



**Frontier of Cyber War:
K-사이버보안의 기술 주권과 미래**



자율주행 기술 트렌드에 따른 반도체 센서 동향 및 사이버보안 기술의 필요성

이정규*

Trends in Semiconductor Sensors According to Autonomous Driving Technology Trends and the Necessity of Cybersecurity Technology

Junggue Lee*

Key Words : Autonomous driving(자율주행), Cybersecyurity(사이버보안), Semiconductor(반도체)

ABSTRACT

자율주행 기술 트렌드는 인식 판단 제어의 전통적인 기술이 고정밀, 고성능 반도체 및 센서의 개발에 의해 확장되고 있는 형태로 바뀌고 있다. 고정밀의 인식 센서의 개발로 기존에 구현하기 어려웠던 안전, 편의 기술에 대한 세부 기술들이 개발되고 있으며, 고성능 반도체 AP 개발로 복잡한 AI 알고리즘을 적용한 정확하고 빠른 판단 로직을 구현할 수 있게 되었다. 자율주행기술은 하드웨어의 진화에 따라 다양한 소프트웨어 기술로 확장되기 때문에 원격 소프트웨어 업데이트(OTA, Over The Air)가 필수적인 미래차 발전 기술로 대두되고 있으며, 중앙집중형 HPC로 차량 아키텍처가 구성됨에 따라 업데이트 대상이 ‘제어’ 뿐만 아니라 ‘인식’, ‘판단’ 에 대한 소프트웨어도 네트워크를 통한 업데이트가 가능하도록 진화하고 있다. 이에 따라 네트워크에 대한 각 소프트웨어의 사이버보안 기술이 필수 기술로 논의가 되고 있다. 본 자료를 통해 자율주행 기술 트렌드 소개와 반도체 센서의 기술 동향, 이에 따른 사이버보안 기술과의 연관성 및 필요성에 대해 소개하고자 한다.

* 한국자동차연구원/책임연구원
E-mail : jglee1@katech.re.kr

AI 활용 사이버보안 코드 검증 및 테스트 케이스 자동화

정원영*

AI-driven Security Code Remediation and Test Case Generation

Won-young Chung*

Key Words : Cyber security(사이버보안), Static analysis(정적분석), Ai-driven security(AI기반보안), Test case generation(테스트케이스생성), Code remediation(코드결함수정), Rag(검색증강생성)

ABSTRACT

This research presents AI-driven approaches for enhancing cyber security code quality and automating test case generation.

First, we address the high false positive rate problem in AI code guidance. When static analysis tools detect code defects, our RAG-based system retrieves relevant coding rules and guidelines from a pre-constructed knowledge base containing organizational coding standards and security best practices. Unlike generic AI models, this retrieval-augmented approach provides precise, context-aware remediation guidance grounded in established policies. The system explains each defect clearly and offers actionable solutions aligned with domain-specific requirements, significantly reducing false positives.

Second, we develop a GAN-based automated test case generation system for CAN protocol security testing. The GAN model is trained on existing CAN protocol test cases to learn valid patterns and generate comprehensive test scenarios. A key feature is the continuous learning mechanism where failed test cases are incorporated back into the training dataset, enabling the model to iteratively improve its generation capabilities and achieve better test coverage organizational policies.

* SM솔루션즈/기술이사

E-mail : wonchung@smsolus.com

민간 스마트선박 사이버보안 기반 조성 추진 현황

김지명*

Progress of Private Sector Initiatives to Establish a Cybersecurity Framework for Smart Ships

Jimyung Kim*

Key Words : Smart Ship(스마트선박), Cybersecurity(사이버보안), Cybersecurity Drill(모의훈련), Security Assessment (보안점검)

ABSTRACT

As advanced technologies such as AI and big data continue to converge with traditional industries, new forms of converged industries are steadily emerging. While these industries bring greater convenience and prosperity to our daily lives, they also introduce unforeseen risks and incidents. In particular, the maritime shipping industry, which serves as the backbone of national economic activity, is no longer operating in isolation. With the adoption of cutting-edge IT and OT technologies and the increasing connectivity between ship and shore, cyber threats traditionally seen in IT environments are now extending into the maritime domain. To address this, the Korea Internet & Security Agency (KISA) is promoting a cybersecurity internalization initiative that aims to proactively identify potential security threats in smart ships and provide various solutions to mitigate them. Through this presentation, KISA seeks to introduce the key activities and progress of its ongoing Smart Ship Cybersecurity Program.

AI와 빅데이터 등의 첨단 기술이 기존 산업과 융합되면서 새로운 융합산업이 지속 등장하고 있습니다. 이러한 융합 산업은 우리의 삶을 더욱 편리하고 풍요롭게 만드는 동시에, 예기치 못한 사고를 초래하기도 합니다. 특히 국가 경제 활동에 필수적인 역할을 수행하는 해상 물류의 중심인 선박 산업도 더 이상 폐쇄적으로 운영되지 않고, 최신 IT 및 OT 기술을 도입하기 시작하며, 육상과의 통신 접점이 증가함에 따라 전통적인 IT 산업에서 발생하던 보안 위협이 선박 산업으로 전이되고 있습니다. 이에 한국인터넷진흥원(KISA)은 스마트선박에서 발생할 수 있는 보안 위협을 사전에 식별하고, 식별된 위협에 대응하기 위한 다양한 솔루션을 제공하기 위한 보안 내재화 지원 사업을 추진하고 있습니다. 이번 발표를 통해 KISA가 추진 중인 스마트선박 보안 사업에 대한 구체적인 내용을 소개하고자 합니다.

* 한국인터넷진흥원/책임연구원
E-mail : jimyungkim@kisa.or.kr

자동차 사이버보안 관리체계(CSMS) 인증 절차

최병국* · 이민표** · 구성서***

Automotive Cybersecurity Management System (CSMS) Certification Procedure

Beoungkug Choi*, Minpyo Lee**, Seongseo Ku***

Key Words : Cybersecurity(사이버보안), UNR155/156, CSMS(사이버보안관리체계), SUMS(소프트웨어업데이트 관리체계)

ABSTRACT

South Korea implemented its automotive cybersecurity regulations starting in August 2025, mandating the compulsory application of cybersecurity measures to all vehicles produced and sold domestically. Europe also enforced its legislation from July 2024. To sell vehicles in both South Korea and Europe, vehicle manufacturers must establish a Cybersecurity Management System (CSMS) and a Software Update Management System (SUMS), apply cybersecurity to their vehicles, and obtain the corresponding certification for compliance. This document introduces the current state of cybersecurity in the automotive market and the trends in cybersecurity legislation, and it explains South Korea's Automotive Cybersecurity Management System (CSMS) certification procedure.

* Fescaro/과장

** Fescaro/팀장

*** Fescaro/상무

E-mail : beoungkug.choi@fescaro.com