호화를 통해 대응할 수 있기 때문이다.

본 연구의 의의는 자율주행차 보안 수준 점검관련 기존 연구가 거의 존재하지 않는 상황에서 국내외 컴플라이언스 분석을 토대로 관리적·기술적·물리적 보안 수준 점검 항목을 도출하고 연구 모형을 실증함으로써 인명 피해까지 초래할 수 있는 사이버 보안 공격에 통합적으로 대응할 수 있도록 하였다. 그리고 조직들이 짧은 시간 안에 보안 수준 식별 혹은 시간과 자원이 부족한 경우 본 연구 결과의 상대적 중요도 항목중 상위 랭킹 순위 항목으로 보안 점검을 선별적으로 수행한다면, 전체 점검 수행 대비 보안 수준에 대한 조기 식별이 가능하고 시간·비용에 대한 효과성을 높일 수 있을 것이다.

본 연구의 신뢰도를 높이기 위해 보안 전문가로 수행하였으나, 다만 대상자가 보안 회사 전문가로만 구성되어 상대적 중요도 순위를 일반화하는데 한계가 있다. 이에 조사 대상 세분화와 시료 확대를 위해 자동차업체 담당자를 대상으로, 향후 연구를 진행하여 상대적 중요도 순위가 상이한지를 비교·분석할 필요가 있을 것이다.

REFERENCES

Jang, S. J.(2016), “SW technology trends related to autonomous vehicles”, *2016 Information and Communication Magazine*, vol. 33, no. 4, pp.29-30.

Kim, Y. J. and Lee, Y. S.(2017), “A Study on the Vulnerability and Security Considerations of Autonomous Vehicles”, *2017 Proceeding of the Summer Conference of the Korea Society of Computer and Information*, vol. 25, no. 2, pp.165-166.

Kim, Y. J.(2020), *A Proposal for Improvement of Safety by Commercialization of Autonomous Vehicles*, Master's Thesis, Sungkyunkwan University, pp.26-42.

Kwon, H. C., Lee, S. J., Choi, J. Y. and Nah, J. C.(2018), “Security Trends for Autonomous Driving Vehicle”, *2018 Electronics and Telecommunications Trends*, vol. 33, no. 1, pp.82-83.

Kwon, S. H. and Lee, J. H.(2020), “Autonomous Vehicle Security Threats and Technology Trends”, *Journal of The Korea Institute of Information Security & Cryptology*, vol. 30, no. 2, pp.32-38.

Lee, S. H.(2020), *A Study on the Improvement of the Law for Securing the Operational Safety of Autonomous Driving Vehicle*, Doctoral Dissertation, Changwon National University, pp.35-44.

National Institute of Korean Language, https://opendict.korean.go.kr/main, 2021.08.17.

Satty, T. L.(1986), “Axiomatic foundation of the Analytic Hierarchy Process”, *Management Sci.*, vol. 32, no. 7, pp.841-850.

Seo, E. B. and Kim, H. K.(2018), “Security of Self-Driving Car from the Point of View of In-Vehicle System”, *Transactions of the Korean Society of Automotive Engineers*, vol. 26, no. 2, pp.244-251.

Seo, H. J., Lee, S. J., Kwon, H. D. and Kwon, Y. B.(2018), “Autonomous Vehicle Security Trends”, *Journal of The Korea Institute of Information Security & Cryptology*, vol. 28, no. 5, pp.10-11.

Wired, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway, 2021.07.30.

Yonhap News, https://www.yna.co.kr/view/AKR20200226049400008, 2021.07.29.