능동안전(일반)

자동차 V2X NCAP 해외 동향 및 국내 연구 방향

김혜수* · 전산암** · 조병찬*** · 정혁****

Overseas Trends and Domestic Research Directions for V2X NCAP

Hyesoo Kim*, Sanam Jeon**, Byeongchan Jo***, Hyuk Jung****

Key Words : V2X(차량사물통신), Connected-Car(커넥티드카), NCAP(자동차안전도평가), Accident prevention(사고예방안전성), C-ITS(차세대지능형교통체계),

ABSTRACT

This paper analyzes trends related to the introduction of V2X functions to NCAP(New Car Assessment Program) in three major overseas countries and presents domestic research directions to introduce V2X functions to KNCAP evaluation items.

유럽자동차안전도평가(EURO NCAP)는 소비자들이 차량 구매 시 참고할 수 있도록 차량에 적용된 최신 안전 기능에 대한 정보를 제공하는 'EURO NCAP ADVANCED REWARD' 제도를 시행하고 있으며 '20년에는 폭스바겐, '22년에는 벤츠 차량에 적용된 차량·사물통신(V2X) 기능을 선정하였다.
REWARD에 선정된 폭스바겐이 제공하는 V2X 기능은 ITS-G5(WAVE기반) 기술을 사용하여 전방 사고 및 도로 위험 정보 등에 대한 주의/경고 알림을 제공하는 것이며, 벤츠의 Car-to-X Communication은 자체 클라우드 서버를 통해 자사 차량에 대해 안전 운전을 위한 경고 알림 서비스를 제공하는 기능이다.
유럽은 'EURO NCAP ROADMAP 2025'에 따라 '23년부터 V2X 기능을 자동차안전도평가(NCAP)의 평가항목에 포함하여 종합평가점수에 반영될 예정이다.
중국은 차량·사물셀룰러통신(C-V2X) 기술을 사용하여 안전 운전 서비스 우선순위 및 경고 기능에 대한 평가기준, 평가방법 등 관련 연구를 진행 중이다. '25년에는 교차로 충돌 방지, 비상제동 조기 경고 서비스 등을 평가에 도입할 예정이며, '26년 이후에는 평가항목 확대를 위한 연구를 수행할 예정이다.
일본도 일본자동차안전도평가(JNCAP)에 V2X 기능을 포함한 안전 운전 지원 기술을 적용하기 위해 '21년부터 평가항목 검토를 시작하였으며 '24년까지 평가방법을 개발하고, '25년에는 NCAP 적용을 위한 예비시험을 진행할 예정이다.
국내에서도 V2X 기능을 한국자동차안전도평가(KNCAP)의 평가항목으로 도입하기 위해 평가기준 및 시험방법 개발 등 관련 연구를 진행하고 있다. 또한 V2X 시스템의 통신성능에 대해 최소한의 성능기준과 이를 평가하기 위한 평가방법 개발에 관한 연구도 함께 진행하고 있다.

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(과제번호 22AMDP-C162964-02: 자동차 V2X 통신성능 안전성 및 전자파 적합성 평가기술 개발)

* 자동차안전연구원 커넥티드카연구처/연구원
** 자동차안전연구원 커넥티드카연구처/연구원
*** 자동차안전연구원 커넥티드카연구처/선임연구원
**** 자동차안전연구원 부품연구처/처장
E-mail : b210245@kotsa.or.kr

자동차 사이버보안 관리체계 해외 동향

염윤숙* · 이하연** · 엄성욱*** · 김성범****

Overseas Trends in the Automotive Cybersecurity Management System

Yoonsook Yeom*, Hayeon Lee**, Sungwook Eom***, Sungbeum Kim****

Key Words : Cybersecurity management system(사이버보안 관리체계), Connected car(커넥티드카), IEC 21434

ABSTRACT

This paper intends to prepare proper Cybersecurity Management System certification assessment methods for domestic situations by analyzing overseas trends related to automotive Cybersecurity Management System.

자동차와 교통 인프라의 지속적인 첨단화에 따라 보다 교통 편의성이 향상되고 있으나, 자동차가 외부와 통신으로 연결되는 등 보안 취약점이 증가하고 있어 자동차에 대한 해킹과 사이버공격이 우려되는 상황이다.
자율주행차 시장은 핵심기술인 센서, V2X통신, AI컴퓨팅 기술 발전에 힘입어 점차 확대되고 있다. 빠른 성장 속도와 함께, 운전자의 주행 안전 및 프라이버시에 대한 우려도 커지고 있다. 자율주행을 위해 더 많은 전자 제어시스템이 탑재되고, 다양한 외부 디바이스들과 실시간 네트워크를 형성할수록, 차량 내외부 위협 범위는 확대되기 때문이다.
이에 따라, UN 산하 자동차 국제기준 담당기구(WP.29)에서 최초의 자동차 사이버보안 국제기준을 2020년 6월에 제정하였고 2022년 7월 시행하였다. 규제를 어길 시 실질적인 무역 장벽으로 작용할 수 있는 만큼, 철저한 대비가 필요하다. 하지만 기존의 자동차의 안전기준들이 각 차량형식들의 인증만 진행하던 것과 달리 UNR 155의 경우 차량형식인증의 사전조건으로 제작사가 사이버보안을 확보한 차량을 만들 수 있는지 제작사의 사이버보안 역량을 인증해주는 사이버보안관리체계(CSMS) 인증개념이 추가되어 있다.
사이버보안관리체계 인증이란, 제작사의 사이버보안 관리시스템에 대한 평가로, 보안 위협을 식별 평가 분류 관리하기 위한 프로세스, 차량 보안 시험을 위한 프로세스, 보안위협을 모니터링하고 탐지 대응하는 프로세스, 차량 사이버보안 확보를 위한 조직체계, 교육 문화 등 제작사의 전반적인 역량에 대한 인증을 말한다. 본 연구는 국제 사이버보안 관리체계 국제 인증 동향을 분석하고 국내 실정에 적합한 CSMS 인증 심사 방안을 검토해 본다.

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(22AMDP-C162334-02:자동차 통합보안 안전성 평가기술 개발)

* 자동차안전연구원 커넥티드카연구처/연구원
** 자동차안전연구원 커넥티드카연구처/연구원
*** 자동차안전연구원 커넥티드카연구처/선임연구원
**** 자동차안전연구원 커넥티드카연구처/처장
E-mail : b220260@kotsa.or.kr

자동차 사이버보안에서 연관 취약점 분석을 위한 휘처 공학 적용 방법

박효승* · 이하연** · 엄성욱*** · 김성범****

Method to Apply Feature Engineering for Analyzing Related Vulnerabilities in Automotive Cyber Security

Hyoseung Park*, Hayeon Lee**, Sungwook Eom***, Sungbum Kim****

Key Words : Cyber security management system(사이버보안 관리체계), Connected car(커넥티드카), Threat analysis and risk assessment(위협 분석 및 위험 평가), Software feature engineering(소프트웨어 휘처 공학)

ABSTRACT

This paper describes a method to secure software design elements and hardware traceability in automotive electronic devices by supplementing feature engineering used in software engineering so that it can be used efficiently in automotive cyber security.

최근 자동차가 무선 네트워크에 연결되는 커넥티드카를 해커가 해킹하여 피해를 입히는 사례가 증가하고 있어 자동차 사이버보안의 경각심이 높아지고 있다. 지프의 체로키 차량은 해킹하여 원격으로 차량을 움직이거나 차량 잠금장치를 해제할 수 있었으며, 테슬라 차량은 운전자의 차량키 데이터를 원격으로 복제하여 차량을 점유할 수 있었다. 이러한 해킹은 자동차를 제어하는 전자장치가 증가하고 전자장치는 소프트웨어로 제어하기 때문에 가능하며, 자동차의 기능이 복잡해지면서 사이버보안 취약점은 하나의 기능, 소프트웨어 모듈, 하드웨어가 아닌 이들 간의 연계로 인해 복합적인 취약점이 발생할 수 있다. 그리고 복합적인 취약점은 정성적인 분석만으로는 발견하기 힘들다는 문제가 있다. 이를 해결하기 위해서는 차량 내부 E/E아키텍처 설계 시 설계 요소간 추적성을 확보해야 한다.
휘처 공학은 소프트웨어 요구사항 분석 방법 중 하나로 소프트웨어 요구사항 정의 및 분석영역인 문제영역과 소프트웨어 설계 영역인 해결영역을 휘처를 이용해 연결하여 추적성을 향상시키는 방법이다. 하지만 휘처 공학은 자동차 사이버보안의 특성을 고려하고 있지 않기 때문에 이점을 보완할 필요가 있다.
본 논문은 소프트웨어 공학에서 사용하는 휘처 공학을 자동차 사이버보안에서 효율적으로 사용할 수 있도록 보완하여 자동차 전자장치내 소프트웨어 설계 요소와 하드웨어 추적성을 확보하는 방법 및 TARA(Threat Analysis and Risk Assessment) 분석 결과와 휘처를 사용하여 연관 취약점 찾아낼 수 있는 방법을 소개하고자 한다.

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(22AMDP-C162334-02:자동차 통합보안 안전성 평가기술 개발)

* 자동차안전연구원 커넥티드카연구처/연구원
** 자동차안전연구원 커넥티드카연구처/연구원
*** 자동차안전연구원 커넥티드카연구처/선임연구원
**** 자동차안전연구원 커넥티드카연구처/처장
E-mail : b210534@kotsa.or.kr

자동차 사이버보안 시험 국제 동향 연구

하동연* · 이하연** · 김성범*** · 이정기****

Dongyeon Ha*, Hayeon Lee**, Sungbeum Kim***, Junggi Lee****

Key Words : Cyber security management system(사이버보안 관리체계), Connected car(커넥티드카), Threat analysis and risk assessment(위협 분석 및 위험 평가)

ABSTRACT

세계적으로도 자동차 보안 기준이 강화되는 추세다. 유엔 유럽경제위원회(UNECE)가 2020년 6월 채택한 자동차 사이버보안 국제기준(UNR 155, WP29)은 올해 7월부터 시행에 들어간다. UNECE 회원국(유럽·아시아 등 60여 개국)에 등록되는 신형 자동차의 차량형식승인(VTA)을 받기 위해서는 자동차사이버보안관리체계(CSMS)에 대한 인증을 의무적으로 취득해야 한다.차량형식인증(vta)는규정을 준수하여 목표 시장에 진출 및 보다 높은 수익 창출하고 제품을 소비자에게 신속하게 제공하며 규정 불이행 또는 리콜로 인한 과징금 및 처벌 방지, 차량 안전을 확보하여 소비자 및 규제 기관으로부터 브랜드 명성 제고 와 같은 장점과 최근 다양한 자동차 공격경로로 서버 공격, 스마트키 악용, 모바일 어플리케이션, obd port, 인포테인먼트 시스템, it 시스템 , 센서 활용, ecu/gw 등 , 차량내 네트워크 wifi/bt/odb 동글, 셀룰러 통신, usb/sd 카드 포트와 같은 사이버보안 공격경로가 다양해지면서 이러한 이유로 일본 및 유럽국가에서 차량형식승인을 시행하고 있다. 본 연구에서는 차량형식승인을 시행하는 해외국가동향을 파악하여 소개하고자 한다.또한 향후 국내 차량형식승인 도입에 관련하여 논하고자한다.

본 연구는 국토교통부/국토교통과학기술진흥원의 지원으로 수행되었음(22AMDP-C162335-02:자동차 통합보안 안전성 평가기술 제도화방안 연구)

* 한국교통안전공단 자동차안전연구원/위촉연구원5급
** 한국교통안전공단 자동차안전연구원/선임
*** 한국교통안전공단 자동차안전연구원/처장
**** 한국교통안전공단 자동차안전연구원/실장
E-mail : b210534@kotsa.re.kr

V2X 이상행위 관리기술 연구동향

한승희* · 박우근** · 노지아*** · 김성범****

Overseas Trend for V2X Misbehavior Management Technology

Seunghui Han*, Woogeun Park**, Nohji Ah***, Sungbum Kim****

Key Words : V2X(차량사물통신), Misbehavior(이상행위), Misbehavior management technology(이상행위 관리기술), Basic safety message(기본안전메시지)

ABSTRACT

V2X Misbehavior management technology detects vehicles sharing incorrect information in the V2X environment due to vehicle failure or hacker cyberattacks, and revokes the relevant certificate to secure a reliable C-ITS environment. In this study, we look at the trends of Misbehavior management technology for a safe V2X environment, and suggests pending issues for domestic application.

자율주행기술이 4차 산업혁명의 핵심기술로 주목받으면서 많은 분야에서 자율주행기술개발이 활발하게 이루어지고 있으며, 다양한 전자부품을 포함하는 자율주행 자동차는 기존의 자동차 제작사와 더불어 IT 및 통신 분야 등의 기업들도 기술개발에 뛰어들고 있다.

이러한 자율주행 자동차는 각종 전장부품을 탑재하고 안전한 주행을 위해 V2X통신을 활용하여 주변 사물과 정보를 교환하며 자율주행의 안전도를 향상시키기 위한 기술개발을 추진하고 있다.

탑승자와 보행자의 안전이 중요한 차량이 통신기술과 접목됨에 따라 안전한 V2X통신 환경의 중요성이 대두되었고, 이를 예방하고 안전한 V2X통신 환경을 위한 V2X 이상행위 관리기술에 대한 연구가 국내외적으로 진행되고 있다.

V2X 이상행위 관리기술은 차량의 고장이나 해커의 사이버공격으로 인해 잘못된 정보(V2X 이상정보)를 V2X 환경에 공유하는 차량을 감지하고, 해당 인증서를 폐지하여 신뢰성 있는 C-ITS 환경을 확보하게 해준다.

따라서 이상행위 관리기술은 차량의 속도, 위치정보 등의 기본안전메시지(BSM)를 기반으로 수신 불가 거리에서 송신한 기본안전메시지, 위치 불일치, 가속정보와 일관되지 않은 위치 등의 차량의 고장에 대한 이상행위의 항목과 검증기관에 보고하기 위한 단일 또는 다수의 기본안전메시지를 포함한 보고규격 등을 규정하고 있다.

현재 북미(SCMS Manger)와 유럽(ETSI) 등 다양한 국가의 표준기관에서 자율주행 자동차의 이상행위 항목 및 보고규격 대한 기준을 수립하고 있다.

본 연구에서는 안전한 V2X통신 환경을 위한 이상행위 관리기술 규격 국제동향 및 국내 기술개발 현황을 알아보고 향후 국내 자율주행 자동차 운행에 이상행위 관리기술을 적용하기 위한 현안사항 및 이슈를 제시한다.

* 자동차안전연구원 커넥티드카연구처/연구원
** 자동차안전연구원 커넥티드카연구처/연구원
*** 자동차안전연구원 커넥티드카연구처/연구원
**** 자동차안전연구원 커넥티드카연구처/처장
E-mail : shhan@kotsa.or.kr

자율주행 돌발 상황 대응을 위한 영상 기반 AI 학습용 엣지케이스 데이터셋 연구

박명진* · 전산암** · 최기웅*** · 김성범****

Study a Edge-case Dataset for Image-based A.I. Learning in Respond to Unexpected Situations

Myungjin Park*, Sanam Jeon**, Giung Choi***, Sungbum Kim****

Key Words : Autonomous driving(자율주행), Unexpected situations(돌발 상황), Training dataset(학습용 데이터셋)

ABSTRACT

Interest in autonomous driving technology is growing in the government and market. As large scale of data is essential to enhance the performance of autonomous vehicles, demand for dataset to train AI is getting larger. Different kinds of dataset are shared these days but to drive on a real road, AI should be trained how to respond to unexpected situations. Building datasets covering all kinds of unexpected situations costs a lot. Therefore, in this paper, we introduce the results of study about developing unexpected scenarios based on accident cases using TAAS(Traffic Accident Analysis System). Scenarios are developed by dividing the types of accident into car-to-car accidents, vehicle-only accidents, and vehicle-to pedestrian accidents. Based on the scenario, we embodied data collection plans using simulator, and study datasets by configuring collection environment.

"모빌리티 혁신 로드맵" 발표 등 자율주행차 상용화에 대한 관심이 정부와 시장에서 커지고 있다. 자율주행은 AI 기반의 신경망을 이용한 딥러닝이 핵심을 이루고 있고 대규모의 빅데이터를 통한 학습이 필요한 만큼 자율주행 차량의 성능 고도화를 위한 학습용 데이터의 수요가 증가하고 있다. 이에, 국내·외에서 KITTI, Waymo 등 자율주행 데이터셋을 구축 및 공개했다.

하지만 공개된 데이터셋은 일반 주행 환경 위주의 데이터를 포함하고 있다. 자율주행 차량의 실도로 주행을 위해서는 일반적인 주행 환경이 아닌 돌발 상황에서의 대응에 대해서도 학습이 되어있어야 한다. 상시 공사 구간, 사고지역, 차량 고장 및 낙하물 등 위험이 있는 상황에서의 회피를 위해 돌발 상황에 대한 AI 학습용 데이터 구축이 필요하다. 운행 중 발생 가능한 모든 위험에 대한 데이터셋을 구축하기 위해서는 많은 비용이 소모된다. 또한, 현재 자율주행 차량의 통계자료가 부족하다. 따라서 본 논문에서는 TAAS(교통사고 분석시스템)를 바탕으로 일반 차량의 실제 사고 사례 기반 돌발 상황 시나리오 개발 및 데이터셋 연구 결과를 소개한다.

TAAS 자료를 기반으로 차대차사고, 차량 단독 사고, 차대 보행자 사고로 유형을 나누어 시나리오를 개발하였다. 시나리오를 바탕으로 시뮬레이터를 이용해 데이터 수집 계획을 구체화하였고 환경을 구성하여 자율주행 데이터셋을 연구하였다.

* 자동차안전연구원 커넥티드카연구처/연구원
** 자동차안전연구원 커넥티드카연구처/연구원
*** 자동차안전연구원 커넥티드카연구처/책임연구원
**** 자동차안전연구원 커넥티드카연구처/처장
E-mail : myung196@kotsa.or.kr