https://doi.org/10.33778/kcsa.2022.22.5.049

자동차 공급망 참여기업 대상 사이버보안 관리체계 구현 평가모델 설계 (ISO/SAE 21434 표준 및 TISAX 평가 요구사항을 기반으로)

백 은 호*

요 약

자동차 분야의 사이버보안은 자동차 생애주기 중 핵심적인 요소로서 전 세계적으로 사이버보안 평가 기준이 강화되고 있다. 또한 자동차의 설계 및 생산을 수행하는 제조사만이 아니라 복잡한 컴포넌트와 다양한 부품으로 이루어진 자동차의 특성상 전체 공급망에 참여하는 기업들의 사이버보안 관리체계 구현 수준이 평가되고 관리되어야만 사이버보안의 안전성을 확보할 수 있다. 이에 본 연구에서는 자동차 사이버보안을 평가하는 대표적인 기준인 ISO/SAE 21434와 TISAX의 요구사항을 분석하여 총 7개 영역, 54개 사이버보안 관리체계를 평가할 수 있는 항목을 도출하였고 이를 국내/외 기업 보안담당자 및 유관 전문가 대상으로 진행한 설문조사를 통해 우선순위 및 업종에 따른 적합성, 타당성 검토를 거쳐서 6개 영역, 45개 평가 기준을 도출하여 최종 평가항목으로 제시하였다. 본 연구는 자동차 공급망에 참여하는 기업이 ISO/SAE 21434와 TISAX 전반의 통제 프로세스를 일률적으로 도입하기 전에 우선 적용하여 해당 기업의 현재 사이버보안 관리 수준을 평가할 수 있는 모델을 제시했다는 점에서 연구로서의 의의가 있다고 할 수 있다.

Designing an evaluation model for cyber security management system implementation for companies participating in the automobile supply chain (based on ISO/SAE 21434 standard and TISAX assessment requirements)

Baek Eun Ho*

ABSTRACT

Cyber security in the automobile sector is a key factor in the life cycle of automobiles, and cyber security evaluation standards are being strengthened worldwide. In addition, not only manufacturers who design and produce automobiles, but also due to the nature of automobiles consisting of complex components and various parts,the safety of cybersecurity can be secured only when the implementation level of the cybersecurity management system of companies participating in the entire supply chain is evaluated and managed. In this study, I analyzed the requirements of ISO/SAE 21434 and TISAX, which are representative standards for evaluating automotive cybersecurity. Through a survey conducted on domestic/overseas company security officers and related experts, suitability and feasibility were reviewed according to priorities and industries, so 6 areas and 45 evaluation criteria were derived and presented as final evaluation items. This study is meaningful as a study in that it presented a model that allows companies participating in the automotive supply chain to evaluate the current cybersecurity management level of the company by first applying ISO/SAE 21434 and TISAX overall control processes before uniformly introducing them.

Key words : ISO/SAE 21434, TISAX, Automotive sector security, Cybersecurity assessment model, VDA ISA

접수일(2022년 12월 11일), 수정일(2022년 12월 27일), 게재확정일(2022년 12월 31일)

* 중앙대학교 대학원 융합보안학과 산업보안전공

1. 서 론

최근 몇 년 동안 자동차 산업분야의 4차 산업 혁명이라 일컬을 수 있는 스마트 자동차에 대한 사이버보안이 핵심 이슈로 떠오르고 있다. 기존 오프라인으로 연결되던 자동차 내 컴포넌트 및 각종 부품이 차량의 전자화가 광범위하게 이루어지며 이제는 대부분의 기능이 ECU와 연결된 컴퓨터에 의해 제어되는 방식으로 진화하고 있다.[1]

이에 따라 IATF 16949, ISO 26262 등 자동차의 품질과 안전에 대한 국제적인 요구사항 외에 차량의 라이프사이클 중심의 사이버보안 표준인 ISO/SAE 21434 및 유럽 자동차 제조사를 중심으로 공급망 자체의 사이버보안에 대한 수준을 평가하는 TISAX와 같은 국제 기준이 자동차 산업분야 사이버보안 표준으로 요구되고 있다.

특히, UNECE(유럽경제위원회)는 2022년 7월 이후 신규 차량이 형식 승인을 요청하는 경우, 사이버보안에 대한 적합성을 요구하고 있어, 향후 유럽에 자동차를 수출하고자 하는 모든 완성차 업체를 포함한 모든 전장부품 업체는 해당 사이버보안 표준에 대한 적합성을 인증받아야 제품에 대한 형식 승인이 가능하며, 이러한 요구사항은 유럽을 시작으로 전 세계로 확대되고 있다.(UNECE WP. 29, 2018)

상대적으로 규모가 크고 잘 관리되어 온 차량 제조사 자체의 사이버보안 관리체계는 ISO/SAE 21434 및 TISAX 등 국제기준 인증을 회사 내 준용하여 운영이 가능하지만 다수의 부품공급사는 급변하는 자동차 산업의 사이버보안 강화에 대한 요구사항을 충족시키기에는 짧은 준비기관과 전문가 부재로 국내외 자동차 공급망 참여 업계에 GDPR 이상의 충격을 줄 것으로 예상된다.

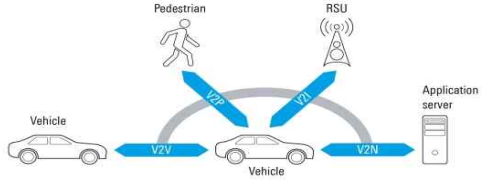
그에 따라 본 연구에서는 ISO/SAE 21434 및 TISAX의 요구사항을 기본으로, 자동차 공급망 참여 업계에서 실질적으로 우선 도입하여 운영이 가능한 사이버보안 관리체계의 표준평가 모델을 수립하여 제시하고자 한다.

2. 이론적 배경과 선행연구

2.1 자동차 환경의 변화

오늘날 대부분의 자동차는 약 70% 이상의 ECU (Electronic Controller Unit)을 사용하고 있으며, 이러한 ECU는 차량 내에서 CAN, Ethernet 등을 토대로 통신하고 있다. 최근 차량 통신기술의 하나인 Vehicle-to-vehicle (V2V), Vehicle - to- infrastructure (V2I) 을 기반으로 차량과 인터넷 통신을 내장한 모뎀/블루투스와 연결된 핸드폰 등을 기반으로 운영되며 이와 같은 Connected vehicle technology는 스마트폰과 태블릿 PC와 같은 외부 디바이스와 연결성을 증대시키고 있다.

프리미엄급 자동차에는 70~100 개의 ECU (Electronic Control Unit)에서 실행되는 1억 줄 이상의 프로그래밍 코드가 포함되어 있는 것으로 추산되고 있으며, 이 숫자는 가까운 장래에 2억 ~ 3억 줄로 증가할 것으로 예상되어, 미래의 차량은 잘못된 통합이나 사람의 실수로 인해 잠재적인 취약성이 많은 매우 복잡한 기계임을 의미한다(Matan Levi, Yair Allouche, and Aryeh Kontorovich, 2017).



(그림 1) V2X 통신 구성(www.epdtonthenet.net)

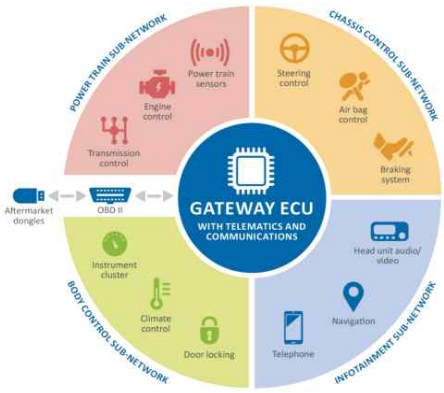
2.2 스마트 자동차 구성

스마트 자동차는 수많은 부품으로 이루어져 있으며 그에 따른 각 분야는 아래와 같은 카테고리로 구분되고 있고, 각각의 카테고리에서 사용하는 프로토콜은 아래와 같다.(EINSA, 2016).

<표 1> 스마트 카의 High-level 구성 개념도

Category	Protocol
파워트레인 제어	CAN
새시 제어	CAN, FlexRay, RF
진단 및 유지관리 제어	OBDII, Ethernet
통신 제어	3G, 5G, Wifi
인포테인먼트 제어	MOST, BT, Wifi

대부분의 스마트 자동차는 다양한 역할을 하는 ECU로 구성되어 있으며, 각 ECU는 Gateway ECU를 통해 상호 통신을 수행한다. 그에 따라 각 모듈 및 기능별 전장 부품들은 ECU를 통해 제어하게 되고 필요 정보를 교환하고 있다.(EINSA, 2016)



(그림 2) 스마트 카의 High-level 구성 개념도

이러한 스마트카의 특성상, 다양한 사이버보안 위협이 존재하며, 해당 위협에 노출될 위험도는 시간이 갈수록 증대되고 있다. 하지만, 자동차 시스템의 특성에 따라 이러한 위험을 사전에 통제하는 것은 쉽지 않으며 많은 자원을 필요로 한다.

2.3 ISO/SAE 21434

UNECE(United Nations Economic Commision for Europe)는 1947년 유럽공동체의 경제적 협력과 구축을 위해 구성된 경제사회적 회의체로 그에 속한 포럼 중 WP.29는 자동차, 장비 및 부품에 대한 형식 승인 및 상호 인증 프로세스를 정의하는 포럼으로 세계에서 가장 큰 국제 차량 규제 시스템을 구성하고 있다.

2020년 6월 WP.29에서는 자동차 사이버보안에 관련한 법규인 UN Regulation No.155 : Cybersecurity Regulation을 채택하였으며 자동차 사이버보안의 생명주기 내에서 사이버보안의 모니터링, 통제, 업데이트를 지원 가능한 일관된 관리체계를 요구하고 있으며 이에 필요한 요구사항을 설계 단계부터 충족하도록 사이버보안 관리체계를 수립하고 적용해야 한다. 이는 차량 제조사에 대해서만 국한된 것이 아니고, 차량 부품을 공급하는 많은 협력사들까지 포함된다.

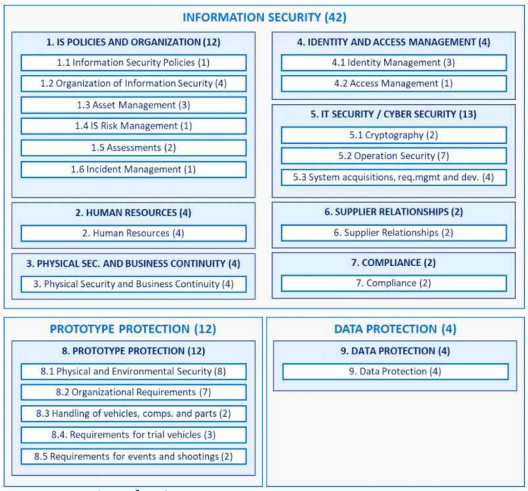
ISO/SAE 21434는 이러한 차량 생명주기 내에서의 사이버보안 요구사항에 대해 정의하고, 관리체계 구축 및 운영을 위한 국제표준으로 ISMS(Information Security Management System)에서처럼 기업의 사이버보안 정책과 조직 구성 등, 거버넌스에 대한 요구사항을 포함하며, 이에 추가로 차량의 기획, 연구개발, 설계, 제조, 출하, 유지관리, 폐기 단계에서 발생 가능한 사이버 공격이나 공격에 대한 위험 발생 확률을 감소시키기 위한 요구사항으로 구성되어 있다.

(그림 3) ISO/SAE 21434 구성도

2.4 TISAX(Trusted Information Security Assessment eXchange)

독일 자동차산업협회(VDA: Verband der Automobilindustrie)는 유럽 자동차 제조사를 중심으로 운영되는 자동차 산업분야의 대표적인 협회로 자동차 산업에서 다양한 사이버보안에 대한 요구사항이 증대함에 따라, ISO/IEC 27001을 기반으로 자체 공급망 사이버보안 수준 평가 체크리스트(VDA ISA Checklist)을 개발하고, 자동차 제조사는 공급망 참여 기업 간 안전한 네트워크 내에서 정보교환을 하기 위하여, 해당 체크리스트를 활용한 TISAX 평가 결과를 부품, 컴포넌트 공급사에게 요구하고 있다.

VDA ISA Checklist는 ISO/IEC 27001 규격 요구사항을 기반으로 자동차 산업분야 공급망 사이버보안 수준을 평가하기 위한 세부 요구사항을 적용하고 있으며, 정보보호, 프로토타입 보호, 데이터 보호 세 개의 영역으로 구성되어 있다. (TISAX participants handbook, 2021)



(그림 4) TISAX Compliance Guide

2.5 그 밖의 자동차 사이버보안 기준

1) ISO 26262 Road Vehicles – Functional Safety 표준은 승용차, 트럭, 버스 및 모터사이클 등 모든 차량에 대한 안전 요구사항으로 안전 기능 중심의 표준이며 Annex E에는 사이버보안 중심의 안전 기능에 대한 요구사항이 포함되어 있다.
2) 미국 고속도로 교통안전국(NHTSA : National Highway Traffic Safety Administration)는 기존 Cybersecurity Best Practices for Modern Vehicles(2016)을 발전시켜, ISO/SAE 21434와 유사한 Best practice draft를 발표하였으며, 이는 자체 평가를 기준으로 자동차 분야 기업의 사이버보안 평가를 수행한다.

3. 자동차 사이버보안 관리체계 평가 모델 개발

3.1 사이버보안 관리체계 평가 범위 선정

앞서 확인한 선행 연구에 따르면 자동차 분야 사이버보안 관리체계는 요구사항이 방대하고, 기업의 규모와 업종을 고려하지 않은 요구사항으로 이루어져 있다. 그에 따라 본 연구에서는 사이버보안 관리체계를 평가 영역별로 구분하고, 대표적인 평가 기준인 ISO/SAE 21434와 TISAX VDA ISA Checklist에서 요구하는 기본적 요구수준을 충족시킬 수 있는 항목을 설계하고자 아래와 같이 영역을 분류하였다.
1) 관리체계 영역 : 사이버보안 거버넌스, 목표, 전략, 정책, 컴플라이언스 등의 대응을 위한 평가 영역
2) 조직관리 영역 : 조직구성, 역량, 역할과 책임 정의, 사이버보안 문화 구축, 조직 구성원 책임 및 의무사항 등의 대응을 위한 평가 영역
3) 위험관리 영역 : 사이버보안 위험 관리 방법론, 위험 식별 및 평가, 위험처리, 취약점 관리, 정보자산 관리 평가 등의 대응을 위한 평가 영역
4) IT보안관리 영역 : IT시스템에 대한 관리, 멀웨어 대응, 이동식 저장장치 관리, 어플리케이션 관리 등의 대응을 위한 평가 영역
5) 개발보안관리 영역 : IT어플리케이션 및 제품 개발 관리, 변경관리, 클라우드 등 외부 서비스 관리, 보안제품에 대한 보안관리 등의 대응을 위한 평가 영역
6) 물리보안관리 영역 : 보호구역 관리 및 방문자 통제, 자산 반출입 관리 등의 대응을 위한 평가 영역
7) 협력사관리 영역 : 협력사 보안 관리, 중요 정보의 유통 및 폐기 등의 대응을 위한 평가 영역

3.2 사이버보안 관리체계 평가 모델 설계

앞에서 분류된 영역에 따라 ISO/SAE 21434와 TASAX VDA ISA Checklist 유구사항을 비교 분석하여 본 연구의 목표인 자동차 사이버보안 관리체계 구현 평가모델 항목을 총 7개 영역, 54개 항목으로 다음과 같이 도출하였다.

<표 2> 사이버보안 관리체계 구현 수준 평가 항목

영역	구분	평가항목	평가목표
관리체계	경영진의 지원과 관심	경영목표에 사이버보안 목표가 포함	경영 목표 달성을 위한 사이버보안 목표를 설정함
		사이버보안 인증 운영(ISO/IEC270	사이버보안 관리체계 운영에 대한 경영진의

영역	구분	평가항목	평가목표
		01, ISO/SAE21434, TISAX 등)	지원
		경영진의 사이버보안 프로그램 및 활동 검토	사이버보안 관리체계 운영 활동에 대한 경영진의 관심과 참여
	정책 및 지침	사이버보안 정책, 규정, 지침 문서화	사이버보안의 정책, 규정, 지침을 문서화 하고 배포함
		주기적인 검토 및 승인	법규, 요구사항에 대한 지속적 검토를 통한 정책 및 규정 개선
		교육 및 홍보 실행	구성원들에게 사이버보안 규정 준수 요구
	법규 및 요구 사항	사이버보안 관련 법률에 대한 검토 및 적용	사이버보안 법규 위반 위험에 대한 선제적 대응
		계약 또는 고객의 사이버보안 요구사항 검토 및 적용	경영 목표 달성을 위한 고객 요구사항 충족
		개인정보보호 규정 수립 및 적용	개인정보보호 법규 위반 위험에 대한 선제적 대응
조직 관리	조직(또는 담당자)	전담조직 또는 담당자 구성	사이버보안 업무를 담당할 자원 결정
		담당자의 전문성 평가 기준	사이버보안 업무 담당자의 역량 확보
		조직(담당자) 평가 기준 내 사이버보안 업무 포함	사이버보안 업무에 대한 평가를 적용, 운영 활동에 대한 동기 부여
	조직(또는 담당자)의 역할과 책임	직무기술서내 사이버보안 역할 지정	조직별, 담당자별 역할과 책임을 결정
		전문 교육 수강 의무(연간 40시간 이상)	담당자의 분야별 전문성 강화
		조직(담당자) 사이버보안 업무 활동 계획	운영 활동을 체계적으로 계획하고 자원을 투입함
	사이버보안 문화 구축	정기/비정기 사이버보안 교육	구성원들의 사이버보안 지식 향상
		비밀유지서약서 작성	구성원들의 사이버보안에 대한 책임 및 의무사항 요구
		정기/비정기 사이버보안 훈련(모의해킹, 악성코드이메일 등)	훈련을 통한 사이버보안 활동에 대한 대응 능력 향상
위험 관리	위험 관리	사이버보안 위험관리 방법	관리범위, 관리주기, 위험식별, 위험처리

영역	구분	평가항목	평가목표
		결정	우선순위 결정을 위함
		사이버보안 위험 식별, 평가 및 개선계획 수립	사이버보안 위험에 대한 지속적 관리 활동
		개선 결과에 대한 점검 및 결과 승인	위험 개선 활동이 효과적으로 수행되었는지 확인
	취약점관리	시스템 취약점에 대한 지속적 점검 및 개선 결과	시스템 취약점을 점검하고, 사전 제거를 함
		신규 취약점에 대한 정보 수집 및 대응 결과	신규 발생 취약점을 적시에 확인하고, 사전 제거를 함
		사이버보안 취약점 공유 및 홍보	구성원들의 사이버보안 문화 구축 및 자율적 참여 유도
	정보자산 관리	중요 정보자산에 대한 분류 기준에 따른 정보자산 목록 작성	중요 자산을 보호하기 위한 자원 투입 우선순위 결정
		IT자산에 대한 목록 및 세부 정보 관리	IT시스템의 신규 취약점 발생 시, 적용해야 할 대상을 결정함
		보안 업데이트 관리	취약점을 근본적으로 제거함
IT 보안 관리	네트워크	네트워크 방화벽 설치 및 관리	내부 네트워크를 외부 접근으로부터 보호함
		웹사이트 접근 통제	유해사이트 및 정보유출경로에 접근하는 것을 통제함
		네트워크 접속 통제	유선 및 무선 네트워크를 비인가자로부터 보호함
	PC관리	사용자 계정관리	사용자 계정 및 패스워드가 정책에 맞게 관리되도록 통제함
		안티바이러스 설치 및 관리	PC 및 서버 운영체계 바이러스/랜섬웨어 등 감염 방지
		저장매체 사용 통제	USB 저장장치, 모바일 저장장치 사용 통제
	업무시스템	정보 전달 시 암호화	이메일, 업무시스템 등 전송되는 중요 정보 보호(VPN, SSL, SSH 등)
		중요정보 저장 시 암호화	중요자산, 개인정보 등 시스템 저장 시 암호화를 통한 보호
		사용자 인증 관리	사용자 계정 생성, 변경, 삭제 관리 및 부가 인증 등을 통한

영역	구분	평가항목	평가목표
			보호
개발 보안 관리	개발 관리	기획, 개발, 이관 단계에서 보안 요구사항 점검	전체 개발 라이프사이클에서 보안 요구사항 검토 및 적용 확인
		개발, 테스트, 운영 시스템의 분리	개발과 운영을 분리하고, 접근 통제를 적용함
		소스코드 관리	소스코드에 대한 접근 제어 및 무결성 관리
	운영 관리	변경관리	변경에 대한 이력 관리 및 승인을 통한 통제
		데이터 관리	개발 및 테스트, 운영 데이터에 대한 기밀성 관리
		클라우드 서비스 관리	클라우드 서비스 사용 시 발생 가능한 위험 관리
	보안 제품 관리	보안 제품 분류 기준 및 자산 관리	고객 요구사항에 따른 보안제품 관리
		보안제품 보관 및 이용 시 접근 통제	비인가자 접근 통제 및 보안제품 노출 통제
		보안제품 취급자 관리	보안제품 취급자에 대한 보안 요구사항 교육 및 인식확보
물리 보안 관리	보호 구역 통제	보호구역 설정	접근 통제를 적용해야하는 보호 구역에 대한 정의
		보호구역내 물리보안시설 설치	출입통제장치, CCTV, 경보장치 등 보안시설을 통한 무단침입방지
		방문자 관리 및 차량 진입 통제	인가되지 않은 외부인 통제
	물품 반출입 관리	사진 촬영기기 통제	보안제품 및 중요 정보자산 촬영 통제
		반입 정보기기 통제	노트북, 모바일저장장치 등 정보 유출 경로 통제
		물류 보안관리	제품에 대한 보안 관리를 통한 보호
	보안 요구 사항	협력사와 계약 내 보안요구사항 포함	협력사의 보안관리 책임을 명시하고 요구사항을 충족하도록 요구함
		협력사와 비밀유지서약서 작성	협력사의 보안관리 책임과 의무사항을 인식함
		중요 정보의 유통, 저장, 폐기 관리 확인	협력사로 전달되는 도면 등 중요정보 유통 및 폐기에 대한 관리 요구

4. 평가모델 검증

4.1 평가항목 적합성 및 타당성 검증

도출한 평가항목에 대한 필요성과 타당성을 검증하기 위해 다수의 국내/외 기업 보안담당자 및 관련 분야 전문가 대상으로 이메일 발송후 자기기입식 응답으로 회신을 받는 설문을 실시하여 총 30명의 유의미한 데이터를 최종 확보하였다. 연구 결과 도출된 항목에 대해 평가항목의 중요도를 5점 리커트 척도로 응답하게 하였고, 필요한 업종(IT운영, 연구개발, 부품제조)을 선택하도록 하였다. 또한 응답자 특성 분석을 위해 근무 경력과 직무, 기업의 업종과 규모를 질문하였다.

선정된 설문 응답자 30명의 특성은 다음과 같다.

<표 3> 설문조사 응답자 특성(1)-업무경력

경력	전체	3년 미만	3-5년	5-10년	10년 초과
사례수 (명)	30	1	1	3	25
비중(%)	100	3	3	10	84

<표 4> 설문조사 응답자 특성(2)-소속기업의 업종

업종	전체	IT 기업	보안 기업	연구 개발	생산	기타(정부/공공/대학 등)
사례수 (명)	30	5	6	1	14	4
비중 (%)	100	17	20	3	47	13

<표 5> 설문조사 응답자 특성(3)-응답자의 담당업무

담당 업무	전체	IT	보안	연구 개발	생산	영업	기타
사례수 (명)	30	6	16	1	1	4	2
비중 (%)	100	20	54	3	3	13	7

<표 6> 설문조사 응답자 특성(4)-응답자의 직책

직책	전체	담당자	중간 관리자	부서장	임원이상
사례수 (명)	30	5	14	5	6
비중 (%)	100	17	46	17	20

<표 7> 설문조사 응답자 특성(5)- 직원 수

규모	전체	30명 이하	30~100명	100~200명	200~500명	500~1000명	1000명 이상
사례수(명)	30	1	1	4	2	1	21
비중(%)	100	3	3	14	7	3	70

총 54개 평가 항목에 대한 필요성 응답 확인 결과 대부분의 항목이 3점 이상의 필요성을 나타내었으며, 특히 IT보안관리 영역의 '네트워크 방화벽 설치 및 관리', '안티바이러스 설치 및 관리' 항목, 위험관리 영역의 '보안업데이트 관리' 항목이 가장 높았다.

또한 54개 평가항목에 대한 리커트 척도(1-5점) 응답 결과를 분석해 보면 항목별 평균은 3.53~4.90, 표준편차 범위는 0.4~0.95로 나타남을 확인할 수 있어 전체 항목 중 타 항목에 비해 편차가 심하지 않다는 것을 확인할 수 있다.

다음으로 신뢰도 검증을 위해 문항 내적 일치도(Internal consistency)를 구하기 위해 Cronbach's α 값을 계산하였다. 도출된 30개 설문항목의 응답에 대한 Cronbach's α 값은 0.881로 나타났으며, 이에 따라 각 설문항목은 신뢰도가 높다고 판단할 수 있다.

조사 결과에서 특징적인 것은 물리보안관리 영역 중 '물류 보안관리' 항목, 위험관리 영역중 '사이버보안 위험관리 방법 결정' 항목, IT보안관리 영역의 '정보 전달 시 암호화' 항목의 필요성이 상대적으로 낮은 것으로 평가되었다.

사이버보안 평가 항목들의 필요성 및 타당성 검토 후에 집단 특성에 의한 통계적 유의성을 추가적으로 분석하였다.

설문 조사결과, 도출한 54개 평가항목 모두 사이버보안 관리체계 구현 수준 평가에 필요한 항목이라고 답변되었지만, 응답 결과 4점 미만인 항목은 우선순위 "중", 4점 이상은 "상"으로 우선순위를 표기하였고, 그 결과 45개의 평가항목이 "상" 우선순위로 나타났다.

<표 8> 설문조사 답변 평균 및 우선순위

영역	구분	평가항목	평균	우선순위
관리체계	경영진의 지원과 관심	경영목표에 사이버보안 목표가 포함	4.33	상
		사이버보안 인증 운영(ISO/IEC27001, ISO/SAE21434, TISAX 등)	3.80	중
		경영진의 사이버보안 프로그램 및 활동 검토	4.00	상
	정책 및 지침	사이버보안 정책, 규정, 지침 문서화	4.40	상
		주기적인 검토 및 승인	4.47	상
		교육 및 홍보 실행	4.27	상
	법규 및 요구사항	사이버보안 관련 법률에 대한 검토 및 적용	4.30	상
		계약 또는 고객의 사이버보안 요구사항 검토 및 적용	4.37	상
		개인정보보호 규정 수립 및 적용	4.20	상
조직관리	조직(또는 담당자)	전담조직 또는 담당자 구성	4.50	상
		담당자의 전문성 평가 기준	4.03	상
		조직(담당자) 평가 기준 내 사이버보안 업무 포함	4.30	상
	조직(또는 담	직무기술서내 사이버보안 역할 지정	4.30	상
		전문 교육 수강 의무(연간 40시간 이상)	3.83	중
		조직(담당자)	4.17	상

영역	구분	평가항목	평균	우선순위
	당자)의역할과책임	사이버보안 업무 활동 계획		
	사이버보안문화구축	정기/비정기 사이버보안 교육	4.40	상
		비밀유지서약서 작성	4.50	상
		정기/비정기 사이버보안 훈련(모의해킹, 악성코드이메일 등)	4.37	상
위험관리	위험관리	사이버보안 위험관리 방법 결정	3.73	중
		사이버보안 위험 식별, 평가 및 개선계획 수립	4.07	상
		개선 결과에 대한 점검 및 결과 승인	4.17	상
	취약점관리	시스템 취약점에 대한 지속적 점검 및 개선 결과	4.50	상
		신규 취약점에 대한 정보 수집 및 대응 결과	4.33	상
		사이버보안 취약점 공유 및 홍보	4.17	상
	정보자산관리	중요 정보자산에 대한 분류 기준에 따른 정보자산 목록 작성	4.10	상
		IT자산에 대한 목록 및 세부 정보 관리	3.87	중
		보안 업데이트 관리	4.67	상
IT보안관리	네트워크	네트워크 방화벽 설치 및 관리	4.90	상
		웹사이트 접근 통제	3.87	중
		네트워크 접속 통제	4.50	상
	PC관리	사용자 계정관리	4.33	상
		안티바이러스 설치 및 관리	4.90	상
		저장매체 사용 통제	4.40	상
	업무	정보 전달 시 암호화	3.80	중
		중요정보 저장 시	4.43	상

영역	구분	평가항목	평균	우선순위
	시스템	암호화		
		사용자 인증 관리	4.10	상
개발보안관리	개발관리	기획, 개발, 이관 단계에서 보안 요구사항 점검	4.03	상
		개발, 테스트, 운영 시스템의 분리	4.17	상
		소스코드 관리	3.97	중
	운영관리	변경관리	4.10	상
		데이터 관리	4.07	상
		클라우드 서비스 관리	4.27	상
	보안제품관리	보안 제품 분류 기준 및 자산 관리	4.07	상
		보안제품 보관 및 이용 시 접근 통제	4.13	상
		보안제품 취급자 관리	4.10	상
물리보안관리	보호구역통제	보호구역 설정	3.90	중
		보호구역내 물리보안시설 설치	4.00	상
		방문자 관리 및 차량 진입 통제	4.17	상
	물품반출입관리	사진 촬영기기 통제	4.57	상
		반입 정보기기 통제	4.00	상
		물류 보안관리	3.53	중
	보안요구사항	협력사와 계약 내 보안요구사항 포함	4.47	상
		협력사와 비밀유지서약서 작성	4.50	상
		중요 정보의 유통, 저장, 폐기 관리 확인	4.10	상

4.2 최종 평가항목 선정

자동차 분야 사이버보안 관리체계 구현 수준 평가모델을 위한 최종 평가 항목은 업종별, 규모별로 분류하여 적용하면 아래와 같다.

※ 응답 우선순위가 '상'이면서 필요도 응답 '80%(24명) 이상인 항목만 채택

<표 8> 설문조사 답변 평균 및 우선순위

영역	구분	평가항목	우선순위	IT운영	연구개발	부품제조
관리체계	경영진의 지원과 관심	경영목표에 사이버보안 목표가 포함	상	V	V	
		사이버보안 인증 운영(ISO/IEC27001, ISO/SAE21434, TISAX 등)	중			
		경영진의 사이버보안 프로그램 및 활동 검토	상	V	V	V
	정책 및 지침	사이버보안 정책, 규정, 지침 문서화	상	V	V	V
		주기적인 검토 및 승인	상	V	V	V
		교육 및 홍보 실행	상	V	V	V
	법규 및 요구사항	사이버보안 관련 법률에 대한 검토 및 적용	상	V	V	V
		계약 또는 고객의 사이버보안 요구사항 검토 및 적용	상	V	V	V
		개인정보보호 규정 수립 및 적용	상	V	V	
조직관리	조직(또는 담당자)	전담조직 또는 담당자 구성	상	V	V	V
		담당자의 전문성 평가 기준	상	V	V	
		조직(담당자) 평가 기준 내 사이버보안 업무 포함	상	V	V	
	조직(또는 담당자)	직무기술서내 사이버보안 역할 지정	상	V	V	V
		전문 교육 수강 의무(연간 40시간 이상)	중			
		조직(담당자)	상	V	V	V
	의역할과 책임	사이버보안 업무 활동 계획				
	사이버보안 문화 구축	정기/비정기 사이버보안 교육	상	V	V	V
		비밀유지서약서 작성	상	V	V	V
		정기/비정기 사이버보안 훈련(모의해킹, 악성코드이메일 등)	상	V	V	
위험관리	위험관리	사이버보안 위험관리 방법 결정	중			
		사이버보안 위험 식별, 평가 및 개선계획 수립	상	V	V	
		개선 결과에 대한 점검 및 결과 승인	상	V	V	
	취약점 관리	시스템 취약점에 대한 지속적 점검 및 개선 결과	상	V	V	V
		신규 취약점에 대한 정보 수집 및 대응 결과	상	V	V	V
		사이버보안 취약점 공유 및 홍보	상	V	V	
	정보자산 관리	중요 정보자산에 대한 분류 기준에 따른 정보자산 목록 작성	상	V	V	
		IT자산에 대한 목록 및 세부 정보 관리	중			
		보안 업데이트 관리	상	V	V	V
IT	네	네트워크 방화벽	상	V	V	V

영역	구분	평가항목	우선순위	IT운영	연구개발	부품제조
보안관리	트워크	설치 및 관리				
		웹사이트 접근 통제	중			
		네트워크 접속 통제	상	V	V	V
	PC 관리	사용자 계정관리	상	V	V	V
		안티바이러스 설치 및 관리	상	V	V	V
		저장매체 사용 통제	상	V	V	V
	업무시스템	정보 전달 시 암호화	중			
		중요정보 저장 시 암호화	상	V	V	V
		사용자 인증 관리	상	V	V	V
개발보안관리	개발관리	기획, 개발, 이관 단계에서 보안 요구사항 점검	상	V	V	
		개발, 테스트, 운영 시스템의 분리	상	V	V	
		소스코드 관리	중			
	운영관리	변경관리	상	V	V	
		데이터 관리	상	V	V	V
		클라우드 서비스 관리	상	V	V	V
	보안제품관리	보안 제품 분류 기준 및 자산 관리	상	V	V	V
		보안제품 보관 및 이용 시 접근 통제	상	V	V	V
		보안제품 취급자 관리	상	V	V	
물리보안관리	보호구역통제	보호구역 설정	중			
		보호구역내 물리보안시설 설치	상	V	V	V
		방문자 관리 및 차량 진입 통제	상	V	V	V
	물품반출입	사진 촬영기기 통제	상	V	V	V
		반입 정보기기 통제	상	V	V	V
		물류 보안관리	중			
	관리					
	보안요구사항	협력사와 계약 내 보안요구사항 포함	상	V	V	V
		협력사와 비밀유지서약서 작성	상	V	V	V
		중요 정보의 유통, 저장, 폐기 관리 확인	상	V	V	V

5. 결 론

자동차 분야 사이버보안 관리체계 구축 수준 평가는 전 세계적으로 범위가 확대되고 요구사항이 강화되고 있으며, 각 공급사의 규모와 업종에 관계없이 의무사항으로 요구되고 있다. 또한, 해당 기준을 충족하기 위해서는 많은 시간과 자원이 투입되고, 장시간 동안 기업 환경에 내재화가 되어야 한다.

본 연구는 현재 대표적인 평가 기준인 ISO/SAE 21434와 TISAX 의 요구사항에 대한 구현을 완벽하게 준수하는 기준이 아니라, 공급망에 참여하는 각 기업들이 기본 수준을 자체적으로 평가하고, 향후 공식적인 인증을 획득하기 위한 기반 환경 구축을 위한 도구로 활용이 가능한 사이버보안 관리체계 구현 모델을 제시하고자 하는 필요성에 의해 시작하였다. 그에 따라, 선행연구를 통해 자동차 분야 사이버보안 관리체계 평가기준을 종합하여 반드시 필요한 평가 항목을 추출하고, 30명의 전문 집단의 설문조사를 통해 타당성과 적합성을 검증한 결과, 총 45개의 항목이 결정되었으며, 기존 ISO/SAE 21434와 TISAX 평가 요구사항을 기준으로 보안 영역별로 자체 평가 가능한 모델이 완성되었으며, 이는 자동차 공급망 참여 기업의 사이버보안 관리체계 구현 수준 평가를 위한 시간과 자원을 절약하고, 사이버보안 수준 향상을 위한 계획 수립에 기초자료를 제공하는 연구로서 의의가 있다고 할 수 있다.

참고문헌

[1] Zhendong Ma and Christoph Schmittner (2016), Threat Modeling for Automotive Security Analysis, Advanced Science and Technology Letters ,Vol. 139, 334-335.

[2] EINSA,(Dec. 2016), “Cyber Security and Resilience of smart cars”

[3] ALJOSCHA LAUTENBACH (2016), On Cyber-Security for In-Vehicle Software, CHALMERS UNIVERSITY OF TECHNOLOGY, 5.

[4] Christoph Schmittner and Georg Macher (2019), Automotive Cybersecurity Standards – Relation and Overview, 4-6.

[5] Matan Levi,Yair Allouche, and Aryeh Kontorovich (2017), Advanced Analytics for Connected Cars Cyber Security, 2.

[6] Stefan Marksteiner and Zhendong Ma (2019), Approaching the Automation of Cyber Security Testing of Connected Vehicles,” 1.

[7] Florian Sommer, Jürgen Dürrwang, and Reiner Kriesten (2019), Survey and Classification of Automotive Security Attacks, 17-18.

[8] Jay Kennedy, Thomas Holt & Betty Cheng(2019), Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking, JOURNAL OF CRIME AND JUSTICE Vol 42, 638.

[9] UNECE(2018), Draft recommendation on Cyber Security of the task force on cyber security and over-the-air isses of UNECE WP.29 GRVA.

[10] Christoph Schmittner, Georg Macher (2020), A Preliminary View on Automotive Cyber Security Management Systems, Conference paper, 3

[11] W. Kerber and D. Moeller (2019), “Access to data in connected cars and the recent reform of the motor vehicle type approval regulation.

[12] UNECE WP.29 GRVA, Draft recommendation on cyber security of the task force on cyber security and over-the-air issues of unece wp.29 grva., https://wiki.unece.org/pages/viewpage.action?pageId=60362218, 2022-10-21

[13] Escrypt(2019), Security Special2019/2020, 4

[14] ENX(2021), Participants handbook, https://www.enx.com/handbook/tisax-participant-handbook.html

[15] Escrypt(2019), Cybersecurity full speed ahead2019/2020, 4

[16] ENISA, 2019, good practices for security of Smart Cars

[17] ENISA, 2016, Cyber Security and Resilience of smart cars

[18] Christof Ebert, Jerome John, 김승훈, 2022, ISO 21434 통한 실질적 사이버 보안 대응, Automotive Electronics Magazine

[19] Navigating New Automotive Cybersecurity Regulations, ESCRYPT

[20] VDA ISA Checklist 5.0(2021), ENX

[21] TISAX Participants handbook(2021), ENX

[22] ybersecurity Best Practices for Modern Vehicles(2016), NHTSA

〔저자소개〕

백 은 호 (Eunho Baek)

2004년 2월 건국대학교 학사
2023년 2월 중앙대학교 석사
email : salue@naver.com